



# Overview

Casdoor is a UI-first [Identity Access Management \(IAM\)](#) / [Single-Sign-On \(SSO\)](#) platform based on OAuth 2.0, OIDC, SAML and CAS.

You need to enable JavaScript to run this app.

Casdoor serves both the web UI and the login requests from the application users.

# Casdoor features:

1. Front-end and back-end separate architecture, developed by Golang, Casdoor supports high concurrency, provides web-based managing UI and supports multiple languages(Chinese, English).
2. Casdoor supports third-party applications login, such as GitHub, Google, QQ, WeChat, etc., and supports the extension of third-party login with plugins.
3. With [Casbin](#) based authorization management, Casdoor supports ACL, RBAC, ABAC, RESTful accessing control models.
4. Phone verification code, email verification code and password retrieval functions.
5. Accessing logs auditing and recording.
6. Alibaba Cloud, Tencent Cloud, Qiniu Cloud image CDN cloud storage.
7. Customizable registration, login, and password retrieval pages.
8. Casdoor supports integration with existing systems by db sync, so users can transition to Casdoor smoothly.
9. Casdoor supports mainstream databases: MySQL, PostgreSQL, SQL Server, etc., and supports the extension of new databases with plugins.

# How it works:



## Step 0 (Pre-knowledge)

1. Casdoor's authorization process is built upon the OAuth 2.0 protocol, therefore it's highly recommended to take a brief look at how indeed does OAuth 2.0 works. An [introduction](#) to OAuth 2.0.

## Abstract Protocol Flow



## Step 1 (Authorization Request)

Your Application (could be a website or whatever) should compose an URL in this format

`endpoint/login/oauth/`

`authorize?client_id=xxx&response_type=code&redirect_uri=xxx&scope=read&state=xxx`.

In the URL replace `endpoint` with your Casdoor's host URL, and replace `xxx` with your own info.

### ⓘ HINTS

How to fill out the `xxx` parts?

- For `client_id`: you can find this under each single Application
- For `redirect_uri`: you should set this to your own Application's callback URL, with this info, Casdoor can know where to send info back after authorization
- For `state`: you should fill this out with your Application name

The Application will speak to the user: *"Hey, now I need some resources and I need your permission to take these resources, Do you mind going to this URL and filling out your*

*username and password for me?"*

With the correctly composed URL, your Application will make a user launch a request to this URL, and the `Authorization Request` is done.

## Step 2 (Authorization Grant)

This step is straightforward: the user is redirected to the URL composed above, and the user will see the login page from Casdoor. By typing the correct username and credential into the login page, Casdoor now knows the identity of the user, and is about to send two keywords: `code` and `state` back to the callback URL set in Step 1.

The user opens the URL and provides the credentials to Casdoor. 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`)*"

With these two keywords sent back to your Application, the authorization is now granted to the app, and thus `Authorization Grant` is completed.



Casdoor also provides third-party logins, in this case, you will not see the credentials entry page but a list of third-party providers. You can login to your app using these providers, with Casdoor as a middle layer (middleware).

## Step 3 (Authorization Grant)

In this step, your Application already has the code in hand from Step 2, and it will speak to Casdoor: "*Hey, now the user agreed to give me the `code`, do you wanna check this `code` out and give me the `access_token`?*"

## Step 4 (Access Token)

In this step, Casdoor speaks back to the Application: "*You know what, this `code` seems legit, you must be the right Application. Come here, it's the `access_token`.*" With this `code`,

Casdoor knows that it is an authorized Application (authorization given by the correct user in Step 2) trying to get the `access_token` (, which will be used later to get more useful things).

## Step 5 (Access Token)

In this step, your Application says: "Nice one, just got the fresh-and-tasty `access_token`, I can now use it to get something more valuable from the `Resource Server`!"

And your Application turns to the `Resource Server`: "Hey buddy, wanna check this `access_token` out? I got this from Casdoor and do you want to see if this is the correct one you had with Casdoor?"

## Step 6 (Protected Resource)

The `Resource Server` speaks back to your Application: "Not bad ~ it seems just like the one I had with Casdoor, and Casdoor says whoever holds this `access_token` can have these `Protected Resources`. Now, you take it!"

And this is basically how Casdoor works with your Application.

### HINT

Casdoor can play both `Authorization Server` and `Resource Server` parts, i.e. Casdoor authorizes our Application to get resources (e.g. usually the current logged in user's info) from Casdoor's database.

## Online demo

### Casdoor

Here is an online demo deployed by Casbin.

- [Casdoor official demo](#)

Global admin login:

- Username: `admin`
- Password: `123`

## Casbin-OA

Casbin-OA is one of Casbin web apps. It uses Casdoor as authentication.

- [Casbin-OA](#)
- Source code: <https://github.com/casbin/casbin-oa>

## Casnnode

Casnnode is the official forum developed by Casbin community.

It uses Casdoor as authentication platform and manage members.

- [Casnnode](#)
- Source code: <https://github.com/casbin/casnnode>

## Architecture

Casdoor contains 2 parts:

Name	Description	Language	Source code
Frontend	Web frontend UI for Casdoor	JavaScript + React	<a href="https://github.com/casdoor/casdoor/tree/master/web">https://github.com/casdoor/casdoor/tree/master/web</a>
Backend	RESTful API backend for Casdoor	Golang + Beego + SQL	<a href="https://github.com/casdoor/casdoor">https://github.com/casdoor/casdoor</a>

# Core Concepts

As Casdoor's administrator, you should get familiar with at least 4 core concepts: Organization, User, Application and Provider.

## 💡 TIP

In the following parts, we will use the demo site: <https://door.casdoor.com> as example.

## Organization

In Casdoor, an organization is a container for users and applications. E.g., all the employees of a company or all the customers of a business can be abstracted as one organization. The Organization class definition is shown as follows:

```
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"`
}
```

## User

A user in Casdoor can log into an application. One user can only belong to one organization, but can have the ability to log into multiple applications that owned by the organization. Currently there are two types of users in Casdoor:

- Users under `built-in` organization, like `built-in/admin`: the global administrators, have the full administrator power on the Casdoor platform.
- Users under other organizations, like `my-company/alice`: normal users, can only sign up, sign in, sign out, change his/her own profile, etc.

In Casdoor API, a user is usually identified as `<organization_name>/<username>`, e.g., the default administrator of Casdoor is denoted as `built-in/admin`. There is also a property in user called `id`, which is a UUID like `d835a48f-2e88-4c1f-b907-60ac6b6c1b40`, it can also be chosen as a ID for a user by an application.

## 💡 TIP

If your application is only for one organization, you can just use `<username>` instead of `<organization_name>/<username>` as user ID across your application for simplicity.

The User class definition is shown as follows:

```

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"`
    UpdatedTime string `xorm:"varchar(100)" json:"updatedTime"`

    Id          string `xorm:"varchar(100)" json:"id"`
    Type        string `xorm:"varchar(100)" json:"type"`
    Password    string `xorm:"varchar(100)" json:"password"`
    PasswordSalt string `xorm:"varchar(100)" json:"passwordSalt"`
    DisplayName  string `xorm:"varchar(100)" json:"displayName"`
    Avatar      string `xorm:"varchar(500)" json:"avatar"`
    PermanentAvatar string `xorm:"varchar(500)" json:"permanentAvatar"`
    Email       string `xorm:"varchar(100) index" json:"email"`
    Phone       string `xorm:"varchar(100) index" json:"phone"`
    Location    string `xorm:"varchar(100)" json:"location"`
    Address     []string `json:"address"`
    Affiliation string `xorm:"varchar(100)" json:"affiliation"`
    Title       string `xorm:"varchar(100)" json:"title"`
    IdCardType  string `xorm:"varchar(100)" json:"idCardType"`
    IdCard      string `xorm:"varchar(100) index" json:"idCard"`
    Homepage   string `xorm:"varchar(100)" json:"homepage"`
    Bio         string `xorm:"varchar(100)" json:"bio"`
    Tag         string `xorm:"varchar(100)" json:"tag"`
    Region      string `xorm:"varchar(100)" json:"region"`
    Language    string `xorm:"varchar(100)" json:"language"`
    Gender      string `xorm:"varchar(100)" json:"gender"`
    Birthday    string `xorm:"varchar(100)" json:"birthday"`
    Education   string `xorm:"varchar(100)" json:"education"`
    Score       int    `json:"score"`
    Ranking     int    `json:"ranking"`
    IsDefaultAvatar bool  `json:"isDefaultAvatar"`
    IsOnline    bool  `json:"isOnline"`
    isAdmin     bool  `json:"isAdmin"`
    IsGlobalAdmin bool  `json:"isGlobalAdmin"`
    IsForbidden bool  `json:"isForbidden"`
    IsDeleted   bool  `json:"isDeleted"`
    SignupApplication string `xorm:"varchar(100)" json:"signupApplication"`
    Hash        string `xorm:"varchar(100)" json:"hash"`
    PreHash     string `xorm:"varchar(100)" json:"preHash"`

    CreatedIp    string `xorm:"varchar(100)" json:"createdIp"`
    LastSigninTime string `xorm:"varchar(100)" json:"lastSigninTime"`
    LastSigninIp  string `xorm:"varchar(100)" json:"lastSigninIp"`

    Github      string `xorm:"varchar(100)" json:"github"`
    Google      string `xorm:"varchar(100)" json:"google"`
    QQ          string `xorm:"qq varchar(100)" json:"qq"`
    WeChat      string `xorm:"wechat varchar(100)" json:"wechat"`
    Facebook    string `xorm:"facebook varchar(100)" json:"facebook"`
    DingTalk    string `xorm:"dingtalk varchar(100)" json:"dingtalk"`
    Weibo       string `xorm:"weibo varchar(100)" json:"weibo"`
    Gitee       string `xorm:"gitee varchar(100)" json:"gitee"`
    LinkedIn    string `xorm:"linkedin varchar(100)" json:"linkedin"`
    Wecom       string `xorm:"wecom varchar(100)" json:"wecom"`
    Lark        string `xorm:"lark varchar(100)" json:"lark"`
    Gitlab      string `xorm:"gitlab varchar(100)" json:"gitlab"`
    Apple       string `xorm:"apple varchar(100)" json:"apple"`
    AzureAD    string `xorm:"azuread varchar(100)" json:"azuread"`
    Slack       string `xorm:"slack varchar(100)" json:"slack"`

    Ldap        string `xorm:"ldap varchar(100)" json:"ldap"`
    Properties  map[string]string `json:"properties"`
}

```

# Application

An application represents a web service that needs to be protected by Casdoor. E.g., a forum site, an OA system, a CRM system are all applications.

```
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:"--" json:"organizationObj"`

    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"`
}
```

Each application can have its own customized sign up page, sign in page, etc. E.g., the root login page `/login` (like: <https://door.casdoor.com/login>) is the sign in page only for Casdoor's built-in application: `app-built-in`.

An application is a "portal" or "interface" for a user to log into Casdoor. A user must go through one application's sign in page to log into Casdoor.

Application	Sign up page URL	Sign in page URL
app-built-in	<a href="https://door.casdoor.com/signup">https://door.casdoor.com/signup</a>	<a href="https://door.casdoor.com/login">https://door.casdoor.com/login</a>
app-casnode	<a href="https://door.casdoor.com/signup/app-casnode">https://door.casdoor.com/signup/app-casnode</a>	<a href="https://door.casdoor.com/login/oauth/authorize?client_id=014ae4bd048734ca2dea&amp;response_type=code&amp;redirect_uri=http://localhost:9000/callback&amp;scope=read&amp;state=casdoor">https://door.casdoor.com/login/oauth/authorize?client_id=014ae4bd048734ca2dea&amp;response_type=code&amp;redirect_uri=http://localhost:9000/callback&amp;scope=read&amp;state=casdoor</a>
app-casbin-oa	<a href="https://door.casdoor.com/signup/app-casbin-oa">https://door.casdoor.com/signup/app-casbin-oa</a>	<a href="https://door.casdoor.com/login/oauth/authorize?client_id=0ba528121ea87b3eb54d&amp;response_type=code&amp;redirect_uri=http://localhost:9000/callback&amp;scope=read&amp;state=casdoor">https://door.casdoor.com/login/oauth/authorize?client_id=0ba528121ea87b3eb54d&amp;response_type=code&amp;redirect_uri=http://localhost:9000/callback&amp;scope=read&amp;state=casdoor</a>

## Login URLs

It's very easy to log into Casdoor via Casdoor's built-in application, just visit Casdoor server's homepage (like: <https://door.casdoor.com> for demo site) and it will automatically redirect you to `/login`. But how to get these URLs for other applications in frontend and backend code? You can either concatenate strings by yourself or call some utility functions provided by Casdoor SDKs to get the URLs:

### 1. By concatenating string manually:

- Sign up page URL
  - Signup for the specified application: `<your-casdoor-hostname>/signup/<your-application-name>`
  - Signup by oauth: `<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`
  - Signup automatically: `<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`
- Sign in page URL
  - Signin for the specified organization: `<your-casdoor-hostname>/login/<your-organization-name>`
  - Signin by oauth: `<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. Use frontend SDK (for frontend Javascript code using React, Vue or Angular):

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

### 3. Use backend SDK (for backend code using Go, Java, etc.):

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

## Provider

Casdoor is a federated single-sign-on system, which supports multiple identity providers via OIDC, OAuth and SAML. Casdoor can also send verification code or other notifications to users via Email or SMS (Short Message Service). Casdoor uses the concept: `Provider` to manage all these third-party connectors.

Currently, All providers supported by Casdoor can be found here: [provider/overview](#)

```
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"
```

## How does Casdoor manage itself?

When you run Casdoor for the first time, Casdoor will create some built-in objects to help the administrator to manage Casdoor itself:

- A built-in organization named `built-in`.
- A user named `admin` in the `built-in` organization.
- A built-in application named `app-built-in`, owned by the `built-in` organization, representing Casdoor itself (Casdoor is actually also an application).

All the users under `built-in` organization, including `admin` will have the full administrator power on the Casdoor platform by default. So if you have multiple administrators, then create new accounts under `built-in` organization. Otherwise, remember to close the sign up channel for the `app-built-in` application.

 CAUTION

The built-in objects are already forbidden to rename or delete in both web UI or RESTful API. Casdoor has hard-coded these reserved names in many places. Do not try to rename or delete them in any way like modifying the DB, otherwise the whole system may crash.

# Server Installation

## Requirements

### OS

All major operating systems including Windows, Linux and macOS are supported.

### Environment

- Go 1.17+
- Node.js LTS (16 or 14)
- Yarn 1.x

 INFO

We strongly suggest you use [Yarn 1.x](#) to run & build Casdoor frontend, using NPM might cause UI styling issues, see more details at: [casdoor#294](#)

 CAUTION

For Chinese users, in order to download the Go dependency packages successfully, you need to use a Go proxy by Configuring the GOPROXY environment variable. We strongly recommend: <https://goproxy.cn/>

## Database

Casdoor uses [XORM](#) to talk to the database. Based on [Xorm Drivers Support](#),

Casdoor currently provides support for following databases:

- MySQL
- MariaDB
- PostgreSQL
- CockroachDB
- SQL Server
- Oracle
- SQLite 3
- TiDB

## Download

The source code of Casdoor is hosted at GitHub: <https://github.com/casdoor/casdoor>. Both the Go backend code and React frontend code are inside the single repository.

Name	Description	Language	Source code
Frontend	Web frontend UI for Casdoor	JavaScript + React	<a href="https://github.com/casdoor/casdoor/tree/master/web">https://github.com/casdoor/casdoor/tree/master/web</a>
Backend	RESTful API backend for Casdoor	Golang + Beego + XORM	<a href="https://github.com/casdoor/casdoor">https://github.com/casdoor/casdoor</a>

Casdoor supports [Go Modules](#). To download the code, you can just simply clone the code via git:

```
cd path/to/folder  
git clone https://github.com/casdoor/casdoor
```

# Configuration

## Configure Database

Casdoor supports mysql, mssql, sqlite3, postgres. Casdoor uses mysql by default. If you use another database, please modify the import package in [object/adapter](#).

### MySQL:

Casdoor will store its users, nodes and topics information in a MySQL database named: `casdoor`. If the database does not exist, it needs to be created manually. The DB connection string can be specified at: <https://github.com/casdoor/casdoor/blob/master/conf/app.conf>

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

### PostgreSQL:

Since we must choose a database when opening Postgres with xorm, you should prepare a database manually before running Casdoor.

Let's assume that you have already prepared a database called `casdoor`, then you should specify `app.conf` like this:

```
driverName = postgres
```

### INFO

For PostgreSQL, make sure `dataSourceName` has non-empty `dbName` and leave the standalone `dbName` field empty like the above example.

## CockroachDB:

You can also use `cockroachdb` with `postgres` driver. It has same configuration as `postgreSQL`.

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

### INFO

For CockroachDB, don't forget to add `serial_normalization=virtual_sequence` to the `dataSourceName` like the above example. otherwise you will get error regarding existed database, whenever the service started or restarted. Notice, this must be added before the database created.

## Sqlite3

You should specify `app.conf` like this:

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

## Via Ini file

Casdoor can be configured via a single file: [conf/app.conf](#), the content of which by default is:

```
appname = casdoor
httpport = 8000
runmode = dev
SessionOn = true
copyRequestBody = true
driverName = mysql
dataSourceName = root:123456@tcp(localhost:3306)-
dbName = casdoor
tableNamePrefix =
showSql = false
redisEndpoint =
defaultStorageProvider =
isCloudIntranet = false
authState = "casdoor"
socks5Proxy = "127.0.0.1:10808"
verificationCodeTimeout = 10
initScore = 2000
logPostOnly = true
origin = "https://door.casdoor.com"
staticBaseUrl = "https://cdn.casbin.org"
enableGzip = true
```

- `appname` is the application name, which currently has no practical use
- `httpport` is the port that your back-end application is listening on
- `runmode` is `dev` or `prod`
- `SessionOn` decides whether to enable session, used by default.
- `driverName`, `dataSourceName` and `dbName` are introduced before, please see [Configure Database](#).

- `verificationCodeTimeout` set the expiration time of the verification code.  
After the expiration, the user needs to obtain it again

Despite all the configurable fields, as a beginner, you only need to modify two items: `driverName` and `dataSourceName` based on your database. This database will be used by Casdoor to store all data, including users, organizations, applications and so on.

- `tableNamePrefix` is prefix of the table when using adapter.
- `showSql` : show SQL statement or not on logger if log level is great than INFO.
- `redisEndpoint` is the Redis endpoint used by Beego session storage. If this parameter is empty, the session data will be stored locally as files in `./tmp` folder. For using Redis as Beego session storage, an example for this value would be: `redis.example.com:6379`. If Redis is deployed in the local machine, you can use `localhost:6379`. If Redis password is enabled, use `redis.example.com:6379, db, password`. See more details at: <https://beego.run/docs/module/session.md#saving-provider-config>
- `defaultStorageProvider` is the default file storage service name. If you need to use file storage services such as avatar upload, you need to set up a storage provider and apply it in your application. See [storage](#) for details.
- `isCloudIntranet` is used to identify whether your provider endpoint is intranet endpoint.
- `authState` is the authorization application name. This parameter will be checked when logging in.
- `socks5Proxy` is the SOCKS proxy server IP address. Set the proxy port, because we have google-related services or use `Google` `GitHub` `Facebook` `LinkedIn` `Steam` as OAuth Provider which will be restricted by the network in some areas.
- `initScore` is the initial score of each user. Each user has a score attribute. Score is used by [Casnode](#). Score does not control anything in Casdoor.

- `logPostOnly` is used to identify whether only use post method to add a record.
- `origin` is the origin backend domain name.
- `staticBaseUrl` is address of the static image when the system initializes the database.
- `enableGzip` will accept and response with gzip encoding when the request header including `Accept-Encoding=gzip`.

## Via Environment Variables

All configuration items defined by Casdoor in the ini file mentioned above can be chosen to configuration via environmental variables, so can some of the beego configurations items(`httpport,appname`).

For example, when you try to start casdoor, you can use something like this to pass the configuration via environmental variables.

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

Besides, `export` derivatives are also a possible method. The names of environmental variables should be exactly the same with the names you want to use in the ini file.

*Note: configurations in environmental variables can override the configurations in ini file.*

## Run

There are currently two methods to start, you can choose one according to your own situation.

# Development mode

## Backend

Casdoor's Go backend runs at port 8000 by default. You can start the Go backend with the following command:

```
go run main.go
```

After the server is successfully running, we can start the frontend part.

## Frontend

Casdoor's frontend is a very classic [Create-React-App \(CRA\)](#) project. It runs at port `7001` by default. Use the following commands to run the frontend:

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

Visit: <http://localhost:7001> in your browser. Log into Casdoor dashboard with the default global admin account: `built-in/admin`

```
admin
123
```

# Production mode

## Backend

Build Casdoor Go backend code into executable and start it.

For Linux:

```
go build  
./casdoor
```

For Windows:

```
go build  
casdoor.exe
```

## Frontend

Build Casdoor frontend code into static resources (.html, .js, .css files):

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

Visit: <http://localhost:8000> in your browser. Log into Casdoor dashboard with the default global admin account: `built-in/admin`

```
admin  
123
```

## TIP

To use another port, please edit `conf/app.conf` and modify `httpport`, then restart the Go backend.

## CASDOOR PORT DETAILS

In dev environment, the frontend is run by `yarn run` in port 7001, so if you want to go to Casdoor login page, you need set Casdoor link as `http://localhost:7001`.

In prod environment, the frontend files is first built by `yarn build` and served in port 8000, so if you want to go to Casdoor login page, you need to set Casdoor link as `http://SERVER_IP:8000` (If you are using reverse proxy, you need to set the link as your domain).

Take our official forum Casnode as an example:

Casnode uses Casdoor to handle authentication.

When we are testing Casnode in dev environment, we set the `serverUrl` as `http://localhost:7001`, so when we test signin and signup functionality using Casdoor, it will go to localhost 7001 which is the Casdoor port.

And when we put Casnode to prod environment, we set the `serverUrl` as `https://door.casdoor.com`, so users can signin or signup using Casdoor.

```
|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",
|10 }
```

# (Optional) Try with Docker

## Requirements

### Hardware

If you want to build the Docker image by yourself, please ensure that your machine has at least 2GB memory. Casdoor's frontend is a NPM project of React. Building the frontend requires at least 2GB memory. Less than 2GB memory may lead to frontend build failure.

If you just need to run the pre-built image, please ensure that your machine has at least 100MB memory.

### OS

All OSes (Linux, Windows and macOS) are supported.

### Docker

You can use docker (docker-engine version  $\geq$  17.05) in Linux or Docker Desktop in Windows and macOS.

- [Docker](#)

Users of all OSes must ensure that the docker-engine version  $\geq$  17.05. It is because we use multi-stage build feature in docker-compose.yml, which was supported in 17.05 and above versions. See <https://docs.docker.com/develop/develop-images/multistage-build/> for more information.

If you also use docker-compose, please ensure that docker-compose version >= 2.2. For Linux users, you also need to make sure that docker-compose is installed, given that it is separated from docker-engine.

## Get the image

We have provided two DockerHub images:

Name	Description	Suggestion
casdoor-all-in-one	Both Casdoor and a MySQL database are inside the image	Already includes a toy database and only for test purpose
casdoor	Only Casdoor is inside the image	Can be connected to your own database and used in production

1. casbin/casdoor-all-in-one, in which casdoor binary, a mysql database and all necessary configurations are packed up. This image is for new users to have a trial on casdoor quickly. With this image you can start a casdoor immediately with one single command (or two) without any complex configuration. Note: we DO NOT recommend you to use this image in productive environment

### Option-1: Use the toy database

Run the container with port 8000 exposed to host. It will automatically pull the image if it doesn't exist in the local host.

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

### **⚠ CAUTION**

Some users in areas like China usually use Docker image mirror services like [Alibaba Cloud Image Booster \(English\)](#) to achieve higher download speed compared to DockerHub. However, it has a known issue that the `latest` tag provided by those services is not up-to-date. It probably results in a very old image by fetching the `latest` tag. To mitigate this issue, you can specify the image version number explicitly by using the following command:

```
docker pull casbin/casdoor-all-in-one:$(`curl -ss "https://hub.docker.com/v2/repositories/casbin/casdoor-all-in-one/tags/?page_size=1&page=2" | sed 's/,/,\\n/g' | grep '"name"' | awk -F '"' '{print $4}')`
```

Note: the above command utilizes Linux tools like `curl`, `sed`, `grep`, `awk`. If you are using Windows, make sure you run it in a Linux-style shell like `Git Shell` or `Cygwin`. `CMD` or `PowerShell` won't work.

Visit: <http://localhost:8000> in your browser. Log into Casdoor dashboard with the default global admin account: `built-in/admin`

```
admin  
123
```

## Option-2: Try with docker-compose

### **⚠ CAUTION**

Some users in areas like China usually use Docker image mirror services

like [Alibaba Cloud Image Booster \(English\)](#) to achieve higher download speed compared to DockerHub. However, it has a known issue that the `latest` tag provided by those services is not up-to-date. It probably results in a very old image by fetching the `latest` tag. To mitigate this issue, you can specify the image version number explicitly by using the following command:

```
docker pull casbin/casdoor:$(curl -sS  
"https://hub.docker.com/v2/repositories/casbin/casdoor/  
tags/?page_size=1&page=2" | sed 's/,/,\\n/g' | grep '"name"'  
| awk -F '"' '{print $4}' )
```

Note: the above command utilizes Linux tools like `curl`, `sed`, `grep`, `awk`. If you are using Windows, make sure you run it in a Linux-style shell like `Git Shell` or `Cygwin`. `CMD` or `PowerShell` won't work.

Create a `conf/app.conf` directory in the same level directory of the `docker-compose.yml` file, then copy `app.conf` from Casdoor. For more details about `app.conf`, you can see [Via Ini file](#).

Create a separate database by docker-compose:

```
docker-compose up
```

That's it! ✨

Visit: <http://localhost:8000> in your browser. Log into Casdoor dashboard with the default global admin account: `built-in/admin`

admin

*Note: if you dive deeper into the docker-compose.yml, you may be puzzled by the environment variable we created in it called "RUNNING\_IN\_DOCKER". When database 'db' is created via docker-compose, it is available on localhost of your pc but not localhost of the casdoor container. To prevent you from the troubles caused by modifying app.conf which are pretty difficult for a new user, we provided this environment variable and pre-assigned it in docker-compose.yml. When this environment variable is true, localhost will be replaced with host.docker.internal so that you casdoor can visit the db.*

## Option-3 Try directly with standard image

### CAUTION

Some users in areas like China usually use Docker image mirror services like [Alibaba Cloud Image Booster \(English\)](#) to achieve higher download speed compared to DockerHub. However, it has a known issue that the `latest` tag provided by those services is not up-to-date. It probably results in a very old image by fetching the `latest` tag. To mitigate this issue, you can specify the image version number explicitly by using the following command:

```
docker pull casbin/casdoor:$(curl -sS "https://hub.docker.com/v2/repositories/casbin/casdoor/tags/?page_size=1&page=2" | sed 's/,/,\\n/g' | grep '"name"' | awk -F '"' '{print $4}')
```

Note: the above command utilizes Linux tools like `curl`, `sed`, `grep`, `awk`. If you are using Windows, make sure you run it in a Linux-style shell like `Git Shell` or `Cygwin`. `CMD` or `PowerShell` won't work.



if it is not convenient to mount the configuration file to a container, using environment variables is also a possible solution.

#### example

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

Create `conf/app.conf`, you can copy it from `conf/app.conf` in Casdoor. For more details about `app.conf`, you can see [Via Ini file](#).

Then run

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

Anyway just mount the app.conf to `/conf/app.conf` and start it.

Visit: <http://localhost:8000> in your browser. Log into Casdoor dashboard with the default global admin account: `built-in/admin`

```
admin  
123
```

# Casdoor Public API

Casdoor is developed in a frontend and backend separated manner (in contrast to JSP or PHP). The Go backend only exposes its functionality via RESTful API. The React frontend code consumes the RESTful API to render the web UI and perform actions. We call the RESTful API as `Casdoor Public API`. The API can usually be used by:

- Casdoor's frontend
- Casdoor client SDKs
- Any other customized code from the application side

The full reference of `Casdoor Public API` can be viewed at Swagger:  
<https://door.casdoor.com/swagger> . This Swagger docs are automatically generated by Beego's Bee tool.

# Tutorials

## Product documentation

Product	Technologies	Docs
Dashboard of PingCAP TiDB	React + Typescript + Go + Gin	<a href="#">Use Casdoor for TiDB Dashboard SSO sign-in</a> (other languages: <a href="#">Chinese</a> , <a href="#">Japanese</a> )
GitLab	Vue + Ruby + Rails	<a href="#">OpenID Connect OmniAuth provider</a>
Apache Shenyu	Java	<a href="#">Casdoor Plugin</a> (other languages: <a href="#">Chinese</a> )
Alist	Typescript + SoildJS + Go + Gin	<a href="#">Casdoor SSO</a> (other languages: <a href="#">Chinese</a> )
BookStack	jQuery + Bootstrap + Go + Beego	<a href="#">Casdoor integrates registration and login</a>

# Articles

Technologies	Language	Title
ASP.Net Core 6	English	ASP.Net Core .net 6 Demo Authentication Project using local Casdoor Docker Container on Windows Subsystem for Linux
OAuth2 Proxy (Go)	Chinese	Use Casdoor + OAuth-Proxy to protect web applications on public networks
Casnnode (Javascript + React + Go + Beego)	Chinese	Use Lighthouse to set up a forum like v2ex
Cloudreve (Go)	Chinese	Modify Cloudreve to support Casdoor
KodExplorer (PHP)	Chinese	Modify KodExplorer to support Casdoor



&gt;

Deployment

# Deployment



## Data Initialization

How to initialize Casdoor data from files



## Hosting Static Files in CDN

Hosting frontend static files in the CDN



## Hosting Static Files in Intranet

How to deploy Casdoor static resource



## DB Migration

Handle DB Migration in Casdoor

# Data Initialization

If you are deploying Casdoor with other services as a whole application, you may want to provide an **out-of-box** feature for users (User can directly use the application without any configuration).

For such a situation, you can use data initialization to register your service in Casdoor through one configuration file. This file can be pre-defined or dynamically generated by your owner service.

## How to use

If there is one configuration file named as `init_data.json` at the root directory of Casdoor, it will be used to initialize data in Casdoor. What you should do is just to put this file at the root directory where Casdoor will run.

If you use official docker image of Casdoor, the following are some scripts that can help you to mount `init_data.json` into the container.

## Docker

If you deploy Casdoor with docker, you can use the `volume` to mount `init_data.json` into the container.

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

# Kubernetes

If you deploy Casdoor with kubernetes, you can use the `configmap` to store `init_data.json`.

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

You can mount the data into Casdoor `pods` by mounting the `configmap`. You may modify your `deployment` as follows:

```
apiVersion: apps/v1
kind: Deployment
...
spec:
  template:
    ...
      spec:
        containers:
          ...
            volumeMounts:
              - mountPath: /init_data.json
                name: casdoor-init-data-volume
                subPath: init_data.json
        volumes:
          - configMap:
              name: casdoor-init-data
              name: casdoor-init-data-volume
```

# File details

There is already a template named `init_data.json.template` at the root directory of Casdoor repository. You can refer to this file to customize your initialization.

The following is the Go struct of each part mapping to and their documentation:

Object	Go Struct	Documentation
organizations	<a href="#">stuct</a>	<a href="#">doc</a>
applications	<a href="#">stuct</a>	<a href="#">doc</a>
users	<a href="#">stuct</a>	<a href="#">doc</a>
providers	<a href="#">stuct</a>	<a href="#">doc</a>
certs	<a href="#">stuct</a>	
Idaps	<a href="#">stuct</a>	<a href="#">doc</a>

If you still feel confused of filling this template, you can call restful api or use the debug mode of your browser to see the response of `GetXXX` to these objects. These response are in the same format as `init_data.json`.

# Hosting Static Files in CDN

Frontend static resource (.js, .css files) are in `web/build/static/`. If you want to deploy it in a CDN service of a public cloud, Casdoor provides a script for you to deploy frontend static files easily. Please follow the steps below.

 NOTE

We assume you have already built the frontend code of Casdoor. If not yet, please follow: [document](#).

## Preparation

First, you need to create a valid [Storage Provider](#) in Casdoor UI. you can refer to the [example](#).

 CAUTION

When you fill in the field `Domain`, please end with '/'

Domain  :

`https://cdn.casbin.com/casdoor/`

## Usage

The script is at [deployment/deploy\\_test.go](#).

In `deploy_test.go`, you need to modify the parameter `id` in `GetProvider()`. The format of provider `id` is `<owner>/<name>`

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

Then use the following commands to run the script:

```
cd deployment
go test
```

If the execution succeeds, you will see:

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

## How it works

The script will:

- It will upload all the files in folders: `css/` and `js/` to the CDN service pointed by the storage provider.
- Replace all the URLs of `.css` and `.js` files in the `web/build/index.html` with the URLs hosted in the CDN.

You still need to keep the `index.html`. After the static files are uploaded to CDN, `index.html` will still be requested by users through Casdoor Go backend, and those static files in the CDN are then requested through the URLs in `index.html`.



# Hosting Static Files in Intranet

If you are deploying Casdoor on an [Intranet](#), you may not be able to access the static resource directly over the Internet. You need to deploy static resources where you can access them, and then modify the configuration in Casdoor in 3 places.

## Deploy static resource

All static resources in Casdoor, including images, logo, css, etc., are stored in [casbin/static repository](#).

Clone the repository and deploy it on a web servers. Make sure you can access the resource.

## Modify in Casdoor

You can simply modify the configuration file to set the static resource address to where you deployed it. Go to [conf/app.conf](#), set `staticBaseUrl` to your deployed address.

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

# DB Migration

When the database is upgraded, it is easy to have a data crash, for example, we need to delete an old field. Fortunately, the [xorm](#) used by Casdoor will help us with a lot of database migration problems. But we still need to handle some schema and data migrations ourselves, such as a field name changed

 NOTE

You can understand xorm Schema operation in [xorm docs](#)

## How it works

As mentioned above, when a field name changes, xorm will not be able to do anything, but xorm provides a [migrate](#) package to help us solve this problem.

You can write code like this to handle field renaming:

```
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 {

```

What we want to achieve is: rename `p_type` to `ptype`. But since xorm does not support field renaming, we can only use a more complicated way: assign the value of `p_type` to `ptype`, and then delete the `p_type` field.

The `ID` field uniquely refers to the migration we performed. After the `m.Migrate()` runs, and the value of the `ID` will be added to the migrations table of the database.

When the project is started again, the database will check the existing `ID` field in the table and will not perform operations with the same `ID`.



> How to Connect to Casdoor

# How to Connect to Casdoor

## Overview

Connect your app to Casdoor

## Standard OIDC Client

Using OIDC discovery to migrate to Casdoor

## Casdoor SDKs

Using Casdoor SDKs instead of standard OIDC protocol

## How to Enable Single Sign-On

Enable Single Sign-On

## Vue SDK

Casdoor Vue SDK

## Desktop SDKs

3 items

## Casdoor Plugin

Using Casdoor plugins or middlewares in other frameworks like Spring Boot, WordPress, Odoo, etc.

## OAuth 2.0

Using AccessToken to authenticate clients

## CAS

Using Casdoor as CAS server



## SAML

3 items



## WebAuthn

Use WebAuthn in Casdoor

# Overview

In this section, we will show how to connect your application to Casdoor.

As Service Provider (SP), Casdoor supports two authentication protocols:

- OAuth 2.0 (OIDC)
- SAML

As Identity Provider (IdP), Casdoor supports 4 authentication protocols:

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

## OAuth 2.0 (OIDC)

What is OAuth 2.0?

OAuth 2 is an authorization framework that enables applications — such as Facebook, GitHub, and Casdoor — to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts a user account and authorizing third-party applications to access that user account. OAuth 2 provides authorization flows for web and desktop applications, as well as mobile devices.

Casdoor's authorization process is built upon the OAuth 2.0 protocol. We recommend using the OAuth 2.0 protocol:

1. The protocol is simple and easy to implement, and can solve many scenarios.
2. High maturity and extensive community support

Therefore, your application will talk to Casdoor via OAuth 2.0 (OIDC). Specifically, there are three ways for connecting to Casdoor:

## Standard OIDC client

**Standard OIDC client**: use a standard OIDC client implementation, which is usually widely provided in any programming language or framework.

What is OIDC?

OpenID Connect (OIDC) is an open authentication protocol that works on top of the OAuth 2.0 framework. Targeted toward consumers, OIDC allows individuals to use single sign-on (SSO) to access relying party sites using OpenID Providers (OPs), such as an email provider or social network, to authenticate their identities. It provides the application or service with information about the user, the context of their authentication, and access to their profile information.

Casdoor has fulfilled the OIDC protocol completely. If your application is already running against another OAuth 2.0 (OIDC) identity provider via a **standard OIDC client library**, and you want to migrate to Casdoor, using OIDC discovery will be very easy for you to switch to Casdoor.

## Casdoor SDKs

[Casdoor SDKs](#): For most programming languages, Casdoor will provide easy-to-use SDK library on top of OIDC, with supporting extended functionality which are only available in Casdoor.

Compared to the standard OIDC protocol, Casdoor provides more functionalities in its SDK, like user management, resource uploading, etc. Connecting to Casdoor via Casdoor SDK costs more time than using a standard OIDC client library but will provide the best flexibility and the most powerful API.

## Casdoor plugin

[Casdoor plugin](#): if your application is built on top of a popular platform (like Spring Boot, WordPress, etc.) and Casdoor (or a third-party) has already provided a plugin or middleware for it, then use it. It will be much easier to use a plugin than manually invoking Casdoor SDK because the former is specially made for the platform.

plugin:

- [Jenkins plugin](#)
- [APISIX plugin](#)

Middleware:

- [Spring Boot plugin](#)
- [Django plugin](#)

# SAML

## What is SAML?

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). What that jargon means is that you can use one set of credentials to log into many different websites. It's much simpler to manage one login per user than it is to manage separate logins to email, customer relationship management (CRM) software, Active Directory, etc.

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user's identity and the authorization to use a service.

Casdoor can be used as SAML IdP. Up to now the Casdoor has supported the main features of SAML 2.0. More details see [SAML](#).

Example:

[Casdoor as a SAML IdP in keycloak](#)

Suggestion:

1. The protocol is **powerful** and covers many scenarios, which can be said to be one of the most comprehensive SSO protocols.
2. The protocol is **too large**, and there are many optional parameters, so it is difficult to cover all application scenarios 100% in the actual implementation.
3. If the application is **newly developed**, SAML is **not recommended** because of

- ▶ its high technical complexity.

## CAS

### What is CAS?

The Central Authentication Service (CAS) is a single sign-on protocol for the web. Its purpose is to permit a user to access multiple applications while providing their credentials (such as user ID and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password.

Casdoor has implemented CAS 1.0, 2.0, 3.0 features. More details see [CAS](#).

### Suggestion:

1. The protocol itself is relatively lightweight and easy to implement, but it can solve a single scenario.
2. The mutual trust between the CAS Client and the CAS Server is established through interface invocation without any encryption or signature mechanism to ensure further security.
3. CAS protocol has no advantage over other protocols.

## Integrations table

Some applications already have examples that connect to Casdoor. You can follow the documentation to quickly connect to Casdoor. You can see all applications in [Integrations table](#).

# Standard OIDC Client

# OIDC discovery

Casdoor has fulfilled the OIDC protocol completely. If your application is already running against another OAuth 2.0 (OIDC) identity provider via a standard OIDC client library and you want to migrate to Casdoor, using OIDC discovery will be very easy for you to switch to Casdoor. Casdoor's OIDC discovery URL is:

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

E.g., the OIDC discovery URL for the demo site is: <https://door.casdoor.com/.well-known/openid-configuration>, with the following content:

# List of OIDC client libraries

Here we list a few OIDC client libraries for some languages like Go and Java:

OIDC client library	Language	Link
go-oidc	Go	<a href="https://github.com/coreos/go-oidc">https://github.com/coreos/go-oidc</a>
pac4j-oidc	Java	<a href="https://www.pac4j.org/docs/clients/openid-connect.html">https://www.pac4j.org/docs/clients/openid-connect.html</a>

The above table is far from being complete. For a full list of OIDC client libraries, please see more details at:

1. <https://oauth.net/code/>
2. <https://openid.net/>
  - i. Certified OpenID Connect Implementations
  - ii. Uncertified OpenID Connect Implementations

## OIDC UserInfo fields

The following table shows how OIDC UserInfo fields (via `/api/userinfo` API) are mapped from properties of Casdoor's User table:

Casdoor User Field	OIDC UserInfo Field
Id	sub
originBackend	iss
Aud	aud
Name	preferred_username
DisplayName	name
Email	email
Avatar	picture
Location	address
Phone	phone

See UserInfo's definition here: <https://github.com/casdoor/casdoor/blob/95ab2472ce84c479be43d6fc4db6533fc738b259/object/user.go#L175-L185>



# Casdoor SDKs

## Introduction

Compared to the standard OIDC protocol, Casdoor provides more functionalities in its SDK, like user management, resource uploading, etc. Connecting to Casdoor via Casdoor SDK costs more time than using a standard OIDC client library but will provide the best flexibility and the most powerful API.

Casdoor SDKs can be divided into two categories:

1. Frontend SDK: Like Javascript SDK, Vue SDK for websites, Android or iOS SDKs for Apps, etc. Casdoor supports providing authentication for both websites and mobile Apps.
2. Backend SDK: SDKs for backend languages like Go, Java, Node.js, Python, PHP, etc.

### TIP

If your website is developed in a frontend and backend separated manner, then you can use the Javascript SDK: [casdoor-js-sdk](#) or React SDK: [casdoor-react-sdk](#) or Vue SDK: [casdoor-vue-sdk](#) to integrate Casdoor in frontend. If your web application is a traditional website developed by JSP or PHP, you can just use the backend SDKs only. See an example: [casdoor-python-vue-sdk-example](#)

Frontend SDK	Description	SDK code	Example code
Javascript SDK	For websites	<a href="#">casdoor-js-sdk</a>	<a href="#">casdoor-raw-js-example</a> , <a href="#">Casnode</a> , <a href="#">Casbin-OA</a> , <a href="#">Confita</a>
Android SDK	For Android apps	<a href="#">casdoor-android-sdk</a>	<a href="#">casdoor-android-example</a>
iOS SDK	For iOS apps	<a href="#">casdoor-ios-sdk</a>	<a href="#">casdoor-ios-example</a>
Electron SDK	For Electron apps	<a href="#">casdoor-js-sdk</a>	<a href="#">casdoor-electron-example</a>
.NET Desktop SDK	For .NET desktop apps	<a href="#">casdoor-dotnet-sdk</a>	WPF: <a href="#">casdoor-dotnet-desktop-example</a> , WinForms: <a href="#">casdoor-dotnet-winform-example</a>
React SDK	For React websites	<a href="#">casdoor-react-sdk</a>	<a href="#">casdoor-nodejs-react-example</a> , <a href="#">casdoor-spring-security-react-example</a>
Vue SDK	For Vue websites	<a href="#">casdoor-vue-sdk</a>	<a href="#">casdoor-python-vue-sdk-example</a>
Angular SDK	For Angular 1.0, 2.0 websites	<a href="#">casdoor-angular-sdk</a>	
Flutter SDK	For Flutter apps	<a href="#">casdoor-flutter-sdk</a>	<a href="#">casdoor-flutter-example</a>
uni-app SDK	For uni-app apps	<a href="#">casdoor-uniapp-sdk</a>	<a href="#">casdoor-uniapp-example</a>

Next, use one of the following backend SDKs based on the language of your backend:

Backend SDK	Description	Sdk code	Example code
Go SDK	For Go backends	<a href="#">casdoor-go-sdk</a>	<a href="#">Casnode</a> , <a href="#">Casbin-OA</a> , <a href="#">Confita</a>
Java SDK	For Java backends	<a href="#">casdoor-java-sdk</a>	<a href="#">casdoor-spring-boot-starter</a> , <a href="#">casdoor-spring-boot-example</a> , <a href="#">casdoor-spring-security-react-example</a>
Node.js SDK	For Node.js backends	<a href="#">casdoor-nodejs-sdk</a>	<a href="#">casdoor-nodejs-react-example</a>
Python SDK	For Python backends	<a href="#">casdoor-python-sdk</a>	<a href="#">casdoor-python-vue-sdk-example</a> , <a href="#">casdoor-python-js-sdk-example</a> , <a href="#">casdoor-fastapi-js-sdk-example</a>
PHP SDK	For PHP backends	<a href="#">casdoor-php-sdk</a>	<a href="#">wordpress-casdoor-plugin</a>
.NET SDK	For ASP.NET backends	<a href="#">casdoor-dotnet-sdk</a>	<a href="#">casdoor-dotnet-sdk-example</a>
Rust SDK	For Rust backends	<a href="#">casdoor-rust-sdk</a>	<a href="#">casdoor-rust-example</a>
C/C++ SDK	For C/C++ backends	<a href="#">casdoor-cpp-sdk</a>	<a href="#">casdoor-cpp-qt-example</a>
Dart SDK	For Dart backends	<a href="#">casdoor-dart-sdk</a>	

For a full list of the official Casdoor SDKs, please see: <https://github.com/orgs/casdoor/repositories?q=sdk&type=all&language=&sort=>

## How to use Casdoor SDK?

### 1. Backend SDK configuration

When your application starts up, you need to initialize the Casdoor SDK config by calling the `InitConfig()` function with required parameters. Take `casdoor-go-sdk` as example: <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)
}
```

All the parameters for `InitConfig()` are explained as follows:

Parameter	Must	Description
endpoint	Yes	Casdoor Server URL, like <code>https://door.casdoor.com</code> or <code>http://localhost:8000</code>
clientId	Yes	Client ID for the Casdoor application
clientSecret	Yes	Client secret for the Casdoor application
jwtPublicKey	Yes	The public key for the Casdoor application's cert
organizationName	Yes	The name for the Casdoor organization
applicationName	No	The name for the Casdoor application

### TIP

The `jwtPublicKey` can be managed in the `Certs` page as below.

Name	Created time	Display name	Type	x509	RSA	4096	20	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>

You can find the public key in the cert edit page, copy it or download it for the sdk.

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

```
-----BEGIN CERTIFICATE-----
MIIEtTCCAuGgAwIBAgDAlEAMA0GCSqGSIb3DQEBCwUAMDAyHxHTAbBgNVBAoT
FENhc2Rvb3tgT3JnW5Spem0aW5uMRUwEwDVQDExwDYXNkb29yENlcnQvhfNCjEx
MDE1MDgxMTUyWhcNDNxExMDME1MDgxMTUyWjA2MR0wGwDVQQExRDYXNkb29yIE9y
Z2FuaxphdGlvbjEVMBMGa1UEAxEMQZg9vcibDZXJ0MjIjAnBqkgkIG9w0B
AQEEAOAcAgAAMIIICgKACgEA5npbSE1ym0f1RISDSE8IR7y+lw+RjJ74e5ejrq4b8zMY
k7HeHCYzRnhwEvNhXu1P0mbeQ5pp/QGo8vgEmAEATnmzl1NjOQCjCwUr
sO/fMn1C0j13x6mV1khZj5rksMhYY1vaxTEP3+VB8Hlgj3MHFWrb07uvFcMje
W8+0KerZCkTR8+9VBjaneBz/zQePFVh79bfZato/lUrPKOG9p1gOvwloC1A
3sHrHTP4Qm1QRt0hqZfbydSpwAqvNnaDfEf7mTsR5B6/wUjNCUBDPTSLVjC0
4WlISf6NkhoZ27kmbPsTj+bxHgsvRAgWtds9h62Kpjjs1Yn/Gau3qt4zo
KbiURyxQjXlvwcQsEftUk5ew5zuPfSDRLoLByQTlxoqjAFNWjW3/pzSDjgD
606fH1mvbZn45mjdyfhdC1kN7N-xtjnfalkweP2REv+RMcOf4xGuhrSnLsmk
mUDey29aBLs9j1YEQfMj2Eq+RVtUx+wB4y8K/D1bcy+fnfG5r8pwDpS262b
oq4RSv5i2Z7Lbw4ZxvOf1/IVLrtfjPoL1H0bnfr/AeZHjIKOVxrfz4y+h+jqzB
8wfDFPr9xY/RbsAF732309yijjEghnUrohnRgCpjkl/Mz2kt84k
-----BEGIN PRIVATE KEY-----
MIUKQBAAKCgAsInpbSE1ym0f1RISDSE8IR7y+lw+RjJ74e5ejrq4b8zMY
k7HeHCYzRnhwEvNhXu1P0mbeQ5pp/QGo8vgEmAEATnmzl1NjOQCjCwUr
sO/fMn1C0j13x6mV1khZj5rksMhYY1vaxTEP3+VB8Hlgj3MHFWrb07uvFcMje
W8+0KerZCkTR8+9VBjaneBz/zQePFVh79bfZato/lUrPKOG9p1gOvwloC1A
3sHrHTP4Qm1QRt0hqZfbydSpwAqvNnaDfEf7mTsR5B6/wUjNCUBDPTSLVjC0
4WlISf6NkhoZ27kmbPsTj+bxHgsvRAgWtds9h62Kpjjs1Yn/Gau3qt4zo
KbiURyxQjXlvwcQsEftUk5ew5zuPfSDRLoLByQTlxoqjAFNWjW3/pzSDjgD
606fH1mvbZn45mjdyfhdC1kN7N-xtjnfalkweP2REv+RMcOf4xGuhrSnLsmk
mUDey29aBLs9j1YEQfMj2Eq+RVtUx+wB4y8K/D1bcy+fnfG5r8pwDpS262b
oq4RSv5i2Z7Lbw4ZxvOf1/IVLrtfjPoL1H0bnfr/AeZHjIKOVxrfz4y+h+jqzB
8wfDFPr9xY/RbsAF732309yijjEghnUrohnRgCpjkl/Mz2kt84k
-----END PRIVATE KEY-----
```

Save
Save & Exit

Then you can select the cert in the application edit page.

The screenshot shows the 'Edit Application' page in the Casdoor web interface. The 'Cert' field is highlighted with a red arrow, indicating it's the current focus. The 'Cert' dropdown menu lists three options: 'cert\_rjeegc', 'cert-built-in', and 'Redirect URL'.

## 2. Frontend configuration

First, install `casdoor-js-sdk` via NPM or Yarn:

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

Or:

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

Then define the following utility functions (better in a global JS file like `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?");
}
```

In the entrance file of your frontend code (like `index.js` or `app.js` in React), you need to initialize the `casdoor-javascript-sdk` by calling the `InitConfig()` function with required parameters. The first 4 parameters should use the same value as the Casdoor backend SDK. The last parameter `redirectPath` is relative path for the redirected URL, returned from Casdoor's login page.

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

xxx.initCasdoorSdk(config);
```

(Optional) Because we are using React as example, our `/callback` path is hitting the React route. We use the following React component to receive the `/callback` call and send to the backend. You can ignore this step if you are redirecting to backend directly (like in JSP or PHP).

```
import React from "react";
import {Button, Result, Spin} from "antd";
import {withRouter} from "react-router-dom";
import * as Setting from "./Setting";

class AuthCallback extends React.Component {
  constructor(props) {
    super(props);
    this.state = {
      classes: props,
      msg: null,
    };
  }

  componentWillMount() {
    this.login();
  }

  login() {
    Setting.signin().then((res) => {
      if (res.status === "ok") {
        Setting.showMessage("success", `Logged in successfully`);
        Setting.goToLink("/");
      } else {
        this.setState({
          msg: res.msg,
        });
      }
    });
  }

  render() {
    return (
      <div style={{textAlign: "center"}>
        {this.state.msg === null ? (
          <Spin
            size="large"
            tip="Signing in..."
            style={{paddingTop: "10%"}}
          />
        ) : (
          <div style={{display: "inline"}>
            <Result
              status="error"
              title="Login Error"
              subTitle={this.state.msg}
              extra={[
                <Button type="primary" key="details">
```

### 3. Get login URLs

Next you can show the "Sign up" and "Sign in" buttons or links to your users. The URLs can either be retrieved in the frontend or backend. See more details at: [/docs/basic/core-concepts#login-urls](#)

### 4. Get and verify access token

Here are the steps:

1. The user clicks the login URL and is redirected to Casdoor's login page, like: `https://door.casdoor.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. The user enters username & password and clicks `Sign In` (or just click the third-party login button like `Sign in with GitHub`).
3. The user is redirected back to your application with the authorization code issued by Casdoor ( like: `https://forum.casbin.com?code=xxx&state=yyy`), your application's backend needs to exchange the authorization code with the access token and verify that the access token is valid and issued by Casdoor. The functions `GetOAuthToken()` and `ParseJwtToken()` are provided by Casdoor backend SDK.

The following code shows how to get and verify the access token. For a real example of Casnode (a forum website written in Go), see: [https://github.com/casbin/casnode/blob/6d4c55f5c9a3c4bd8c85f2493abad3553b9c7ac0/controllers/account.go#L51-L64](#)

```
// get code and state from the GET parameters of the redirected URL
code := c.Input().Get("code")
state := c.Input().Get("state")

// exchange the access token with code and state
token, err := auth.GetOAuthToken(code, state)
if err != nil {
    panic(err)
}

// verify the access token
claims, err := auth.ParseJwtToken(token.AccessToken)
if err != nil {
    panic(err)
}
```

If `ParseJwtToken()` finishes with no error, then the user has successfully logged into the application. The returned `claims` can be used to identify the user later.

### 4. Identify user with access token



#### INFO

This part is actually your application's own business logic and not part of OIDC, OAuth or Casdoor. We just provide good practices as a lot of people don't know what to do for the next step.

In Casdoor, access token is usually identical as ID token. They are the same thing. So the access token contains all information for the logged-in user.

The variable `claims` returned by `ParseJwtToken()` is defined as:

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

1. `User`: the User object, containing all information for the logged-in user, see definition at: [/docs/basic/core-concepts#user](#)
2. `AccessToken`: the access token string.
3. `jwt.RegisteredClaims`: some other values required by JWT.

At this moment, the application usually has two ways to remember the user session: `session` and `JWT`.

## Session

The Method to set session varies greatly depending on the language and web framework. E.g., Casnode uses [Beego web framework](#) and set session by calling: `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) // set session
```

## JWT

The `accessToken` returned by Casdoor is actually a JWT. So if your application uses JWT to keep user session, just use the access token directly for it:

1. Send the access token to frontend, save it in places like localStorage of the browser.
2. Let the browser send the access token to backend for every request.
3. Call `ParseJwtToken()` or your own function to verify the access token and get logged-in user information in your backend.

## 5. (Optional) Interact with the User table



### INFO

This part is provided by [Casdoor Public API](#) and not part of the OIDC or OAuth.

Casdoor Backend SDK provides a lot of helper functions, not limited to:

- `GetUser(name string)`: get a user by username.
- `GetUsers()`: get all users.
- `AddUser()`: add a user.
- `UpdateUser()`: update a user.
- `DeleteUser()`: delete a user.
- `CheckUserPassword(auth.User)`: check user's password.

These functions are implemented by making RESTful calls against [Casdoor Public API](#). If a function is not provided in Casdoor Backend SDK, you can make RESTful calls by yourself.



> How to Connect to Casdoor

> How to Enable Single Sign-On

# How to Enable Single Sign-On

## Introduction

You have connected Casdoor and configured more than one application in an organization. You want users to sign in once to any app in nomeguythe organization, and then be able to sign in when they go to another app, without any extra clicks.

We offer this single sign-on, you just need to:

- Enable Auto signin button.
- Fill in the URL for home page.
- Add a Silent Signin function to the application home page.

### NOTE

The basic sign in process provided by Casdoor allows users to log in to other applications in the organization by selecting the user who is currently logged in or using another account.

After enable the auto signin, the selection box will not display, the logged user will log in directly.

# Configure

1. Fill the field **home**. It can be the application's home page or the login page.

Screenshot of the Casdoor application configuration interface:

The top navigation bar includes: Casdoor logo, Home, Organizations, Users, Roles, Permissions, Models, Adapters, Providers, and Applications (which is highlighted).

The main form has the following fields:

- Edit Application (button)
- Save (button)
- Save & Exit (button)
- Name: app-casbin-oa
- Display name: Casbin OA
- Logo:
  - Preview: An owl logo with a shield containing a checkmark.
  - URL: https://cdn.casbin.org/img/casbin\_logo\_1024x256.png
- Home: https://oa.casbin.com (This field is highlighted with a red box.)
- Description: OA system for Casbin

2. Enable Auto signin button.

Password ON ? :

Enable signup ? :

Signin session ? :

Auto signin ? :   

Enable code signin ? :

Enable WebAuthn signin ? :

## Add Silent Signin

In fact, we implement auto login by carrying parameters on the URL. So your applications need to have a method to trigger the login after jumping to the URL. We provide [casdoor-react-sdk](#) for you to quickly implement the feature. You can see details in [use-in-react](#).



### How it works

1. In the URL to the application home page, we will carry the `silentSignin` parameter.
2. In your HomePage to determine whether you need to log in

`silently`(automatically) by the parameter `silentSignin`. If `silentSignin` === 1, the function returns the `SilentSignin` component, it will help you initiate a login request. And since you have auto-login enabled, users will log in automatically without clicking.

## Add Popup Signin

`popup signin` will pop up a small window. After logging in to Casdoor in the child window, it will send authentication information to the main window and then close automatically. We implement it by carrying parameters on the URL.

### INFO

#### How to use

Use the method `popupSignin()` in sdk [casdoor-js-sdk](#) to quickly implement the feature. You can see a demo in [casdoor-nodejs-react-example](#).

#### How it works

1. In the URL to the application home page, we will carry the `popup` parameter.
2. When `popup=1` in login params, Casdoor will send `code` and `state` as a message to main window and finish get `token` in main window by SDK.

# Using SSO

The configuration is complete, below will show you how to use auto login.

## INFO

Make sure in your application can redirect to user's profile page. The API `getMyProfileUrl(account, returnUrl)` is provided in our SDK for each language.

Open the profile page and go to the "Home" page (`/` URL path). You will see the application list provided by the organization. It's notable that only users in organizations other than `built-in` can see the application list in the "Home" page. All the global administrators (aka in the `built-in` organization) cannot see it.



Click on a tile in the application list, it will jump to the homepage URL of that application with GET parameter: `?silentSignin=1` and automatically log into the application if the application has integrated with Casdoor SSO (so it will recognize

the `?silentSignin=1` parameter and perform silent login in the background).

# Vue SDK

Casdoor Vue SDK is designed for Vue2 and Vue3 which is very convenient to use.

The Vue SDK is based on casdoor-js-sdk, you can also use the casdoor-js-sdk directly which will be more customizable.

This plugin is still in development. If you have any questions and suggestions, please contact us at [issue](#)

We will show you the steps below.

if you still don't know how to use it after reading README.md, you can go to the example: [casdoor-python-vue-sdk-example](#) for more details.

The example' front-end is built with casdoor-vue-sdk, and the back-end is built with casdoor-python-sdk, you can see the source code in the example.

## Installation

```
# NPM  
npm i casdoor-vue-sdk  
  
# Yarn  
yarn add casdoor-vue-sdk
```

# Init SDK

Initialization requires 5 parameters, which are all string type:

Name (in order)	Must	Description
serverUrl	Yes	your Casdoor server URL
clientId	Yes	the Client ID of your Casdoor application
appName	Yes	the name of your Casdoor application
organizationName	Yes	the name of the Casdoor organization connected with your Casdoor application
redirectPath	No	the path of the redirect URL for your Casdoor application, will be <code>/callback</code> if not provided

install:

For Vue3:

```
// in main.js
import Casdoor from 'casdoor-vue-sdk'
const config = {
  serverUrl: "http://localhost:8000",
  clientId: "4262bea2b293539fe45e",
  organizationName: "casbin",
  appName: "app-casnnode",
  redirectPath: "/callback",
```

For Vue2:

```
// in main.js
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')
```

## example

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

## Auto Fix

If the `postinstall` hook doesn't get triggered or you have updated the Vue version, try to run the following command to resolve the redirecting.

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

More info about Vue version switch at: [vue-demi docs](#)



> How to Connect to Casdoor > Desktop SDKs

# Desktop SDKs



## Electron App

An Electron app example for Casdoor



## Dotnet Desktop App

An Dotnet desktop app example for Casdoor



## Qt Desktop App

An Qt desktop app example for Casdoor

# Electron App

An [Electron app example](#) for Casdoor.

## How to run example

### Initialization

You need to initialize 6 parameters, which are all string type:

Name	Description	Path
serverUrl	your Casdoor server URL	<code>src/App.js</code>
clientId	the Client ID of your Casdoor application	<code>src/App.js</code>
appName	the name of your Casdoor application	<code>src/App.js</code>
redirectPath	the path of the redirect URL for your Casdoor application, will be <code>/callback</code> if not provided	<code>src/App.js</code>
clientSecret	the Client Secret of your Casdoor application	<code>src/App.js</code>
casdoorServiceDomain	your Casdoor server URL	<code>public/electron.js</code>

If you don't set these parameters, this project will use the [Casdoor online demo](#) as the default Casdoor server and use the [Casnode](#) as the default Casdoor application.

### Available commands

In the project directory, you can run:

`npm run dev` or `yarn dev`

Builds the electron app and run this app.

`npm run make` or `yarn make`

Package and distribute your application. It will create the `out` folder where your package will be located:

```
// Example for macOS out/
└── 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
```

### Preview

After you run this electron application, a new window will be showed on your desktop.



If you click `Login with Casdoor` button, your default browser will be opened automatically and show the login page.



Made with ❤ by Casdoor

After you login successfully, your electron application will be opened and your user name will be showed on your application.



You can preview the whole process by the gif image below.



## How to integrate

### Set the custom protocol

Firstly, you need to set the custom protocol called `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);
}
```

This will help the browser to open your electron application and send the login info to the electron application.

### Open the login url by the browser

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

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

You can change the first 5 parameters.

## Listen to the open application event

After you login successfully in the browser, the browser will open your electron application. You need to listen to the open application event.

```
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);
            }
        }
    });
}
```

You can get the code from the browser, which is `casdoor_code` or `params.code`.

## Parse the code and get the user info

```
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;
```

Finally, you can parse the code and get the user info just by following the [OAuth docs page](#).

# Dotnet Desktop App

An [Dotnet desktop app example](#) for Casdoor.

## How to run example

### Prerequisites

[dotnet6 sdk](#)

[webview2 runtime](#) (It's already preinstalled in your windows generally)

### Initialization

The initialization requires 5 parameters, which are all string type:

Name	Description	File
Domain	Your Casdoor server host/domain	<a href="#">CasdoorVariables.cs</a>
ClientId	The Client ID of your Casdoor application	<a href="#">CasdoorVariables.cs</a>
AppName	The name of your Casdoor application	<a href="#">CasdoorVariables.cs</a>

Name	Description	File
CallbackUrl	The path of the callback URL for your Casdoor application, will be <code>casdoor://callback</code> if not provided	CasdoorVariables.cs
ClientSecret	The Client Secret of your Casdoor application	CasdoorVariables.cs

If you don't set these parameters, this project will use the [Casdoor online demo](#) as the default Casdoor server and use the [Casnode](#) as the default Casdoor application.

# Running

## Visual Studio

1. Open casdoor-dotnet-desktop-example.sln
2. Press Ctrl + F5 to start

## Command line

1. cd src/DesktopApp
2. dotnet run

# Preview

After you run this dotnet desktop application, a new window will be showed on

your desktop.



If you click `Casdoor Login` button, a login window will be showed on your



desktop.

After you login successfully, a user profile window will be showed on your desktop. It displays your user name.



You can preview the whole process by the gif image below.



# How to integrate

## Open the login window

```
var login = new Login();
// Trigger when login succeeded, you will receive auth code in
event handler
login.CodeReceived += Login_CodeReceived;
login.ShowDialog();
```

## Use auth code to get the user info

```
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",
```



# Qt Desktop App

A [Qt desktop app example](#) for Casdoor.

## How to run example

### Prerequisites

[Qt6 sdk](#)

[OpenSSL toolkit](#)

### Initialization

You need to initialize 7 parameters, which are all string type:

Name	Description	File
endpoint	Your Casdoor server host/domain	<a href="#">mainwindow.h</a>
client_id	The Client ID of your Casdoor application	<a href="#">mainwindow.h</a>
client_secret	The Client Secret of your Casdoor application	<a href="#">mainwindow.h</a>
certificate	The public key for the Casdoor application's cert	<a href="#">mainwindow.h</a>

Name	Description	File
org_name	The name of your Casdoor organization	mainwindow.h
app_name	The name of your Casdoor application	mainwindow.h
redirect_url	The path of the callback URL for your Casdoor application, will be <code>http://localhost:8080/callback</code> if not provided	mainwindow.h

If you don't set the parameter `endpoint`, this project will use the <http://localhost:8000> as the defult Casdoor server.

## Running

### Qt Creator

1. Open casdoor-cpp-qt-example.pro
2. Set the `INCLUDEPATH` of OpenSSL in casdoor-cpp-qt-example.pro
3. Press Ctrl + R to start

## Preview

After you run this Qt desktop application, a new window will be showed on your desktop.



If you click `Sign In` button, a login window will be showed on your desktop.



After you login successfully, a user profile window will be showed on your desktop, it dispaly your user information.



You can preview the whole process by the gif image below.



# How to integrate

## Open the login window

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

## Listen to the open application event

```
// 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()));
```

## Use auth code to get the user info

```
// Get token and parse it with the JWT library
std::string token = m_casdoor->GetOAuthToken(code.toStdString());
auto decoded = m_casdoor->ParseJwtToken(token);
```

# Casdoor Plugin

Casdoor also provides plugins or middlewares for some very popular platforms, like Java's SpringBoot, PHP's WordPress, Python's Odoo etc.

Casdoor plugin	Language	Source code
Spring Boot plugin	Java	<a href="https://github.com/casdoor/casdoor-spring-boot-starter">https://github.com/casdoor/casdoor-spring-boot-starter</a>
Spring Boot example	Java	<a href="https://github.com/casdoor/casdoor-spring-boot-example">https://github.com/casdoor/casdoor-spring-boot-example</a>
WordPress plugin	PHP	<a href="https://github.com/casdoor/wordpress-casdoor-plugin">https://github.com/casdoor/wordpress-casdoor-plugin</a>
Odoo plugin	Python	<a href="https://github.com/casdoor/odoo-casdoor-oauth">https://github.com/casdoor/odoo-casdoor-oauth</a>
Django plugin	Python	<a href="https://github.com/casdoor/django-casdoor-auth">https://github.com/casdoor/django-casdoor-auth</a>

For a full list of the official Casdoor plugins, please see: [Casdoor repositories](#).

# OAuth 2.0

## Introduction

Casdoor supports AccessToken to authenticate clients. In this section, we will show you how to get AccessToken, how to verify AccessToken and how to use AccessToken.

## How to get AccessToken

You have two ways to get the AccessToken: you can use the [Casdoor SDKs](#), for details please refer to the SDK documentation, here we will mainly show you how to use the API to get the AccessToken.

Casdoor supports four OAuth grant types: [Authorization Code Grant](#), [Implicit Grant](#), [Resource Owner Password Credentials Grant](#), and [Client Credentials Grant](#).

For security reasons, the Casdoor app has the authorization code mode turned on by default. If you need to use other modes, please go to the appropriate app to set it.

The screenshot shows a user interface for selecting OAuth grant types. On the left, there is a label 'Grant types (2)' followed by a dropdown menu with four options: 'Authorization Code', 'Password', 'Client Credentials', and 'Token'. The 'Token' option is currently selected, indicated by a blue background. To the right of the dropdown, there is a list of provider names: 'Authorization Code', 'Password', 'Client Credentials', 'Token', and 'ID Token'. The 'Token' provider name is also highlighted with a blue background, matching the selection in the dropdown.

## Authorization Code Grant

First redirect your users to:

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

## Available scopes

Name	Description
openid (no scope)	sub (user's id), iss (issuer) and aud (audience)
profile	user profile info, include name, displayName, avatar
email	user's email address
address	user's address
phone	user's phone number

### INFO

Your OAuth Application can request the scopes in the initial redirection. You can specify multiple scopes by separating them with a space using %20:

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

For more details, please see [OIDC standard](#)

After your user has authenticated with casdoor, casdoor will redirect him to:

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

Now that you have obtained the authorization code, make a POST request to:

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

in your backend application:

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

You will get the following response:

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

 NOTE

Casdoor also supports [PKCE](#) feature, when getting the authorization code, you can add two parameters to enable PKCE:

```
&code_challenge_method=S256&code_challenge=YOUR_CHALLENGE
```

When getting the token you need to pass `code_verifier` parameter to verify PKCE. It is worth mentioning that with PKCE enabled, Client\_Secret is not required, but if you pass it, it must be the correct value.

## Implicit Grant

Maybe your application doesn't have a backend, and you need to use Implicit Grant. First you need to make sure you have Implicit Grant enabled, then redirect your users to:

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

After your user has authenticated with casdoor, casdoor will redirect him to:

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

Casdoor also supports `id_token` as `response_type`, which is a feature of OpenID.

## Resource Owner Password Credentials Grant

If your application doesn't have a frontend that redirects users to Casdoor, then you may need this.

First you need to make sure you have Password Credentials Grant enabled, and send a POST request to:

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

```
{  
    "grant_type": "password",  
    "client_id": ClientId,
```

You will get the following response:

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

## Client Credentials Grant

You can also use Client Credentials Grant when your application does not have a frontend.

First you need to make sure you have Client Credentials Grant enabled, and send a POST request to

[https://<CASDOOR\\_HOST>/api/login/oauth/access\\_token](https://<CASDOOR_HOST>/api/login/oauth/access_token):

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

You will get the following response:

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

It is important to note that the AccessToken obtained in this way differs from the first three in that it corresponds to the application rather than to the user.

## RefreshToken

Maybe you want to update your accessToken, then you can use the `refreshToken` you got above.

First you need to set the expiration time of refreshToken in the application (default is 0 hours), and send a POST request to [https://<CASDOOR\\_HOST>/api/login/oauth/refresh\\_token](https://<CASDOOR_HOST>/api/login/oauth/refresh_token)

```
{  
    "grant_type": "refresh_token",  
    "refresh_token": REFRESH_TOKEN,
```

You will get the response like:

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

## How to verify AccessToken

Casdoor currently has support for [token introspection](#) endpoint. Currently the endpoint is protected by Basic Authoritarian(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
```

You will get the following response like:

```
{  
    "active": true,  
    "client_id": "c58c... ",  
    "username": "admin",  
    "token_type": "Bearer",  
    "exp": 1647138242,  
    "iat": 1646533442,  
    "nbf": 1646533442,  
    "sub": "7a6b4a8a-b731-48da-bc44-36ae27338817",  
    "aud": [  
        "c58c... "  
    ],  
    "iss": "http://localhost:8000"  
}
```

## How to use AccessToken

You can use AccessToken to access Casdoor APIs that require authentication.

For example, two different ways to request [/api/userinfo](#).

Type 1. Query parameter

```
https://<CASDOOR\_HOST>/api/userinfo?accessToken=<your\_access\_token>
```

Type 2. HTTP Bearer token

```
https://<CASDOOR\_HOST>/api/userinfo with the header: "Authorization: Bearer <your_access_token>"
```

Casdoor will parse the access\_token, returning corresponding user information according to the scope. You will get the same response like:

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

If you expect more user's information, adding scope when getting AccessToken in step [Authorization Code Grant](#).

## Differences between `userinfo` and `get-account` APIs

- `/api/userinfo`: returns user information as part of OIDC protocol. Less information is returned, including only the basic information in OIDC standards. Please see [available scopes](#) that Casdoor supports.
- `/api/get-account`: gets the user object for the currently logged-in account. It is a Casdoor-only API to obtain all information of the `user` in Casdoor.

# CAS

## Using Casdoor as CAS server

Casdoor now can be used as CAS server. Up to now the casdoor has supported the feature of CAS3.0 .

### Overview

The prefix of CAS endpoint in Casdoor is `<Endpoint of casdoor>/cas/<organization name>/<application name>`, which means:

Suppose the endpoint of Casdoor is `https://door.casdoor.com`, which contains an application called `cas-java-app` which belongs to an organization called `casbin`, and if we are trying to let user login in via CAS, then

- `/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`

See <https://apereo.github.io/cas/6.6.x/protocol/CAS-Protocol-Specification.html> for more information about CAS and its different versions, as well as parameters for these endpoints.

### An example

Here is an offical example <https://github.com/apereo/cas-sample-java-webapp>, which contains an example web app utilizing the offical CAS java client <https://github.com/apereo/java-cas-client>. By going through this example, we will illustrate how to connect to Casdoor via CAS.

 NOTE

Note: Currently Casdoor only support all three versions of CAS: CAS 1.0 & 2.0 & CAS 3.0 .

The cas configuration is located in `src/main/webapp/WEB-INF/web.yml`.

By default, this app uses CAS 3.0, which is specified by the following configurations.

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

Suppose you want to protect this web app via CAS 2.0, you are supposed to change CAS Validation Filter to the following content.

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

If you want to use CAS 1.0, use

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

For all the appearances of parameter 'casServerUrlPrefix', change them to

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

For all the appearances of parameter 'casServerLoginUrl' change them to

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

If you need to customize more configurations, see <https://github.com/apereo/java-cas-client> for detailed information.

 NOTE

Actually, we have already have this demo app run on <https://cas-java-app.casdoor.com>. You can visit here to experience using Casdoor via CAS.



> How to Connect to Casdoor

> SAML

# SAML



## Overview

Using Casdoor as SAML IdP



## Keycloak

Using Casdoor as SAML IdP



## Appgate (POST)

How to use Casdoor as SAML IdP for Appgate

# Overview

Casdoor now can be used as SAML IdP. Up to now the Casdoor has supported the main feature of SAML 2.0 .

## Configuration in SP

Generally, SP needs the Single Sign-On, Issuer and Public Certificate three required fields. Most of the SP can get these fields by uploading the XML Metadata file or the XML Metadata URL to autocomplete.

The metadata of SAML endpoint in Casdoor is <Endpoint of casdoor>/api/saml/metadata?application=admin/<application name>. Suppose the endpoint of Casdoor is https://door.casdoor.com, which contains an application called app-built-in. The XML Metadata endpoint will be:

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

And you can also find the metadata in the application edit page. Click the button to copy the URL and paste it in browser to download the XML Metadata.

```
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.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+TCCAUgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENhc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDIxNrb2...
                </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-built-in"></SingleSignOnService>

```

[Copy SAML metadata URL](#)

# Configuration in Casdoor IdP

Casdoor supports both GET and POST `SAMLResponse`. Casdoor need to know what types of request the SP supports, when Casdoor sends the `SAMLResponse` to SP. You need to configure the application in casdoor based on the `SAMLResponse` type supported by your SP.

## INFO

If you fill the `Reply URL`, Casdoor will send the `SAMLResponse` by POST Request. If the Reply URL is empty, Casdoor will use GET request. You might wonder how casdoor knows the `Reply URL` of the SP, if the `Reply URL` is empty. Actually, Casdoor can get the URL called `AssertionConsumerServiceURL` by parsing the `SAMLRequest`. And send the request with `SAMLResponse` to `AssertionConsumerServiceURL`.

The `Reply URL` will overwrites the `AssertionConsumerServiceURL` in `SAMLRequest`.

- Reply URL Type in the URL of the ACS verifying the SAML response.

The screenshot shows the Casdoor configuration interface for a specific application. At the top, under 'Grant types', 'Authorization Code' and 'Password' are selected. Below that, the 'SAML Reply URL' field contains the value `https://mycontroller.mycompany.com/admin/saml`, which is highlighted with a red box. To the left of this field is a question mark icon. Further down, there is a toggle switch labeled 'Enable SAML' and another question mark icon. The entire configuration section is enclosed in a light blue border.

Grant types : Authorization Code × Password ×

SAML Reply URL : `https://mycontroller.mycompany.com/admin/saml`

Enable SAML compress :

- Redirect URL Type in a unique name. This may be called `Audience` or `Entity`

ID in your SP. Make sure you fill the same Redirect URL here as in your SP.

Redirect URLs :

Redirect URLs Add

Redirect URL

- appgate
- https://git.casbin.com/user/oauth2/casdoor/callback
- http://localhost:3000/callback

## User profile

After logged in successfully, the user profile in the SAMLResponse Casdoor returned has three fields. The attributes in the xml and the attributes of the user in casdoor are mapped as follows:

XML Attribute Name	User field
Email	email
DisplayName	displayName
Name	name

See [https://en.wikipedia.org/wiki/SAML\\_2.0](https://en.wikipedia.org/wiki/SAML_2.0) for more information about SAML and its different versions.

## An example

The [gosaml2](#) is a SAML 2.0 implementation for Service Providers based on etree

and goxmldsig, a pure Go implementation of XML digital signatures. And we use this library to test the SAML 2.0 in Casdoor as below.

Suppose you can access Casdoor through `http://localhost:7001/`, and your Casdoor contains an application called `app-built-in` which belongs to an organization called `built-in`. The URLs, `http://localhost:6900/acs/example` and `http://localhost:6900/saml/acs/example`, should be added to the Redirect URLs in `app-built-in`.

```
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)
    }
}
```

Run the above codes and the console will display the following message.

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](http://localhost:6900/v1/_saml_callback)

Click the URL to authenticate, the login page of Casdoor will display.



You will get the response messages as below after authenticating.









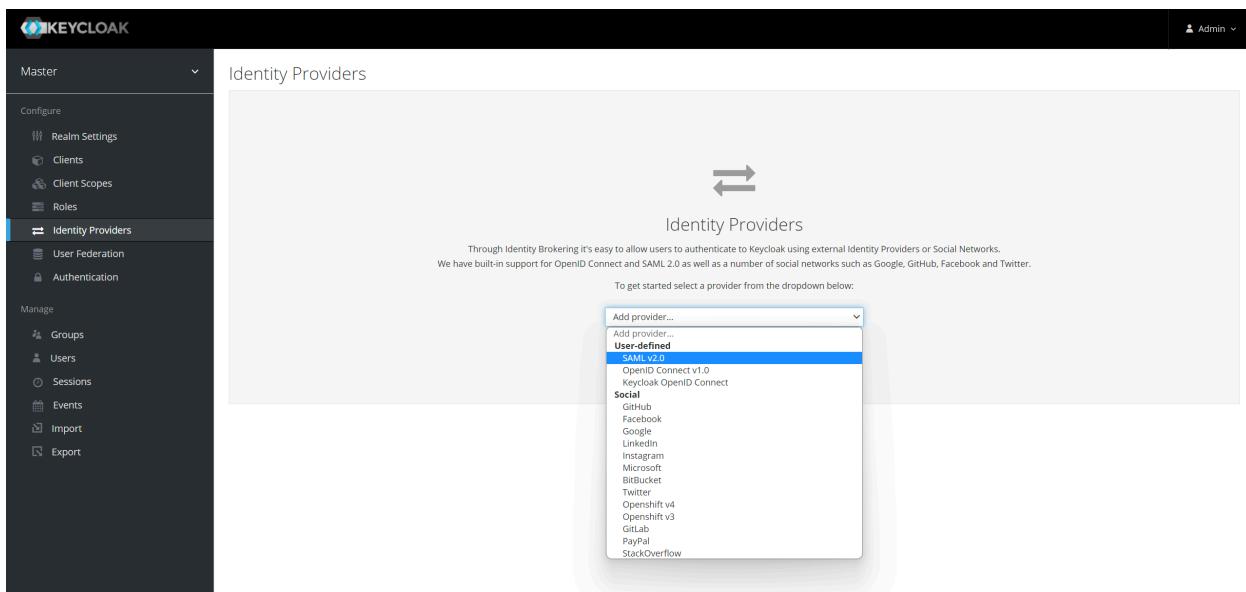
# Keycloak

## Casdoor as a SAML IdP in keycloak

This guide will show you how to configure Casdoor and Keycloak to add Casdoor as a SAML IdP in Keycloak.

### Add SAML IdP in Keycloak

Open Keycloak admin page, click **Identity Providers** and select **SAML v2.0** from the list of providers.



#### INFO

You can visit Keycloak SAML Identity Providers [documentation](#) to get more detailed information.

Enter the Alias and the Import from URL in Keycloak IdP edit page. The content of Import from URL can be found in the Casdoor application edit page. Click Import and the SAML config will be filled automatically.

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

You should remember the Service Provider Entity ID and then save the configuration.

## Configure SAML application in Casdoor

In the application edit page, add a redirect URL which the content of it is Service Provider Entity ID in Keycloak. And you should enable SAML compress for Keycloak.

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="signing"><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">MIIE+TCCAwGAWIBAgIDAeJAMAOGCCqGSIB3DQEBCwIAMDYxHTAbBgNVBAoTFENhc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29jIElcnQWhicNMjExMDE1MDgxM...</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/app-built-in"></SingleSignOnService>

Copy SAML metadata URL

## Login using Casdoor SAML

Open the Keycloak login page and you can find the additional button that allows you to login to Keycloak using the Casdoor SAML provider.



Click on the button and you will be redirected to the Casdoor SAML provider for the authentication. After the successful authentication, you will be redirected back to Keycloak. Then you need to assign users to the application.



We also provide a demo video to demonstrate the entire process, which we hope will be helpful to you.

# Appgate (POST)

## Casdoor as a SAML IdP in Appgate

Appgate accepts the `SAMLResponse` sent by POST Request. If you use other SP that also supports POST request, you can refer to this document.

### Casdoor configuration

Go to your Casdoor and add a new application.

Enter basic SAML configuration in the application:

- Redirect URLs – Type in a unique name. This may be called `Audience` or `Entity ID` in your SP. See the table below.

Redirect URLs [?](#) :

Redirect URLs	Add
Redirect URL	
<a href="#">appgate</a>	
<a href="https://git.casbin.com/user/oauth2/casdoor/callback">https://git.casbin.com/user/oauth2/casdoor/callback</a>	
<a href="http://localhost:3000/callback">http://localhost:3000/callback</a>	

- Reply URL – type in the URL of the ACS verifying the SAML response, refer to the table below

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

SAML Reply URL <https://mycontroller.mycompany.com/admin/saml> (?)

Enable SAML compress [?](#)

Administrator Authentication	User Authentication
Redirect URL = "AppGate"	Redirect URL = "AppGate Client"
SAML Reply URL = <a href="https://mycontroller.mycompany.com/admin/saml">https://mycontroller.mycompany.com/admin/saml</a>	SAML Reply URL = <a href="https://redirectserver.mycompany.com/saml">https://redirectserver.mycompany.com/saml</a>

## Download the XML metadata file

You can copy the URL of metadata and download the file from your browser.

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 CAuGgAwIBAgIDAeJAM40GCSqGSIb3DQEBCwUAMDXxHTAbBgNVBAtTFENhc2Rvb3IgT3JnYW5pemFOaW9uMRUwEwYDVQQDEwxDYXNkb...
```

# Add SAML IdP in Appgate

In your AppGate SDP console:

- Select System > Identity Providers
- Create a new Identity Provider
- Choose the type SAML
- Start configuring your identity provider following the details in the tables below

Administrator Authentication	
Name	Enter a unique name eg: "Casdoor SAML Admin"
Single Sign-on URL	See below
Issuer	See below
Audience	Type in the Redirect URL from the Casdoor application
Public Certificate	See below

- Upload the XML Metadata file to autocomplete **Single Sign-On**, **Issuer** and **Public Certificate** fields
- Click **Choose a file** and select the metadata file that you created previously - this will autocomplete the relevant fields

## Map Attributes

Mapping the **Name** to **username**, your completed form should look something like this:

The screenshot shows a user interface titled "Map Attributes to User Claims". At the top right is a blue button labeled "Add New" with a plus sign icon. Below the title, there is a single row in a table-like structure. The first column contains the text "Name mapped to claim username". The second column is empty. The entire row is highlighted with a light gray background.

Attribute	Claim Type
Name mapped to claim username	

## Test Integration

On your AppGate SDP Controller console:

- Log out of the admin UI
- Log in using the following information:
  - Identity Provider – choose your Azure IdP from the drop down list
  - Click Sign in with browser to connect to your authenticator
- You may see the following message: “You don’t have any administration rights”
  - this confirms that the test user credentials have been successfully authenticated by your Identity Provider.

## Access Policy

Your need to modify the access policy that the administrator can log in the Appgate by the SAML idp. Enter Builtin Administrator Policy:

Your completed form should look something like this:

## 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



# WebAuthn

## Overview

We are delighted to inform the Casdoor's customers that Casdoor now supports logging in with WebAuthn, which means, you may be able to log in with your biological identifications like fingerprints or facial recognition even U-disks, provided that your device support these cool authorization method and WebAuthn.

## What is WebAuthn?

The Web Authentication API (also known as WebAuthn: <https://webauthn.io/>) is a specification written by the W3C and FIDO, with the participation of Google, Mozilla, Microsoft, Yubico, and others. The API allows servers to register and authenticate users using public key cryptography instead of a password. It allows servers to integrate with the strong authenticators now built into devices, like Windows Hello or Apple's Touch ID.

To be concise, WebAuthn asks users to generate a public key - private key pair, and hand over the public key to the website. When a user wants to log in to a website, the web generates a random number and asks the user to encrypt it with its private key and send back the result. After receiving the result, the website will try to use the public key to decrypt, and if the decrypted number is the same as the random number generated before, the user will be regarded as a legal user and he will be allowed to log in. We call the public key combined with necessary information (like username or information about user's authorizer ) the Webauthn Credential, which is exactly what is stored by the website.

The public key - private key pair is exclusively uniquely distinguished three information: (user's username, user's authorizer, and the website's url). This means, if the (user's username, user's authorizer, and the website's url) is all the same, the key pair should be identical, and vice versa.

For more detailed information about the WebAuthn Technology, you can visit <https://webauthn.guide/>.

## How to use WebAuthn in casdoor?

In the login page, you must have already seen the choice of using WebAuthn to login in. But considering that you haven't got a Webauthn credential (webauth password, if this inaccurate explanation can make you understand better) yet, so in this tutorial, we are going to show you how to create and manage a credential first and then, how to log in with the credential.

**Step0: modify the configurations and turn on the WebAuthn authentication**

In conf/app.conf you can see

```
origin = "http://localhost:8000"
```

Please ensure this configuration is EXACTLY the url of your website

**Only https is supported for WebAuthn unless you are using localhost**

Then log in as the administrator and go to the edit page of your application. Turn the switch on "Enable WebAuthn signin". By default, this feature is not enabled.

**Step 1: go to "my account" page**

Step 1: go to account page. On this page, you shall see the "Add WebAuthn Credential" Button and a list manifesting all the Webauthn credentials you have

previously registered.

The screenshot shows a user interface for managing credentials. At the top, there's a field for "Signup application" with a placeholder "(empty)". Below it, a section for "3rd-party logins" shows a GitHub icon with the text "(empty)" and a "Link" button. Under "WebAuthn credentials", there's a table with one row. The row contains a GitHub icon, the text "GitHub:", and a "Delete" button. The table has columns for "WebAuthn credentials" and "Action". In the "Actions" column, there's a red "Delete" button. Below the table, there are sections for "Roles" (with a "Save" button) and "Permissions" (with toggle switches for "Is admin", "Is global admin", "Is forbidden", and "Is deleted"). At the bottom, there are "Save" and "Save & Exit" buttons.

Press the button and then follow the instructions of your device to register a new credential into casdoor.

You can remove any credentials via the "delete" button in the list.

## Step 2: log in via WebAuthn

Before this step starts, make sure you have logged out the casdoor.

Go to the log in page, choose the wenauthn login method, enter your username and press the login button, and follow the instructions of your device.

(For example, if you use fingerprint and Window Hello, you are supposed to see something like this)



Windows Security

>Password [WebAuthn](#)

Auto sign in [Forgot password?](#)

[Sign in with WebAuthn](#)



Then you will see that you have already logged in.



&gt;

Developer Guide

# Developer Guide



## Frontend

Casdoor frontend development guide



## Generating Swagger Files

Generating Swagger Files

# Frontend

The source code for Casdoor's frontend is inside the `/web` folder:

<https://github.com/casdoor/casdoor/tree/master/web>

It is a [Create-React-App \(CRA\)](#) project, which has a classic CRA folder structure as follows:

File/Directory	Description
public	the HTML root file for React
src	source code
craco.config.js	the Craco config file, can change the theme color (blue by default) here
crowdin.yml	Crowdin i18n config file
package.json	NPM/Yarn dependency file
yarn.lock	Yarn lock file

Inside `/src`, there are several important files or folders as follows:

File/Directory	Description
account	the "My profile" page for logged-in users

File/Directory	Description
auth	all code related to authentication, like OAuth, SAML, sign up page, sign in page, forget password page, etc.
backend	the SDK for calling Go backend API, contains all the <code>fetch()</code> calls
basic	the homepage (dashboard page) for Casdoor, it contains several card widgets
common	shared UI widgets
locales	i18n translation files in JSON, synced with our Crowdin project: <a href="https://crowdin.com/project/casdoor-site">https://crowdin.com/project/casdoor-site</a>
App.js	the entrance JS file, containing all routes
Setting.js	the utility functions used by other code
OrganizationListPage.js	the page for the organization list, similar to all other XXXListPage.js
OrganizationEditPage.js	the page for editing one organization, similar to all other XXXEditPage.js

# Generating Swagger Files

## Overview

As we know, beego framework provides support for generating swagger file in order to clarify the api via the command line tool called "bee". Casdoor is built based on beego too. However, we found that the swagger files generated by bee failed to categorize the apis with "@Tag" label, so we modified the original bee to implement the function.

## How to write the comment

Most rules are exactly identical to the original bee comment formats, and the only discrepancy is that the api shall be divided into different groups according to the "@Tag" label, therefore developers are obliged to ensure that this tag is correctly added. Here is an example:

```
// @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() {
```

api with same "@Tag" labels will be put into the same group.

## How to generate the swagger file

0. write comments for api in correct format
1. fetch this repository <https://github.com/casbin/bee>
2. build the modified bee, for example, in the root directory of casbin/bee, run

```
go build -o mybee .
```

3. copy mybee to the base directory of casdoor
4. in that directory, run

```
mybee generate docs
```

Then you will find the new swagger files are generated.



> Organizations

# Organizations



## Overview

Casdoor basic unit — organization



## Organization Tree

the user's groups



## Password Complexity

Support different password complexity options.



## Account Customization

Customizing users' account items

 **Customize theme**

Customize themes for organizations and applications under the organization

 **Manage Multi-Factor authentication items**

Config Muti-Factor authentication items in organization

# Overview

Organization is the basic unit of Casdoor, which manages users and applications. If a user signed in to an organization, then he can access all applications belonging to the organization without signing in again.

In the config of [applications](#) and [providers](#), choosing an organization is important, it determines whether a user can access the application using specific providers.

We can also set up LDAP in Casdoor. For more details, please see [LDAP](#).

Casdoor provides multiple password storage algorithms that can be selected in the organization edit page.

Name	Algorithm	Description	Scenario
plain	-	The password will be stored in cleartext. (default)	-
salt	<a href="#">SHA256</a>	<a href="#">SHA-256</a> is a patented cryptographic hash function that outputs a value that is 256 bits long.	-
md5-salt	<a href="#">MD5</a>	The <a href="#">MD5 message-digest algorithm</a> is a cryptographically broken but still widely used hash function producing a 128-bit hash value.	<a href="#">Discuz!</a>

Name	Algorithm	Description	Scenario
bcrypt	bcrypt	<code>bcrypt</code> is a password-hashing function and is used to hash and salt passwords securely.	Spring Boot, WordPress
pbkdf2-salt	SHA256 and PBKDF2	<code>PBKDF2</code> is a simple cryptographic key derivation function, which is resistant to dictionary attacks and rainbow table attacks. It's originally implemented in Casdoor for Keycloak syncer. Select this option if you import users by Keycloak syncer.	Keycloak



Besides logging into Casdoor via an application (which redirects to Casdoor for SSO), a Casdoor user can also choose to directly log into Casdoor via the organization's login page: `/login/<organization_name>`, e.g., <https://door.casdoor.com/login/casbin> in the demo site.

# Organization Tree

Groups is a collection of users under an organization. A user can be in multiple groups.

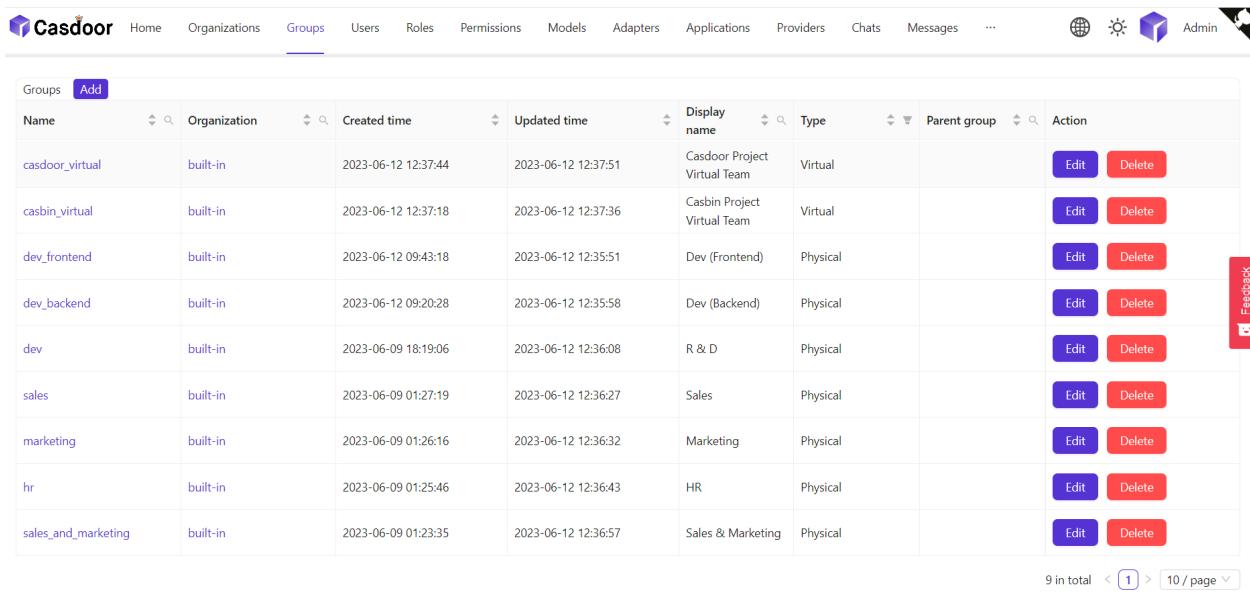
## Group properties

- `Owner` Owner organization of the group
- `Name` Group name (unique)
- `displayName`
- `CreatedTime`
- `UpdatedTime`
- `Type` Groups have two types: `Physical` and `Virtual`, a user can only be in one `Physical` group, but can be in multiple `Virtual` groups.
- `ParentGroup` Parent group of the group (The parent group of top groups in the organization is the organization itself)

## Manage groups

There are two ways to manage groups:

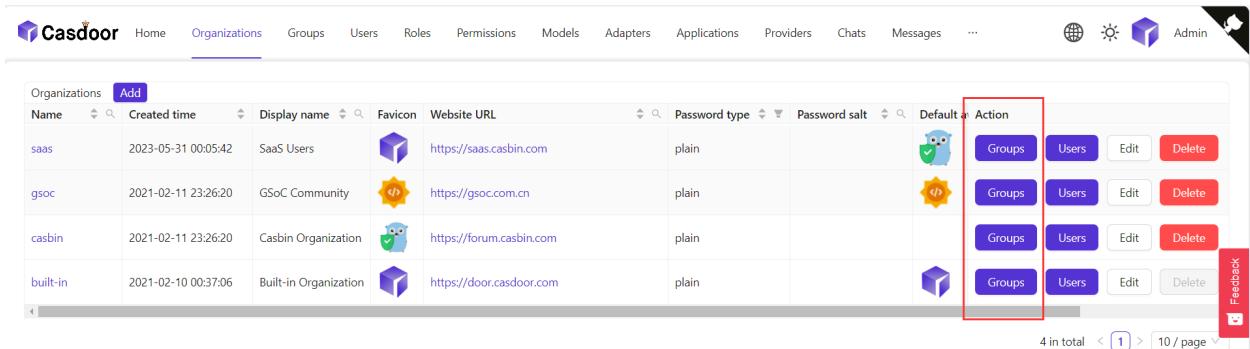
1. In the groups list pages, you can see all the groups in organizations.



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. Click the Groups button in organization list page



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>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>
gsoc	2021-02-11 23:26:20	GSoC Community		https://gsoc.com.cn	plain		<button>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>
casbin	2021-02-11 23:26:20	Casbin Organization		https://forum.casbin.com	plain		<button>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>
built-in	2021-02-10 00:37:06	Built-in Organization		https://door.casdoor.com	plain		<button>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>

4 in total < 1 > 10 / page

Then you can see the tree structure of the groups in the organization.

The screenshot shows the Casdoor interface for managing organizations. On the left, there is a sidebar titled "Built-in Organization" with a tree structure of groups:

- Casdoor Project Virtual Team
- Casbin Project Virtual Team
- R & D
  - Dev (Frontend)
  - Dev (Backend)
- HR
- Sales & Marketing
  - Sales
  - Marketing

A red box highlights the "R & D" group and its sub-items. To the right of the sidebar is a table titled "Users" with the following columns: Organization, Application, Name, Created time, and Display name. The table contains six rows of user data:

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

Here is a video show you how to manage groups:

The screenshot shows the Casdoor interface for managing groups. The "Groups" tab is selected in the navigation bar. The table below lists ten groups:

Name	Organization	Created time	Updated time	Display name	Type	Parent group	Action
group_smf8bl	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_zkak7d	built-in	2023-06-11 23:28:45	2023-06-13 23:24:36	New Group - zkak7d	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_5acaqx	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_azpdaf	forum	2023-06-06 08:19:32	2023-06-09 10:50:25	顶级1	Virtual		<button>Edit</button> <button>Delete</button>
group_r09hga	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>

Groups can be also edit in user profile.

Title <a href="#">?</a> :	1122
Homepage <a href="#">?</a> :	
Bio <a href="#">?</a> :	
Tag <a href="#">?</a> :	222
Karma <a href="#">?</a> :	333
Signup application <a href="#">?</a> :	app-built-in
Groups <a href="#">?</a> :	<div style="border: 1px solid #ccc; padding: 2px;"> Dev (Frontend) <span style="font-size: small;">×</span> :: Casdoor Project Virtual Team <span style="font-size: small;">×</span></div>
Roles <a href="#">?</a> :	
Permissions <a href="#">?</a> :	

# Password Complexity

Casdoor supports customizing password complexity options for user password in each organization.

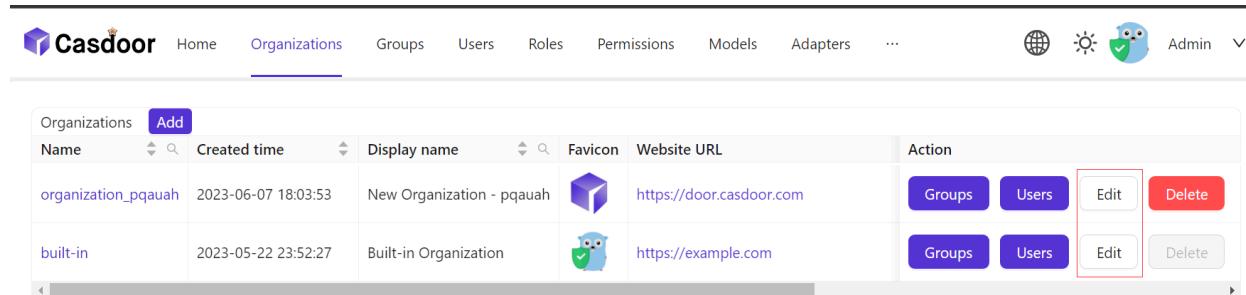
## Supported Complexity Options

We currently support 5 options:

- `AtLeast6`: The password must have at least 6 characters
- `AtLeast8`: The password must have at least 8 characters
- `Aa123`: The password must contain at least one uppercase letter, one lowercase letter and one digit
- `SpecialChar`: The password must contain at least one special character
- `NoRepeat`: The password must not contain any repeated characters

If you want to use multiple options, you can select them on the organization edit page:

1. Click the Edit button in organization list page



Organizations						Add			
Name	Created time	Display name	Favicon	Website URL	Action	Groups	Users	Edit	Delete
organization_pquaah	2023-06-07 18:03:53	New Organization - pquaah		<a href="https://door.casdoor.com">https://door.casdoor.com</a>		<a href="#">Groups</a>	<a href="#">Users</a>	<a href="#">Edit</a>	<a href="#">Delete</a>
built-in	2023-05-22 23:52:27	Built-in Organization		<a href="https://example.com">https://example.com</a>		<a href="#">Groups</a>	<a href="#">Users</a>	<a href="#">Edit</a>	<a href="#">Delete</a>

2. Then select the option you need in the **Password complexity options** column.

The screenshot shows the Casdoor web application interface. The top navigation bar includes links for Home, Organizations, Groups, Users, Roles, Permissions, Models, Adapters, Applications, Providers, and Admin. The 'Organizations' tab is active. Below the navigation, there's a form for editing an organization. The 'Name' field contains 'built-in'. The 'Display name' field contains 'Built-in Organization'. The 'Favicon' field shows a preview of a blue owl icon with a green shield. The 'Website URL' field contains 'https://example.com'. The 'Password type' dropdown is set to 'plain'. The 'Password salt' field is empty. The 'Password complexity options' section contains several validation rules: 'The password must have at least 8 characters', 'The password must contain at least one special character', 'The password must not contain any repeated characters', 'The password must contain at least one uppercase letter, one lowercase letter and one digit', 'The password must have at least 6 characters', 'The password must have at least 8 characters', and 'The password must contain at least one uppercase letter, one lowercase letter and one digit'. A tooltip for the 'Supported country codes' section lists 'Germany +49', 'United Kingdom +44', and 'India +91'.

# Password Complexity Validation

We support password complexity validation on the following pages:

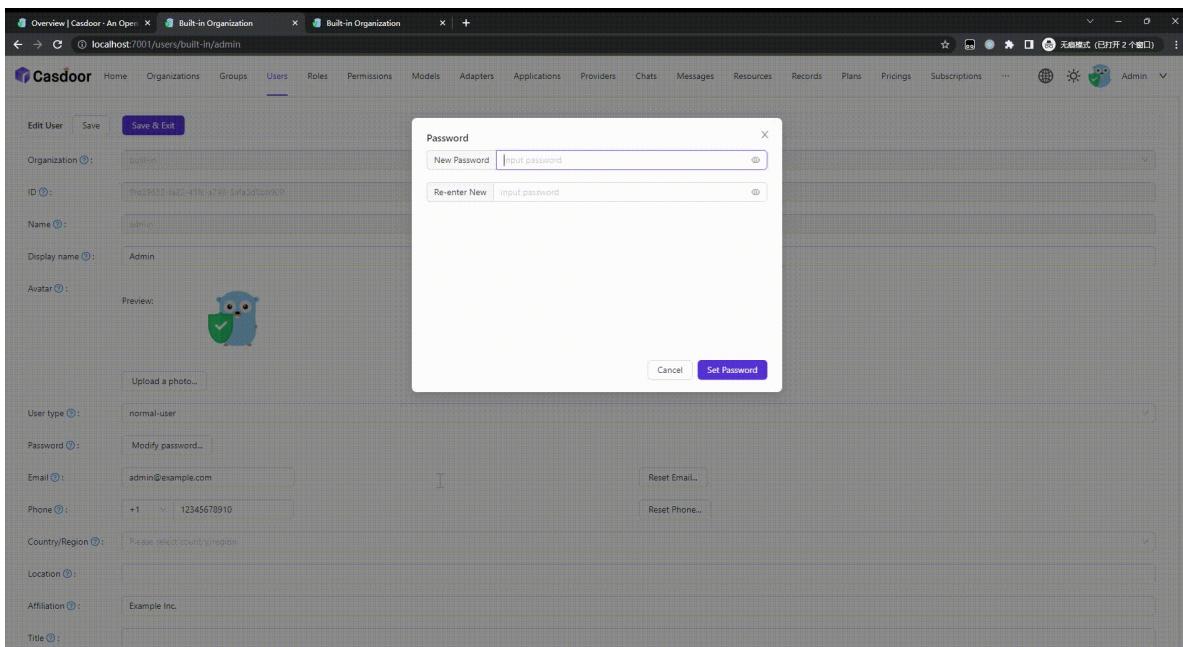
1. Sign up page

The screenshot shows the Casdoor sign-up interface. At the top, there are three tabs: "Overview | Casdoor - An Open", "Built-in Organization", and "Built-in Organization". The URL in the address bar is "localhost:7001/signup". The main form has fields for "Username" (filled with "eee"), "Display name" (filled with "222"), "Password", "Confirm", and "Email". Below these are two sets of fields for "Email code" and "Phone code", each with an "Enter your code" input field and a "Send Code" button. There is also a "Phone" field set to "+1". A checkbox for "Accept Terms of Use" is checked, and a "Sign Up" button is at the bottom right, with a link "Have account? sign in now" nearby. The footer says "Powered by Casdoor".

## 2. Forget password page

The screenshot shows the Casdoor retrieve password page. The title is "Casdoor" and the subtitle is "Retrieve password". Below the title are three tabs: "Account" (selected), "Verify", and "Reset". The "Account" tab contains fields for "Password" and "Confirm". A "Change Password" button is at the bottom. The footer says "Powered by Casdoor".

## 3. User edit page



# Account Customization

## Introduction

In an organization, you can customize users' account items. This includes whether each item is **visible**. If visible, its **view rule** and **modify rule**.

When you customize account items in an organization, this configuration takes effect on the home page of all members of that organization.

## How to customize?

Account item has four attributes:

Column Name	Selectable Value	Description
Name	-	Account item name.
Visible	True / False	Select whether this account item is visible on the user home page.
ViewRule	Rule Items	Select a rule to use with view the account item.
ModifyRule	Rule Items	Select a rule to use with modify the account item.

Enter the Organization Edit page, you will find the following:

Account items <small>(1)</small>		visible	viewRule	modifyRule	Action
Name	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	  

Casdoor provides very simple operations to configure:

- Set the item to be visible or invisible

Account items <small>(1)</small>		visible	viewRule	modifyRule
Name	Organization	<input checked="" type="checkbox"/>	Public	Admin
ID		<input type="checkbox"/>	Public	Admin
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

- Set viewing and modifying rules

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"/>

There are 3 rules:

- Public: Everyone has permission
- Self: The users has their own permission
- Admin: The administrator has permission

## Account table

The following are all the fields in account item. For a description, you can see [user](#).

- Organization
- ID
- Name
- Display name
- Avatar
- User type
- Password
- Email
- Phone
- Country/Region

- Location
- Affiliation
- Title
- Homepage
- Bio
- Tag
- Signup application
- 3rd-party logins
- Properties
- Is admin
- Is global admin
- Is forbidden
- Is deleted

# Customize theme

Casdoor allows you to customize theme to satisfy UI diversity from business or brand requirements, including primary color, border radius.

In Casdoor, the scope of theme includes global, organization, and application.

1. Global scope: this is the default theme of Casdoor and is applied to any organization that chooses to follow the global theme. It can only be modified in Casdoor source code, there is no way to modify it in web UI.
2. Organization scope: the theme for an organization can be customized in the organization edit page. The theme takes effect in all the Casdoor after-login pages for the users in the organization and the entry pages (signup, signin, forget password, etc.) of the applications that follow the organization theme.
3. Application scope: the theme for an application can be customized in the application edit page. The theme takes effect in the the entry pages (signup, signin, forget password, etc.) of the application.

## Customize organization theme

We provide a demo to demonstrate how to config theme in organization:

The screenshot shows the Casdoor theme editor interface. On the left, there is a sidebar with a tree view of configuration items: Roles, Permissions, 3rd-party logins, Properties, Is admin, Is global admin, Is forbidden, Is deleted, WebAuthn credentials, and Managed accounts. Each item has a toggle switch and a dropdown menu with options like Public, Immutable, Admin, Self, and various edit icons. Below this sidebar is a "Theme" section with "Follow global theme" and "Customize theme" buttons. Under "LDAPs", there is a table with columns: Server Name, Server, Base DN, Auto Sync, Last Sync, and Action. One entry is shown: "BuildIn LDAP Server" with "example.com:389" in the Server column, "ou=BuildIn,dc=example,dc=com" in the Base DN column, and "Disable" in the Auto Sync column. At the bottom are "Save" and "Save & Exit" buttons, and a footer note: "Powered by Casdoor".

### ⚠ INFO

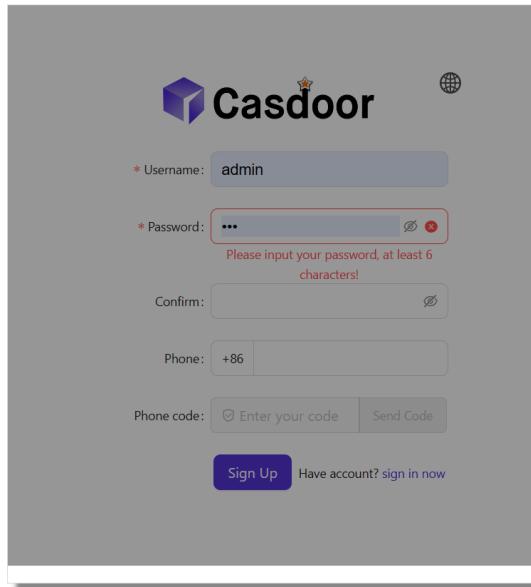
If your account organization is same as the organization you are editing, after you save the configuration, it will take effect immediately as the video above show. But if they are different, you need to log in the organization to see the effect.

## Customize application theme

Applications customize theme use the same theme editor as the organization. But even more conveniently, you can preview the theme in the preview panel.

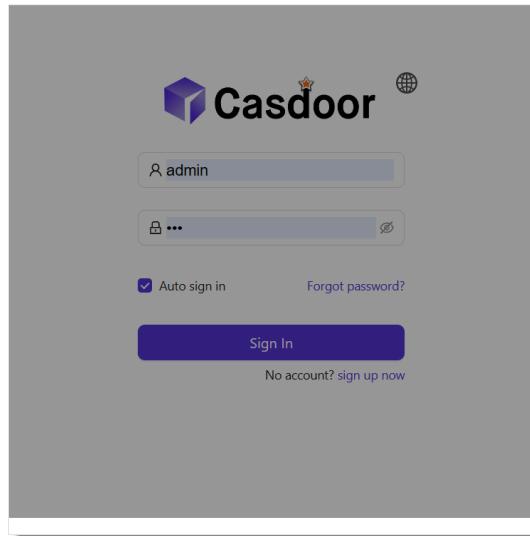
Preview ⓘ

 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

# Manage Multi-Factor authentication items

## Add Multi-Factor authentication item in organization

In organization, admin can add the Multi-factor authentication item in account items so that user can config the Multi-factor authentication in their owner profile page.

The screenshot shows the Casdoor web interface for managing organization settings. At the top, there are fields for 'Master password' (set to \*\*\*), 'Languages' (English, 中文, Español, Français, Deutsch, Indonesia, 日本語, 한국어, Русский, Tiếng Việt), 'Init score' (0), 'Soft deletion' (disabled), and 'Is profile public' (disabled). Below these settings is the 'Account items' section, which lists various account-related fields: Organization, ID, Name, Display name, Avatar, User type, Password, Multi-factor authentication, Email, and Phone. Each field has a 'Visible' switch, a 'View rule' dropdown (Public or Admin), a 'Modify rule' dropdown (Admin, Immutable, Self), and a set of 'Action' buttons (Edit, Delete). A red box highlights the 'Multi-factor authentication' row, indicating it is the item being added or edited.

Name	Visible	View rule	Modify rule	Action
Organization	<input checked="" type="checkbox"/>	Public	Admin	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
ID	<input checked="" type="checkbox"/>	Public	Immutable	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Name	<input checked="" type="checkbox"/>	Public	Admin	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Display name	<input checked="" type="checkbox"/>	Public	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Avatar	<input checked="" type="checkbox"/>	Public	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
User type	<input checked="" type="checkbox"/>	Public	Admin	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Password	<input checked="" type="checkbox"/>	Self	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Multi-factor authentication	<input checked="" type="checkbox"/>	Self	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Email	<input checked="" type="checkbox"/>	Public	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Phone	<input checked="" type="checkbox"/>	Public	Self	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

# Manage Multi-Factor authentication items

You can manage Multi-Factor authentication to determine which Multi-Factor authentication method are available to users.

There are two rules for managing Multi-Factor authentication items:

- optional: Users can choose whether to enable this type Multi-Factor authentication.
- required: Users must enable this type Multi-Factor authentication .

MFA items		Add		
?	Name		Rule	Action
	Email		Required	▲ ▼ ⏚
	Phone		Optional	▲ ▼ ⏚

Here is a demo video to demonstrate the entire process, which we hope will be helpful to you.

feat: Added new locales pt-br br

localhost:8000/organizations/forum

Role	Public	Immutable
Roles	Public	Immutable
Permissions	Public	Immutable
3rd-party logins	Self	Immutable
Properties	Admin	Immutable
Is admin	Admin	Immutable
Is global admin	Admin	Immutable
Is forbidden	Admin	Immutable
Is deleted	Admin	Immutable
WebAuthn credentials	Self	Immutable
Managed accounts	Self	Immutable

MFA items (0):

MFA items Add

Name	Rule	Action
No data		

Theme (0):

Follow global theme Customize theme

Theme

This screenshot shows a web-based administration interface for managing user roles and MFA items. The top section displays a grid of user properties (Roles, Permissions, 3rd-party logins, Properties, Is admin, Is global admin, Is forbidden, Is deleted, WebAuthn credentials, Managed accounts) with their corresponding role assignments (Public, Admin, Self) and immutable status. Below this, the 'MFA items' section is shown with zero items currently added. At the bottom, there is a 'Theme' section with options to follow the global theme or customize it.



&gt;

Applications

# Applications



## Overview

Casdoor application overview



## Terminology reference

Terminology reference



## Application Config

Configure your applications authentication



## Signup Items Table

configure the signup items table to create a custom registration page



## Login UI Customization

Customize the login page UI for your application



## Specify login Organization

Specify login Organization in login page

# Overview

Every application in Casdoor is called an [application](#), and they are not related and do not affect each other, which means you can deploy or stop any application separately, as long as you like.

If you want to use Casdoor to provide login service for your web Web APPs, you can add them as Casdoor applications.

Users can access all applications in their organizations without login twice.

The application configuration is very flexible and simple. You can set whether to allow password login or third-party login, configure the third-party applications you want users to log in, and you can even customize the signup items of the application, etc.

In this chapter you will learn how to start an application of your own, everything from scratch.

Let's explore together!

# Terminology reference

- `Name` The name of the created app
- `CreatedTime` The time when the application is created
- `DisplayName` The name which the application display to public
- `Logo` Application logos will display on the login and sign up page
- `HomepageUrl` The url of the application homepage
- `Description` Describe the application
- `Organization` The organization that the APP belongs to
- `EnablePassword` If users can login via password
- `EnableSignUp` If users can sign up. If not, accounts of the application
- `SignupItems` fields that need to be filled in when users register
- `Providers` Provide all kinds of services for the applications (such as OAuth, Email, SMS service)
- `ClientId` OAuth client id
- `ClientSecret` OAuth client secret
- `RedirectUris` Casdoor will navigate to one of the uris if user logged in successfully
- `TokenFormat`: The format of the generated token. It can be either `JWT` (containing all `User` fields) or `JWT-Empty` containing all non-empty values
- `ExpireInHours` Login will expire after hours
- `SigninUrl`
- `SignupUrl` If you provide a sign up service independently out of Casdoor, please fill the url here
- `ForgotUrl` Same as `SignupUrl`
- `AffiliationUrl`



# Application Config

After you deploy your casdoor on your server, and setup your organization, you can deploy your applications now!

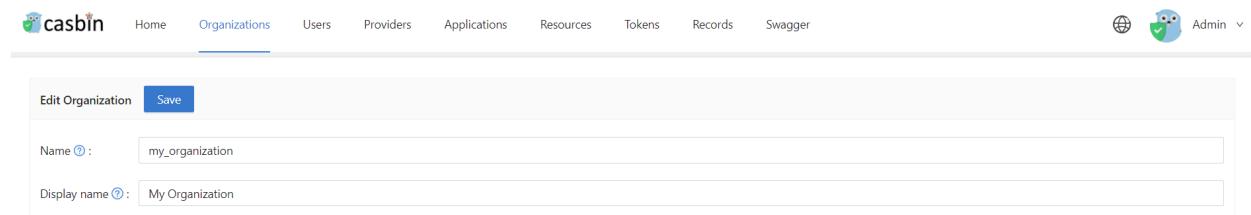
Let's see how to config your applications authentication using Casdoor!

 NOTE

Here, for example, I want to setup my Forum using [Casnode](#)

I create my application and fill some necessary configures.

Select organization I created to make users in this organization can use this application.



The screenshot shows the Casdoor application configuration 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 and the text "Admin". Below the navigation bar, the main content area has a title "Edit Organization" with a "Save" button. There are two input fields: "Name" (containing "my\_organization") and "Display name" (containing "My Organization").

While this organization is named `my_organization`, so I choose it in drop-down menu.

Edit Application Save

Name ? : my\_forum

Display name ? : My Forum

Logo ? : URL: [https://cdn.casbin.com/logo/logo\\_1024x256.png](https://cdn.casbin.com/logo/logo_1024x256.png)

Preview:



Home ? :

Description ? :

Organization ? : built-in

Client ID ? : my\_organization  
built-in

Then I want my users can use Casdoor to complete authentication when they are signing up, so I fill the redirect url here as <https://my-site-url.com/callback>

### ⚠ CAUTION

So here, we need to remember the `callback URL` in provider application is Casdoor's callback url, and the `Redirect URL` in Casdoor is your website callback url

### Further understanding

If I want the authentication progress to work, the detailed progress should

be like this:

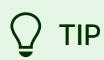
Users send a request to Casdoor, Casdoor use the **Client ID** and **Client Secret** to get authentication from GitHub, Google or other providers.

If the authentication success, GitHub callback to Casdoor to tell Casdoor authentication success, so the GitHub authorization callback URL should be my Casdoor callback URL which is <http://your-casdoor-url.com/callback>, then Casdoor tells the application authentication success which means the Casdoor callback URL should be my application callback URL, that is <http://your-site-url.com/callback>.

Then you can add which third party apps can sign up by adding providers and setting its properties.

Providers	Add	Name	canSignUp	canSignIn	canUnlink	prompted	Action			
provider_casbin_email	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casbin_sms	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_storage_aliyun_oss	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.github_localhost	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.github	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.google	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.qq	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor_wechat	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.facebook	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.gitee	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>
provider_casdoor.gitlab	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="^"/>	<input type="button" value="v"/>	<input type="button" value="d"/>

You need to enable JavaScript to run this app.



#### TIP

Note that if you don't want users to access your app using a **username/password**, you can switch off the **Password On** button, so users can only access app using third party services:

Token expire [?](#) :  Hours

Password ON [?](#) :

Enable signup [?](#) :

# Signup Items Table

On the application configuration page, we can configure the signup items table to create a customized registration page. And we can add or delete any signup item on this signup items table.

Signup items :		Add	Visible	Required	Prompted	Rule	Action		
Name	ID	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Random			
	Username	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			
	Display name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			
	Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			
	Confirm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			
	Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Normal			
	Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			
	Agreement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	None			

For a detailed explanation of each signup item, please see the table below.

Column Name	Selectable Value	Description
Name	-	Signup item name.
visible	True / False	Select whether this signup item is visible on the registration page.
required	True / False	Select whether this signup item is mandatorily required.
prompted	True / False	Select whether to give a prompt when user forget to fill in this signup item.

Column Name	Selectable Value	Description
rule	<input type="button" value="Rule"/> <input type="button" value="Items"/>	Select a rule to use with this signup item. The rule is to add some customization to this signup item. The detailed rules are described in the table below.
Action	-	Users can take some action here, such as moving this signup item up, moving this signup item down, or deleting this signup item.

So far, the signup items that support configuration rules include , ,  and .

Item Name	Selectable Rules	Description
ID	<input type="button" value="Random"/> / <input type="button" value="Incremental"/>	Select whether the user ID is randomly generated or incremented.
Display name	<input type="button" value="None"/> / <input type="button" value="Real name"/> / <input type="button" value="First, last"/>	Choose the presentation of the display name. Choose <input type="button" value="None"/> will show <input type="button" value="Display name"/> Choose <input type="button" value="Real name"/> will show <input type="button" value="Real name"/> Choose <input type="button" value="First, last"/> will show <input type="button" value="First name"/> and <input type="button" value="last name"/>
Email	<input type="button" value="Normal"/> / <input type="button" value="No verification"/>	Select whether to verify the verification code of the mailbox. Choose <input type="button" value="Normal"/> will verify the email code. Choose <input type="button" value="No verification"/> will not

Item Name	Selectable Rules	Description
		verify the email code.
Agreement	<input type="checkbox"/> None / <input type="checkbox"/> Signin / <input type="checkbox"/> Signin <input type="checkbox"/> (Default True)	Select whether the user needs to confirm terms of use when logging in. Choose <input type="checkbox"/> None to not display terms of use, and users can log in directly. Choose <input type="checkbox"/> Signin to require users to confirm the terms before logging in. Choose <input type="checkbox"/> Signin (Default True) to set the terms confirmed by default, and users can log in directly.

### NOTE

Here, for example, I want to setup my registration page bring a mailbox but do not require a mail verification code.

Firstly, I added some signup items necessary for registration, such as ID, Username, Password, Email.



The screenshot shows a configuration interface for 'Signup Items'. There are four items listed: 'Name', 'ID', 'Username', 'Password', and 'Email'. Each item has a 'visible' switch (on), a 'required' switch (on), and a 'prompted' switch (off). The 'rule' dropdown for 'Email' is set to 'No verification'. There are also 'Incremental' and 'Action' dropdowns and a row of edit icons.

Name	visible	required	prompted	rule	Action
ID	On	On	Off	Incremental	Up/Down/Delete
Username	On	On	Off	No verification	Up/Down/Delete
Password	On	On	Off	No verification	Up/Down/Delete
Email	On	On	Off	No verification	Up/Down/Delete

And I selected the email row's rule item to  No verification. As a result, the generated preview registration page can get the expected effect.



\* Username:

\* Password:

\* Email:

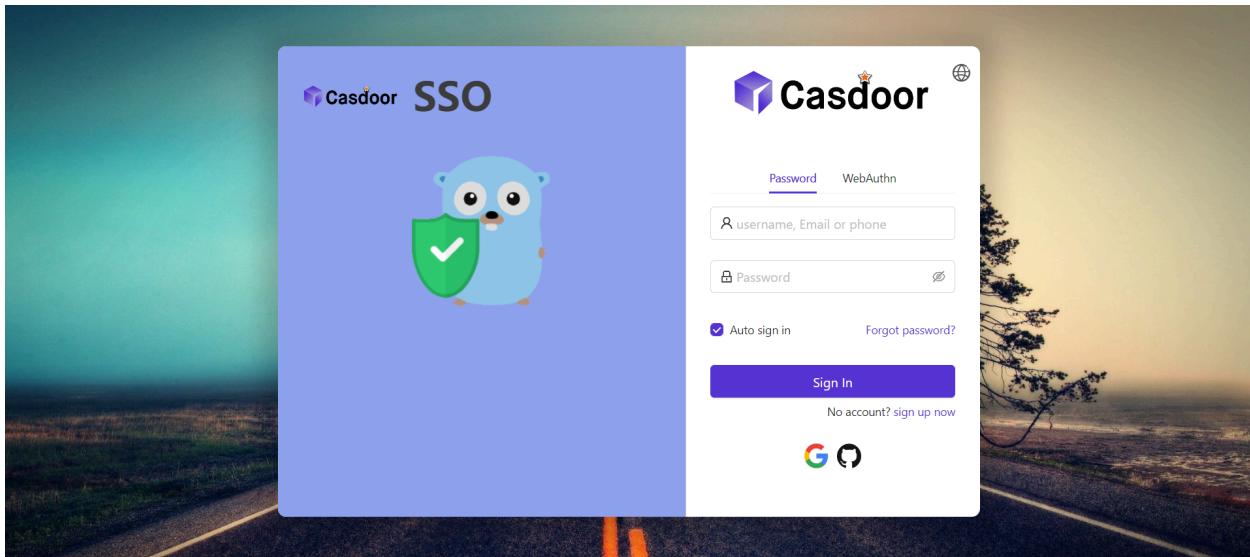
Sign Up

Have account? [sign in](#)

now

# Login UI Customization

You have created the application. Here will show you how to customize the login page UI of the application. In this guide we will create the following application login page:



Let's start!

## Part1: Add a background image

First, let's add a background image. The default background is white. It looks very simple.



Password    WebAuthn

Auto sign in      [Forgot password?](#)

[Sign In](#)

No account? [sign up now](#)



Powered by Casdoor

- **Background URL** The background image url.

Choose the background image you like and fill the **Background URL**. The preview area will display the image, if you fill the valid url.

Background URL ?:	URL ?: <input type="text" value=""/>
Preview:	
Form CSS ?: <input type="text"/>	
Form position ?: <input type="button" value="Left"/> <input type="button" value="Center"/> <input type="button" value="Right"/> <input type="button" value="Enable side panel"/>	

## Part2: Customize the login panel

Here's where you were at the end of the 1st part:



Powered by Casdoor

Now you need to add some css to make the panel look nice. You can copy the code below and paste it in the field `Form CSS`.

```
<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:



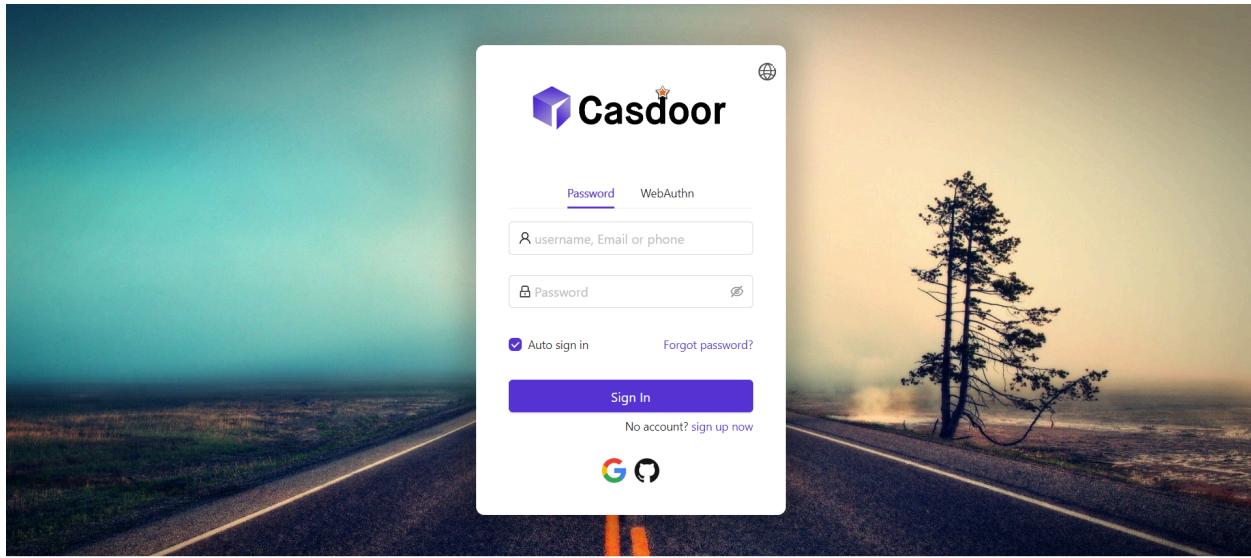
Form CSS ? :

Form position ? : Left Center Right Enable side panel

### TIP

When you edit the `form CSS`, if the value is empty, the editor will show the default value. But it is not fill in the field. You need to copy the content and paste.

After filling the `form CSS`, don't forget to save the config at the bottom. Ok, let's see the effect.



## Part3: Select the Panel position

Now the login page is much prettier than it did at the beginning. We also provide three buttons for you to decide the position of the panel.

Background URL

?

URL ? :



<https://static.runoob.com/images/demo/demo2.jpg>

Preview:



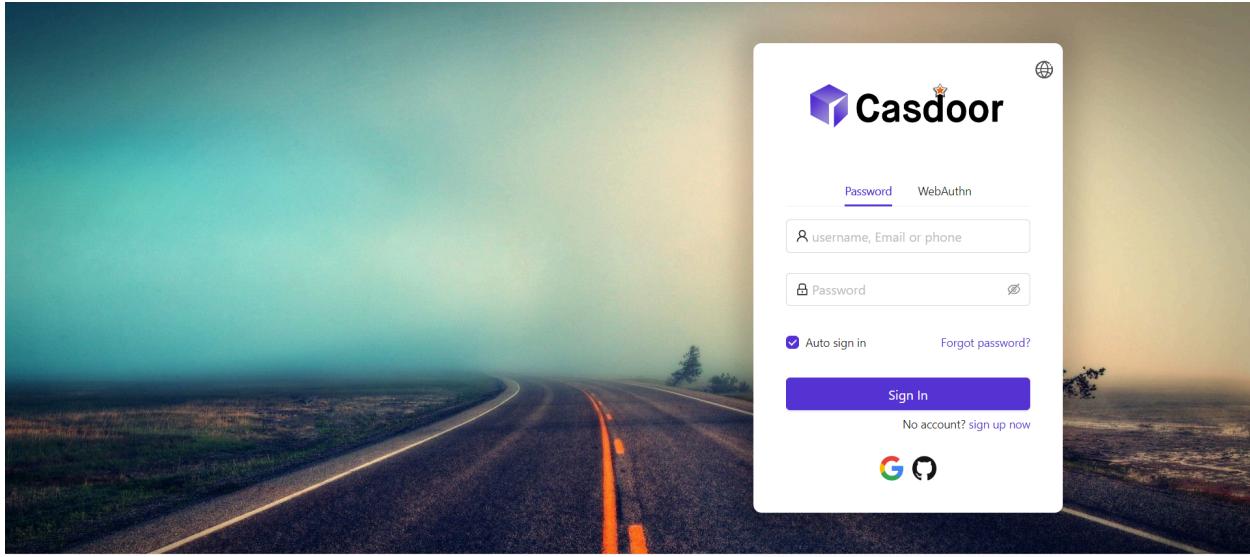
Form CSS ? :

```
<style>.login-panel{ padding: 40px 30px 0 30px; border-radius: 10px; }
```

Form position ? :

Left	Center	Right	Enable side panel
------	--------	-------	-------------------

For example, select the Right button:



Powered by Casdoor

## Part4: Enable the side panel

You will see now how you can enable a side panel and customize the style.

First, select the button. In enable side panel mode, the panel will be in center.

Form position [?](#) :

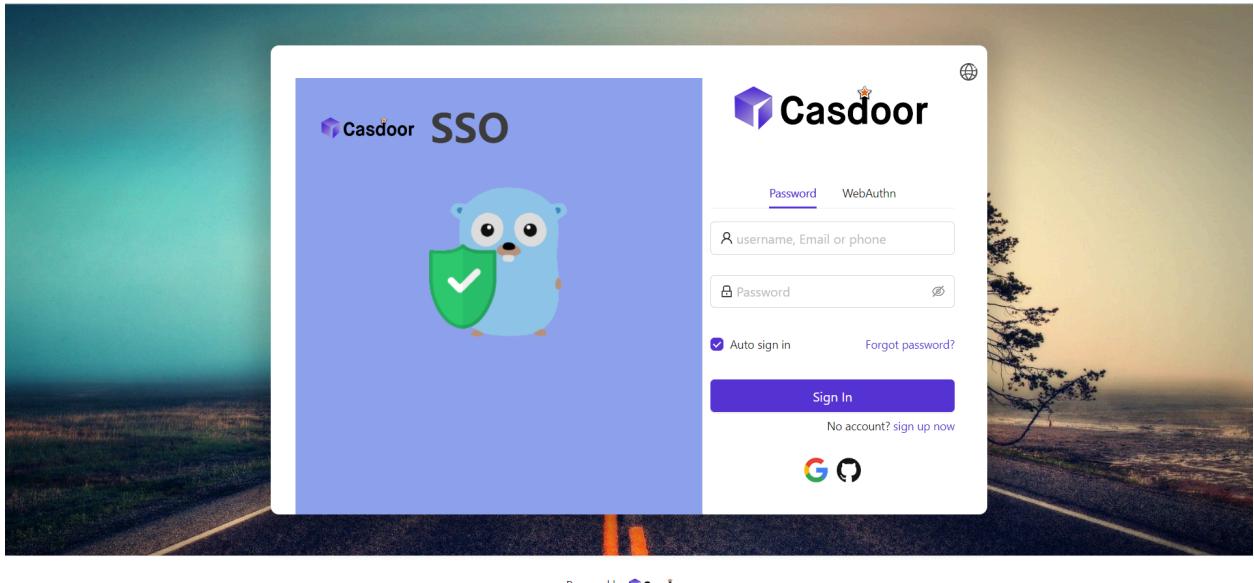
Left	Center	Right	Enable side panel
------	--------	-------	-------------------

Side panel HTML [?](#) :

Then edit the `Side panel HTML`, it decides what content will show in the side panel. Same as the `Form CSS`, we provide a default template. Just copy and paste.

```
<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;
    font-size: 2.4rem;
    line-height: 1.3;
    margin-left: 16px;
    color: #404040;
  }
  .img{
    max-width: none;
    margin: 41px 0 13px;
  }
</style>
<div class="left-model">
  <span class="side-logo"> 
    <span>SSO</span>
  </span>
  <div class="img">
    
  </div>
</div>
```

Let's see the effect. The side panel with a logo and image is shown, but the result was not satisfactory.



You need to modify and add some css in `form CSS`.

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: #ffffff; box-shadow: 0 0 30px 20px rg }</style>
```

Form position :

Left   Center   Right   **Enable side panel**

Side panel HTML :

```
<style> .left-model{ text-align: center; padding: 30px; background-color: #8ca0ed; position: absolute }
```

Signup items :

Signup items **Add**

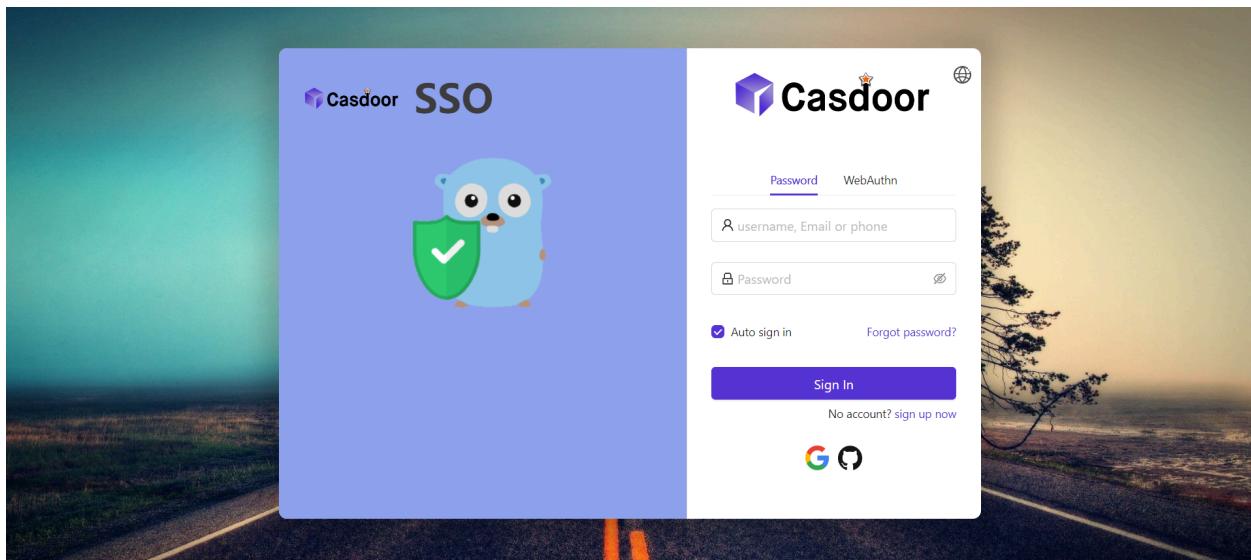
The final code is as follows.

```
<style>
.login-panel{
  border-radius: 10px;
  background-color: #ffffff;
  box-shadow: 0 0 30px 20px rgba(0, 0, 0, 0.20);
}
.login-form {
  padding: 30px;
}
</style>
```

### ⓘ INFO

.login-panel, .login-form are the class names of div. They correspond to different areas of the page. For more details, you can check them through developer tools. After making sure the class names, you can customize the login page more flexibly by writing CSS here.

Finally, we get a beautiful login page.



Powered by Casdoor

# Review

OK, so let's sum it up: we have added a background image, customized the login panel style and enabled the side panel.

More introduction about application in Casdoor:

- [Customize theme](#) Customize the theme, including primary color, border radius.
- [Signup Items Table](#)
- [Application Config](#)

Thanks for reading!

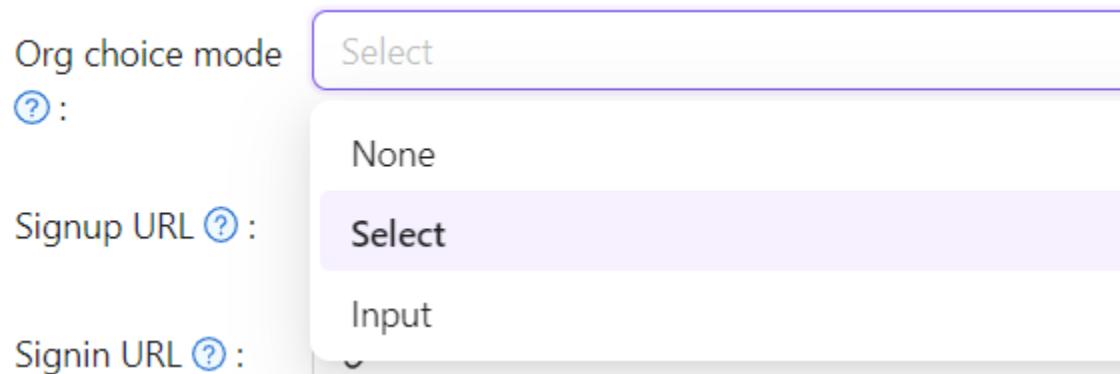
# Specify login Organization

Here will show you how to enable specify login organization page for the application.

For example, endpoint `/login` is default sign in to accounts belonging to the built-in organization. You can enable the specify login organization page in app-built-in application that belong to built-in organization. So that the user can select an organization to login. After the user selects the organization, it will redirect to `/login/<organization>`.

## Config

In the application edit page, you can see the `Org choice mode` config. You can select the mode in the dropdown list.



- None: Don't show the organization select page.
- Input: The user can input the organization name in the input box.
- Select: The user can select the organization in the dropdown list.



Please type an organization to sign in

built-in

Confirm



Please select an organization to sign  
in



built-in

forum

test

Star



INFO

The organization select page only shows when the route is `/login`, `<organization>/login`. That means the application should be set as default application in the organization or the app-built-in.





&gt;

Permissions

# Permissions



## Overview

Using Casbin to manage users' access rights in organization



## Permission Configuration

Using exposed Casbin APIs to manage users' access rights in organization



## Exposed Casbin APIs

Using exposed Casbin APIs to manage users' access rights in organization



## Adapter

Config adapter and basic CRUD to policy

# Overview

## Introduction

All users associated with a single Casdoor organization are shared between the organization's applications and therefore have access to the applications. Sometimes you may want to restrict users' access to certain applications, or certain resources in a certain application. In this case, you can use [Permission](#) implemented by [Casbin](#).

Before going further, you should have an understanding of how Casbin works and its related concepts, such as Model, Policy, and Adapter. In short, Model defines your permission policy structure, and how requests should match these permission policies and their effects. Policy is the description of your specific permission rules. After Casbin obtains Model and Policy information, it can enforce permission control on incoming requests. As an abstraction layer, Adapter shields the source of Policy for Casbin's executor, so that Policy can be stored everywhere, such as files or databases.

Back to the topic of permission configuration in Casdoor. In the Casdoor Web UI, you can add a Model for your organization in the [Model](#) configuration item, and a Policy for your organization in the [Permission](#) configuration item. With [Casbin Online Editor](#), you can get Model and Policy files suitable for your usage scenarios. You can easily import the Model file into Casdoor through the Casdoor Web UI for use by the built-in Casbin. But for Policy (that is, the [Permission](#) configuration item in the Casdoor Web UI), some additional instructions are required here. Let us continue to mention later.

Just as your application needs to enforce permission control through the built-in

Casbin of Casdoor, as a built-in application, Casdoor also uses its Model and Policy to control the calling permissions of the API interface through Casbin. However, Casdoor can call Casbin from internal code, but external applications cannot. Therefore, Casdoor exposes an API for calling the built-in Casbin to external applications. We will show you the definitions of these API interfaces and how to use them later.

End of the chapter, we will use a practical example to show you how Casdoor cooperates with external applications for permission control.

Let's start!

# Permission Configuration

Let's explain each item in the Permission configuration page in turn.

- **Organization**: The name of the organization to which the policy belongs. An organization can have multiple permission policy files.
- **Name**: The permission policy name, which is globally unique in the organization. Used to identify the permissions policy file.
- **Display name**: Nothing important.
- **Model**: The name of the model file describing the permission policy structure and its matching patterns.
- **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 Adapter menu item in the Casdoor Web UI. Casdoor uses its own database to store permission policies being configured. If this field is empty, the permission policy will be stored in the **permission\_rule** table, otherwise 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. We strongly recommend specifying different adapters for different models, as keeping all policies in the same table may cause conflicts.
- **Sub users**: Which users will be applied to this permission policy.
- **Sub roles**: If the RBAC model is used, which roles will be applied to the permission policy. This will add permission policies such as **g user role** for every user in this role.
- **Sub domains**: Which domains will be applied to this permission policy.
- **Resource type**: In fact, in the current version, Casdoor does not use this field

for external applications that want to authenticate. You can ignore it for now.

- **Resources**: This field describes the resources for which you wish to enforce permission control. Note, however, that the resources here are not those configured in the Resources menu item of the Casdoor Web UI. You can add any string you want here, such as a URL or a filename.
- **Actions**: This field describes actions to operate resources. Same as resource, it can be any string you want, such as Http Method or other natural language. But please note that Casdoor will convert all these strings to lowercase before storing. Additionally, Casdoor will apply all actions to each resource. You cannot specify that an action only take effect on certain resources.
- **Effect**: This option takes effect for Casdoor itself to control application access. If you want an external application to enforce permission controls using the interface Casdoor exposes, it won't do anything. You should describe the effect of pattern matching in the Model file.

As you can see, this configuration page is almost tailor-made for the `(sub, obj, act)` model.

# Exposed Casbin APIs

## Introduction

Let's assume that your application front-end has obtained the `access_token` of the logged-in user, and now wants to authenticate the user for some access. You cannot simply place the `access_token` to the HTTP request header to use these APIs, because Casdoor uses the `Authorization` field to check the access permission. Like any other APIs provided by Casdoor, the `Authorization` field consists of the application client id and secret, using the [Basic HTTP Authentication Scheme](#). It looks like `Basic XXX`. For this reason, Casbin APIs should be called by the application backend server. Here are steps about how to do it.

1. The front end passes the `access_token` to the backend server through the HTTP request header.
2. The backend server gets the user id from the `access_token`.

As a note in advance, these interfaces are also pretty much designed (for now) for the `(sub, obj, act)` model. The `permissionId` in the url parameters is the identity of the applied permission policy, which consists of the organization name and the permission policy name (ie `organization name/permission name`). The body is the request format defined by the Casbin model of the permission, usually representing `sub`, `obj` and `act` respectively.

In addition to the API interface for requesting enforcement of permission control, Casdoor also provides other interfaces that help external applications obtain permission policy information, which is also listed here.

## Enforce

Request:

```
curl --location --request POST 'http://localhost:8000/api/enforce?permissionId=example-org/example-permission' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic client_id_and_secret' \
--data-raw '[{"example-org/example-user", "example-resource", "example-action"}'
```

Response:

```
{
  "status": "ok",
  "msg": "",
  "sub": "",
  "name": "",
  "data": [
    true
  ],
  "data2": null
}
```

## BatchEnforce

Request:

```
curl --location --request POST 'http://localhost:8000/api/batch-enforce?permissionId=example-org/example-permission' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic client_id_and_secret' \
```

Response:

```
{  
    "status": "ok",  
    "msg": "",  
    "sub": "",  
    "name": "",  
    "data": [  
        [  
            true,  
            true,  
            false  
        ]  
    ],  
    "data2": null  
}
```

## GetAllObjects

Request:

```
curl --location --request GET 'http://localhost:8000/api/get-all-objects' \  
--header 'Authorization: Basic client_id_and_secret'
```

Response:

```
[  
    "app-built-in"  
]
```

## GetAllActions

Request:

```
curl --location --request GET 'http://localhost:8000/api/get-all-actions' \
--header 'Authorization: Basic client_id_and_secret'
```

Response:

```
[  
  "read",  
  "write",  
  "admin"  
]
```

## GetAllRoles

Request:

```
curl --location --request GET 'http://localhost:8000/api/get-all-roles' \
--header 'Authorization: Basic client_id_and_secret'
```

Response:

```
[  
  "role_kcx661"  
]
```

# Adapter

Casdoor supports using the UI to connect the adapter and manage the policy rules. In Casbin, the policy storage is implemented as an adapter (aka middleware for Casbin). A Casbin user can use an adapter to load policy rules from a storage, or save policy rules to it.

# Adapter

- `type` : Adapter type. Now support database adapter.
- `Host`
- `Port`
- `User`
- `Password`
- `Database type` : Now support MySQL, PostgreSQL, SQL server, Oracle, SQLite 3.
- `Database` : The database name.
- `Table` : The table name. If the table does not exist, it will be created.
- `model` : You can select one model belonging to the organization of the adapter.

Edit Adapter Save Save & Exit

Organization [?](#) : built-in

Name [?](#) : casdoor\_adapter

Type [?](#) : Database

Host [?](#) : localhost

Port [?](#) : 3306

User [?](#) : root

Password [?](#) : 123456

Database type [?](#) : MySQL

Database [?](#) : casdoor

Table [?](#) : casbin\_rule

Model [?](#) : casbin\_rule

Policies [?](#) : Sync

### ! INFO

After fill all the fields, please don't forget to **save** the config. Then click the **sync** button to load the policy rules. The policy rules will be shown in the below table.

Policies [?](#) : Sync Add

Rule Type	V0	V1	V2	V3	V4	V5	Option
p	built-in	*	*	*	*	*	<span>edit</span> <span>trash</span>
p	app	*	*	*	*	*	<span>edit</span> <span>trash</span>
p	*	*	POST	/api/signup	*	*	<span>edit</span> <span>trash</span>
p	*	*	POST	/api/get-email-and-phone	*	*	<span>edit</span> <span>trash</span>
p	*	*	POST	/api/login	*	*	<span>edit</span> <span>trash</span>
p	*	*	GET	/api/get-app-login	*	*	<span>edit</span> <span>trash</span>
p	*	*	POST	/api/logout	*	*	<span>edit</span> <span>trash</span>
p	*	*	GET	/api/logout	*	*	<span>edit</span> <span>trash</span>
p	*	*	GET	/api/get-account	*	*	<span>edit</span> <span>trash</span>
p	*	*	GET	/api/userinfo	*	*	<span>edit</span> <span>trash</span>

< 1 2 3 4 5 >

Is enabled [?](#) : On

↑

# Basic CURD

If you connect the adapter successfully, you can make basic CURD to the policy rules.

- Add

The screenshot shows a table of policy rules. The columns are labeled V0, V1, V2, V3, V4, V5, and Option. The rows show various API endpoints and methods. The 'Option' column contains icons for edit and delete.

Policies ⓘ	Sync	Add	V0	V1	V2	V3	V4	V5	Option
Rule Type									
p	built-in	↳	*	*	*	*	*	*	edit delete
p	*	*	POST	/api/signup	*	*	*	*	edit delete
p	*	*	POST	/api/get-email-and-phone	*	*	*	*	edit delete
p	*	*	POST	/api/login	*	*	*	*	edit delete
p	*	*	GET	/api/get-app-login	*	*	*	*	edit delete
p	*	*	POST	/api/logout	*	*	*	*	edit delete
p	*	*	GET	/api/logout	*	*	*	*	edit delete
p	*	*	GET	/api/get-account	*	*	*	*	edit delete
p	*	*	GET	/api/userinfo	*	*	*	*	edit delete
p	*	*	POST	/api/webhook	*	*	*	*	edit delete



You can only add one policy at one time. The newly added policy is in the first row in the table, but actually, it will be saved in the last row. So next time you sync the policies, they will appear in the last row of the table.

- Edit

casbin_rule										
Model		casbin_rule								
Policies		Sync	Add	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	*	*	 

- Delete

casbin_rule										
User		root								
Password		123456								
Database type		MySQL								
Database		casdoor								
Table		casbin_rule								
Model		casbin_rule								
Policies		Sync	Add	V0	V1	V2	V3	V4	V5	Option
p	*	*		*	*	GET	/api/get-default-application	*	*	 
p	test	*		*	*	*	*	*	*	 



&gt;

Providers

# Providers



## Overview

Add third-party services to your application



## OAuth

19 items



## Email

Using email to complete authentication



## SMS

Using SMS to complete authentication

 Storage

3 items

 SAML

3 items

 Payment

2 items

 Captcha

6 items

# Overview

Casdoor uses providers to provide third-party services for the platform. In this chapter you will learn how to add providers for Casdoor.

## What we have

Now, we have 6 kinds of providers:

- OAuth providers

Casdoor allows users to sign in through other OAuth applications. You can add GitHub, Google, QQ and many other OAuth applications to Casdoor. For more details, please see [OAuth](#).

- SMS Providers

Casdoor sends SMS to users when they want to verify their phone numbers. SMS providers are used to send SMS in Casdoor.

- Email Providers

Email providers are similar to SMS providers.

- Storage Providers

Casdoor allows users to store files using local file system or cloud oss services.

- Payment Provider

Casdoor can add payment providers, which will be used to add payment methods to products on the product page. Currently, the supported payment providers include Alipay, WeChat Pay, PayPal and GC.

- **Captcha Provider**

Casdoor supports configurable captcha in user flows. Currently, the supported captcha providers include Default Captcha, reCAPTCHA, hCaptcha, Aliyun Captcha and Cloudflare Turnstile.

## How to config and use

### Scope

Providers have different scopes. The scope of the provider depends on the creator. Only the Administrator has the permission to add and config providers. There are two kinds of Administrator in Casdoor.

- **Global Administrator:** All users under the `built-in` organization and the user enable `IsGlobalAdmin`. The providers created by Global Administrator can be used by all applications.
- **Organization Administrator:** The user enable `IsAdmin`. The providers created by Organization Administrator can **only** be used by the applications under the organization. (Developing...)

### Add to application

Following under steps to add providers to your application. You still can not use the provider in your application before you add the provider to it.

1. Go to the application edit page and add a new provider row.

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. Select a provider you want to add to the application. Here will show all the providers that the application can use.

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. For OAuth and Captcha providers, you can config the usage. See [OAuth](#) and [Captcha](#)

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"/>	

Last, save the config. Then you can have a try to use the provider in your application.

# OAuth

## Overview

Add OAuth providers to your application

## Custom Provider

Add your own custom OAuth provider

## Twitter

Add Twitter OAuth provider to your application

## Weibo

Add Weibo OAuth provider to your application

 **Wechat**

Add Wechat OAuth provider to your application

 **WeCom**

Add WeCom OAuth provider to your application

 **Tencent QQ**

Add Tencent QQ OAuth provider to your application

 **DingTalk**

Add DingTalk OAuth provider to your application

 **Steam**

Add Steam OAuth provider to your application

 **GitHub**

Add Github OAuth provider to your application

 **Gitee**

Add Gitee OAuth provider to your application

 **Linkedin**

Add Linkedin OAuth provider to your application

 **Facebook**

Add Facebook OAuth provider to your application

 **Google**

Add Google OAuth provider to your application

 **Baidu**

Add Baidu OAuth provider to your application

 **AD FS**

Add AD FS as a third party service to complete authentication

 **AzureAD**

Add AzureAD as a third party service to complete authentication

 **Infoflow**

Add Infoflow OAuth provider to your application

 **Okta**

Add Okta OAuth provider to your application

# Overview

Casdoor can use other OAuth applications as a signin method.

Now, Casdoor supports many OAuth application providers. Icons of providers will be shown in login and signup pages after adding to Casdoor. Here are the providers Casdoor supports:

Provider	Logo	Provider	Logo	Provider	Logo	Provider	Logo
Adfs		Alipay		Amazon		Apple	
Auth0		AzureAD		Baidu		Battle.net	
Bilibili		Bitbucket		Box		Casdoor	
Cloud Foundry		Dailymotion		Deezer		DigitalOcean	
DingTalk		Discord		Douyin		Dropbox	
Eve Online		Facebook		Fitbit		Gitea	
Gitee		GitHub		GitLab		Google	
Heroku		InfluxCloud		Infoflow		Instagram	
Intercom		Kakao		Lark		Lastfm	

Provider	Logo	Provider	Logo	Provider	Logo	Provider	Logo
Line		LinkedIn		Mailru		Meetup	
MicrosoftOnline		Naver		Nextcloud		Okta	
OneDrive		Oura		Patreon		Paypal	
QQ		SalesForce		Shopify		Slack	
SoundCloud		Spotify		Steam		Strava	
Stripe		TikTok		Tumblr		Twitch	
Twitter		Typetalk		Uber		VK	
WeChat		WeCom		Weibo		Wepay	
Xero		Yahoo		Yammer		Yandex	
Zoom		Email		SMS			

We will show you how to apply for a third-party service and add it to Casdoor.

## Apply to become a developer

Before this, there are some general concepts you need to understand.

- **RedirectUrl**, Redirect address after authentication, fill in your application address, such as  
`https://forum.casbin.com/`
- **Scope**, Permission granted to you by the user, such as basic profile, Email address and posts and others.
- **ClientId/AppId, ClientKey/AppSecret**, This is the most important information, and it is what you need to get after you apply for a developer account. You **can not share** the key/secret with anyone.

## Add an OAuth provider

1. Navigate to your Casdoor index page
2. Click `Providers` in the top bar
3. Click `Add`, then you can see a new provider in the list top
4. Click the new provider to modify it
5. Select `OAuth` in `Category`
6. Choose the OAuth provider you need in `Type`
7. Fill the most important information, `Client ID` and `Client Secret`

## Applied in application

1. Click `Applicaton` in the top bar and choose one application, edit
2. click provider add button, select the provider you just added
3. Modify the permissions of the provider, such as allowing registration, login, and unbinding
4. Done!

# Custom Provider

## NOTE

Casdoor supports custom providers, but the custom providers must follow the standard process of 3-legged OAuth, and the return value of `Token URL` and `Userinfo URL` must follow the format specified by Casdoor.

First, go to the provider page of Casdoor, and create a new provider. Select “Custom” in the Type item. It can be seen that in addition to `Client ID` and `Client Secret`, you need to fill in `Auth URL`, `Scope`, `Token URL`, `Userinfo URL` and `Favicon`.

Type  :

Custom

Auth URL  :

<https://door.casdoor.com/login/oauth/authorize>

Scope  :

openid profile email

Token URL  :

[https://door.casdoor.com/api/login/oauth/access\\_token](https://door.casdoor.com/api/login/oauth/access_token)

Userinfo URL  :

<https://door.casdoor.com/api/userinfo>

Favicon  :

URL  :



Preview:

Client ID  :



Client secret  :



- `Auth URL` is the custom provider's OAuth login page address.

Suppose we fill in `https://door.casdoor.com/login/oauth/authorize` at the `Auth URL`, then when the user logs in with this custom provider, the browser will first jump to

```
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}`
```

After authorization is completed, the custom provider should redirect to

```
https://{{your-casdoor-hostname}}/callback?code={code}
```

Then the code parameter in this URL will be recognized by Casdoor.

- `Scope` is the scope parameter carried when accessing the `Auth URL`, which is filled in according to the requirements of the custom provider.
- `Token URL` is the API address for obtaining accessToken.

After obtaining the code in the previous step, Casdoor needs to use this code to get the accessToken.

Suppose we fill in `https://door.casdoor.com/api/login/oauth/access_token` at the `Token URL`, then Casdoor will access the Token URL as follows

```
curl -X POST -u "{ClientID}:{ClientSecret}" --data-binary  
"code={code}&grant_type=authorization_code&redirect_uri=https://{{your-casdoor-  
hostname}}/callback" https://door.casdoor.com/api/login/oauth/access_token
```

The custom provider should return at least the following

```
{  
  "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6Ixxxxxxxxxxxxxx",  
  "refresh_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6Ixxxxxxxxxxxxxx",  
  "token_type": "Bearer",  
  "expires_in": 10080,  
  "scope": "openid profile email"  
}
```

- `UserInfo URL` is the API address for obtaining user information by accessToken.

Suppose we fill in `https://door.casdoor.com/api/userinfo` at the `UserInfo URL`, then Casdoor will access the UserInfo URL as follows

```
curl -X GET -H "Authorization: Bearer {accessToken}" https://door.casdoor.com/api/userinfo
```

The custom provider should return at least the following

```
{
  "name": "admin",
  "preferred_username": "Admin",
  "email": "admin@example.com",
  "picture": "https://casbin.org/img/casbin.svg"
}
```

- `Favicon` is the logo URL of a custom provider.

This logo will be displayed on Casdoor's login page along with other third-party login providers.

# Twitter

## Twitter(still working🚧)

Twitter's application steps are somewhat troublesome, and the official restrictions are a bit strict, so it may be more difficult to apply for a developer account than other third-party platforms.

Visit [Developer Portal](#), register if you don't have an account. Twitter needs to know what you are applying for a developer account for. You must fill in it carefully, otherwise it will not pass.

After the application is approved, create an application, fill in the callback address and other information, you need to do two things, which will be set in Authentication settings section.

- Manually turn on 3-legged OAuth, for Sign in with Twitter, posting Tweets on behalf of other accounts and more.
- Enable Request email address from users, for getting user email address.

# Weibo

## Weibo✓

Weibo's developer account application is not difficult, but the speed is relatively slow. It takes about 2-3 days.

Visit [Developer Website](#), filling in basic information and waiting for a long review...

After the review is approved, you can get the Client Id and Client Secret.

# Wechat

## WeChat✓

Visit [WeChat developer platform](#), and register as a developer. After your web application or your mobile application is approved, then you get your App Id and App Secret.

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

Name ⓘ :	provider_00bws7
Display name ⓘ :	New Provider - 00bws7
Category ⓘ :	OAuth
Type ⓘ :	WeChat
Client ID ⓘ	
Client secret ⓘ	
Client ID 2 ⓘ	
Client secret 2 ⓘ	
Enable QR code ⓘ	<input type="checkbox"/>
Provider URL ⓘ :	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>

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

The WeChat provider offers two different sets of keypairs:

- The first keypair (`Client ID`, `Client Secret`) is for [WeChat Open Platform](#)

(◇◇◇◇◇◇), it's only for the PC login scenario. It can show QR code in PC browser and the user can use the WeChat APP in mobile phone to scan the code, so the PC browser will allow to sign in with WeChat.

- The second keypair (Client ID 2, Client Secret 2) is for WeChat Media Platform (◇◇◇◇◇◇), it's only for the inside-WeChat-app login scenario. It allows the user to log in with WeChat built-in browser inside WeChat mobile APP, it will jump to your WeChat Official Account (◇◇◇◇◇) to log in. It's notable that in the mobile scenario, WeChat itself doesn't support logging in outside of WeChat APP, like in other mobile browsers (H5) or APPs. This is a limitation of WeChat instead of Casdoor.

If you fill in the second keypair (Client ID 2, Client Secret 2) and enable the Enable QR code switch, when the user clicks on the WeChat button to log in, Casdoor will first ask the user to follow the WeChat official account (◇◇◇◇◇), then continue the login process. It's notable that this is only available in PC login scenario because a mobile phone cannot scan the QR code by itself. Casdoor will automatically skip this step when used in mobile scenario (aka the WeChat built-in browser inside WeChat mobile APP).

#### TIP

We recommend setting the two key sets at the same time, and linking your WeChat Open Platform (◇◇◇◇◇◇) account and WeChat Media Platform (◇◇◇◇◇◇) account together inside WeChat Open Platform (◇◇◇◇◇◇). So a WeChat user logged-in through PC and mobile can be recognized as the same user in Casdoor.

#### NOTE

Due to the limitations of WeChat OAuth, there is currently no way to log in

via WeChat in a 3rd-party mobile APP or in a mobile browser other than WeChat APP. The mobile login must happen inside WeChat APP for now.

For more detailed information, please visit [WeChat Open Platform](#).

# WeCom

## Introduction

The WeCom provides the authorized login method of OAuth, which can obtain members' identity information from the webpage opened by the WeCom terminal, eliminating the need for login.

There are two different types of applications: internal applications and third-party applications.

## Basic

To configure a WeCom provider, the following table describes the required parameters.

Parameter Description:

Parameter	Description
Sub type	Internal or Third-party
Method	Silent or Normal
Client ID	The enterprise CorpID
Client secret	The enterprise CorpSecret

Parameter	Description
Agent ID	Application agentid

(!) INFO

WeCom has two authorization methods. Silent authorization and normal authorization.

**Silent authorization:** After the user clicks the link, the page is

`redirect_URI? code=CODE&state=STATE`

**Normal authorization:** After the user clicks the link, a middle page is displayed for the user to choose whether to authorize or not. After the user confirms the authorization, go to `redirect_uri?code=CODE&state=STATE`

For more details, please see [document](#).

## More

For more information about internal application, please see [Internal application](#).

About Third-party application, please see [Third-party application](#).

# Tencent QQ

## Tencent QQ✓

Visit authentication platform of QQ - [Connect QQ](#).

First you need to apply to [become a developer](#). After the review is approved, follow the instructions of the platform and get your Client Id and Client Secret.

# DingTalk

## DingTalk✓

Visit [DingTalk developer platform](#) and log in using your DingTalk account. After entering the platform, follow the instructions of the platform and you will get your Client Id and Client Secret.

For more detailed information, please visit [DingTalk developer docs](#).

In addition, you need to add the following permissions to the dingtalk application:

The screenshot shows the DingTalk Developer Platform interface. The top navigation bar includes '首页', 'Providers', 'OAuth', and 'DingTalk'. Below the navigation is a large 'DingTalk' logo. A sub-section title 'DingTalk✓' is displayed. The main content area has a heading 'In addition, you need to add the following permissions to the dingtalk application:' followed by a horizontal line. Below this, there is a screenshot of the '应用开发' (Application Development) section of the platform. On the left, a sidebar lists various categories like '基础信息', '应用信息', '开发管理', '权限管理' (which is selected and 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 shows a table of permissions. Several rows are highlighted with red boxes: 1. '个人权限' (Personal Permissions) section: '个人手机号信息' (Personal mobile phone number information) with permission 'Contact.User.mobile' and status '已开通' (Enabled). 2. '通讯录管理' (Address Book Management) section: '个人支付宝绑定信息' (Personal Alipay binding information) with permission 'Contact.User.alipayAccount' and status '未开通' (Not enabled). 3. '考勤' (Attendance) section: '日历应用中日程写权限' (Calendar application event write permission) with permission 'Calendar.Event.Write' and status '未开通' (Not enabled). 4. '消息通知' (Message Notifications) section: '日历应用中日程读权限' (Calendar application event read permission) with permission 'Calendar.Event.Read' and status '未开通' (Not enabled). 5. '硬件' (Hardware) section: '通讯录个人信息读权限' (Address book personal information read permission) with permission 'Contact.User.Read' and status '已开通' (Enabled).

# Steam

## Steam✓

Visit [Steam WebAPI platform](#) and log in using your Steam account, then apply for an API Key for your casdoor domain or ip, and finally fill in your API Key as Client Secret into Casdoor. (ClientID does not need to be filled, and your steam account needs to have games to apply for the API)

For more detailed information, please visit [Steam WebAPI doc.](#)

# GitHub

GitHub OAuth supports both web application flow and device flow. Please continue reading to obtain OAuth credential.

First, please visit [GitHub developer settings](#) to register a new GitHub App.

**⚠ CAUTION**

Tricks: We recommend that you use GitHub Apps to replace the OAuth Apps, because GitHub Apps can add multiple redirect uri, which can bring convenience when deploying test and production environments. [GitHub](#) official also recommend using GitHub Apps instead of OAuth Apps.

## Settings / Developer settings



[GitHub Apps](#)



[OAuth Apps](#)



[Personal access tokens](#)

Then fill the GitHub App name, Homepage URL, description and Callback 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

Identifying and authorizing users

The full URL to redirect to after a user authorizes an installation.

Callback URL

http://localhost:7001/callback

Delete

Callback URL

https://door.casdoor.com/callback

Delete

## ❗ SET AUTHORIZATION CALLBACK URL CORRECTLY

In GitHub App config, the `Callback URL` must be your Casdoor's callback url, and the `Redirect URL` in Casdoor should be your application callback url

For more details, please read [App config](#)

After registering your GitHub App, you can generate your `Client Secret` now!

## 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](#)



Client secret

\*\*\*\*\*dba81954

Added 5 minutes ago by [REDACTED]

Last used within the last week

[Delete](#)



Client secret

\*\*\*\*\*15822f89

Added on 15 Feb by [REDACTED]

Last used within the last week

[Delete](#)

Add a GitHub OAuth provider and fill the `Client ID` and `Client Secret` in your Casdoor

Edit Provider

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...2e
Client secret <small>②</small>	***
Provider URL <small>②</small>	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>

Now you can use GitHub as third party service to complete authentication.

# Gitee

To set up Gitee OAuth provider, please go to [Gitee developer](#), if you have not created applications before, the gitee workbench would like this:



Then you can create your gitee app.

## Create Third-party Application

Application Name \*

Application Name

Application Description

Application Description

Application Homepage \*

Your Application Homepage

Application Callback Address \* +

User authorization after redirection address, for example: https://gitee.com/login

Fill in the name, description, homepage and callback URL and carefully choose the permissions.

### ⚠ SET AUTHORIZATION CALLBACK URL CORRECTLY

In Gitee OAuth config, the `authorization callback URL` must be your Casdoor's callback url, and the `Redirect URL` in Casdoor should be your application callback url

For more details, please read [App config](#)

Then you can create you gitee app and get `Client ID` and `Client Secrets` now!

### 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](#)

Add a Gitee OAuth provider and fill the `Client ID` and `Client Secrets` in your Casdoor.

Edit Provider

Save

Name [?](#) :

my\_gitee\_provider

Display name [?](#) :

Gitee provider

Category [?](#) :

OAuth

Type [?](#) :

Gitee

Client ID [?](#)

300ff94d994a7597850bbafb2d5dc67929676dd8e7176b029e067dc6966ef9c4

Client secret [?](#)

\*\*\*\*\*

Now you can use Gitee as third party service to complete authentication!

### CAUTION

Since Casdoor needs to obtain the user's email, the email option must be checked, otherwise it will cause scope authorization errors.

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**

# Linkedin

To set up Linkedin OAuth provider, please go to [Linkedin developer](#) to create a new app.

 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](#)

After filling in the form above and creating your app, you'll need to verify the LinkedIn page associated with the app



## 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](#)



**NOTE**

Only the company page administrator can verify your app, and give permission to your app

After your app is verified, you can continue:

 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 ↗](#)

Add Authorized redirect URLs for your app as your Casdoor callback URL.

**Authorized redirect URLs for your app**

*No redirect URLs added*

**+ Add redirect URL**

**!** SET AUTHORIZED REDIRECT URLs CORRECTLY

In Linkedin OAuth config, the `authorized redirect URLs` must be your Casdoor's callback url, and the `Redirect URL` in Casdoor should be your application callback url

For more details, please read [App config](#)

Then you can obtain your `Client ID` and `Client Secret`

## Application credentials

### Authentication keys

#### Client ID:

860t47n8b4jh7w

#### Client Secret:

.....



Add a Linkedin OAuth provider and fill the `Client ID` and `Client Secret` in your Casdoor.

Edit Provider

Save

Name [?](#) : my\_linkedin\_provider

Display name [?](#) : Linkedin provider

Category [?](#) : OAuth

Type [?](#) : LinkedIn

Client ID [?](#) : 860t47n8b4jh7w

Client secret [?](#) : \*\*\*\*

Now you can use LinkedIn as third party service to complete authentication!

# Facebook

To set up Facebook OAuth provider, please go to [Facebook developer](#) to create a new app.

Select what kind of app you are going to create.

## 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](#)

After filling in your name and contact email, you can enter facebook developer dashboard.

**FACEBOOK for Developers**

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.

**Audience Network**  
Monetize your app and grow revenue with ads from Facebook advertisers.

**App Events**  
Understand how people engage with your business across apps, devices, platforms and websites.

**Messenger**  
Customize the way you interact with people on

**Webhooks**  
Subscribe to changes and receive updates in real

**Instant Games**  
Create a cross-platform HTML 5 game hosted on

Read Docs Set Up Read Docs Set Up Read Docs Set Up

Then set up Facebook login:



## Facebook Login

The world's number one social login product.

Read Docs

Set Up

Choose Web platform for this app:

Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.



iOS



Android



Web



Other

After fill the website url, you can go to **Facebook Login > Settings**, and fill valid OAuth Redirect URIs

#### Client OAuth Settings

Yes

##### Client OAuth Login

Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [?]

Yes

##### Web OAuth Login

Enables web-based Client OAuth Login. [?]

Yes

##### Enforce HTTPS

Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]

No

##### Force Web OAuth Reauthentication

When on, prompts people to enter their Facebook password in order to log in on the web. [?]

No

##### Embedded Browser OAuth Login

Enable webview Redirect URIs for Client OAuth Login. [?]

Yes

##### Use Strict Mode for Redirect URIs

Only allow redirects that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

#### Valid OAuth Redirect URIs

A manually specified redirect\_uri used with Login on the web must exactly match one of the URIs listed here. This list is also used by the JavaScript SDK for in-app browsers that suppress popups. [?]

Valid OAuth redirect URIs.

### ❗ SET AUTHORIZED REDIRECT URLs CORRECTLY

In Facebook OAuth config, the `Valid OAuth Redirect URIs` must be your Casdoor's callback url, and the `Redirect URL` in Casdoor should be your application callback url

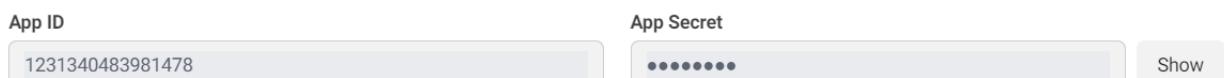
For more details, please read [App config](#)

Basic app configuration is almost done!

Switch mode from **In development** to **Live** in the top bar of dashboard



Then your **App ID** and **App secrets** can be used in Casdoor.



Add a Facebook OAuth provider and fill the **Client ID** and **Client Secrets** with **App ID** and **App Secrets** in your Casdoor.

A screenshot of the Casdoor OAuth provider configuration form for Facebook. The form includes fields for "名称" (Name) set to "my\_facebook\_provider", "显示名称" (Display Name) set to "Facebook provider", "分类" (Category) set to "OAuth", "类型" (Type) set to "Facebook", "Client ID" set to "1231340483981478", and "Client secret" set to "\*\*\*\*\*". A "修改提供商" (Edit Provider) button and a large blue "保存" (Save) button are at the top left of the form.

Now you can use Facebook as third party service to complete authentication!

# Google

To set up Google OAuth provider, please go to [Google API console](#) and log in using your Google account.

Project name \*

My Casdoor



Project ID: my-casdoor. It cannot be changed later. [EDIT](#)

Location \*

No organization

[BROWSE](#)

Parent organization or folder

[CREATE](#)

[CANCEL](#)

Then navigate to OAuth consent screen tab to configure OAuth consent screen.

**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**

And register your Google app.

## 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

Then navigate to Credential tab.

## 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		

And create Credential for your app:

[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 \*



### **⚠ SET AUTHORIZED REDIRECT URIS CORRECTLY**

In Google OAuth config, the `Authorized redirect URIs` must be your Casdoor's callback url, and the `Redirect URL` in Casdoor should be your application callback url

For more details, please read [App config](#)

After create Client ID and obtain `Client ID` and `Client Secrets`

## 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

Add a Google OAuth provider and fill the `Client ID` and `Client Secret` in your Casdoor

[Edit Provider](#) [Save](#)

---

Name [?](#) :

Display name [?](#) :

Category [?](#) :

Type [?](#) :

Client ID [?](#) :

Client secret [?](#) :

Provider URL [?](#) : <https://console.cloud.google.com/apis/credentials/oauthclient/498643462012-46>

Now you can use Google as third party service to complete authentication.

# Baidu

To set up Baidu OAuth provider, please read the [Baidu documentation](#) and follow their steps to complete the [application creation](#).

**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.baiu.com>

◀ **创建工程**

\* 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**

After creating your app, the redirect url is set in the following position:

**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

Add your Casdoor domain in the following position:

The screenshot shows the Casdoor configuration interface. On the left sidebar, there are several tabs: 基本信息 (Basic Information), 接入类型 (Access Type), 其他应用 (Other Applications), 开发者服务 (Developer Services), OAuth2.0, and 安全设置 (Security Settings). The 安全设置 tab is active, displaying the 'Security Settings' page. In the center, there is a section titled 'Implicit Grant 授权方式' (Authorization Method) with two radio buttons: '启用' (Enable) and '禁用' (Disable), where '禁用' is selected. Below this is a '授权回调页' (Authorization Callback Page) input field containing a placeholder URL. To the right of the input field is a note about OAuth security. Further down, there is a '根域名绑定' (Root Domain Binding) input field containing 'door.casbin.com'. A red box highlights this input field. Below it is a checkbox labeled '限制访问OpenAPI的Referer' (Restrict OpenAPI Referer). To the right of this section is another note about OpenAPI referer restrictions. At the bottom of the page are '确定' (Confirm) and '取消' (Cancel) buttons.

### ⚠ CAUTION

This part is very different from the actual situation in the documentation given by Baidu:

1. Adding the url to the callback url setting will most likely fail to validate the url and cause the login to fail, so we add our domain name to the domain setting.
2. Only one url or domain name can be added, which is very different from the documentation.

Then you can get `Client ID` and `Client Secrets` now!

The screenshot shows the Casdoor web application. On the left sidebar, there are several options: 基本信息 (Basic Information), 接入类型 (Integration Type) with a dropdown menu, 其他应用 (Other Applications), 开发者服务 (Developer Services) with a delete icon, OAuth2.0, and 安全设置 (Security Settings). The main content area is titled "基本信息" (Basic Information). It displays a Baidu Developer logo, fields for 名称 (Name: Casdoor), Icon (Icon: a gear icon), and ID (ID: a blurred value). Below these are two red-bordered input fields: "Client ID" with the value "API Key: HnhK7...QmAp61" and "Client Secret" with the value "Secret Key: DTgBZ...ls1bLm1Gha". To the right of these fields is a "Reset" button. Below these fields are two timestamped entries: "创建时间: 2022-01-22 16:20:05" and "更新时间: 2022-01-23 15:45:06".

Add a Baidu OAuth provider and fill the `Client ID` and `Client Secrets` in your Casdoor.

The screenshot shows the Casbin web application. The top navigation bar includes Home, Organizations, Users, Roles, Permissions, Providers (which is highlighted), Applications, Resources, and Tokens. The main content area is titled "Edit Provider" and shows fields for Name (Baidu), Display name (Baidu), Category (OAuth), Type (Baidu), Client ID (HsM...nWT), Client secret (\*\*\*) (both fields are red-bordered), and Provider URL (https://github.com/organizations/xxx/settings/applications/1234567). At the bottom are "Save" and "Save & Exit" buttons.

Now you can use Baidu as third party service to complete authentication!

### (!) GENERAL TROUBLESHOOTING

If you encounter a Baidu prompt that your redirect url is incorrect, here are some ways you might be able to fix it:

1. Add your domain name to the appropriate location, and then reset the Secret (Baidu reset Secret has a bug, it will prompt you an error, but after refreshing the page the Secret has been refreshed)
2. If the above methods do not solve the problem, we suggest you delete the application and create a new one, and set your domain name first.

Another problem is that the user name returned by Baidu is masked, unlike its documentation which shows the user name and the displayed name, so we can currently only use the masked name as the user name.

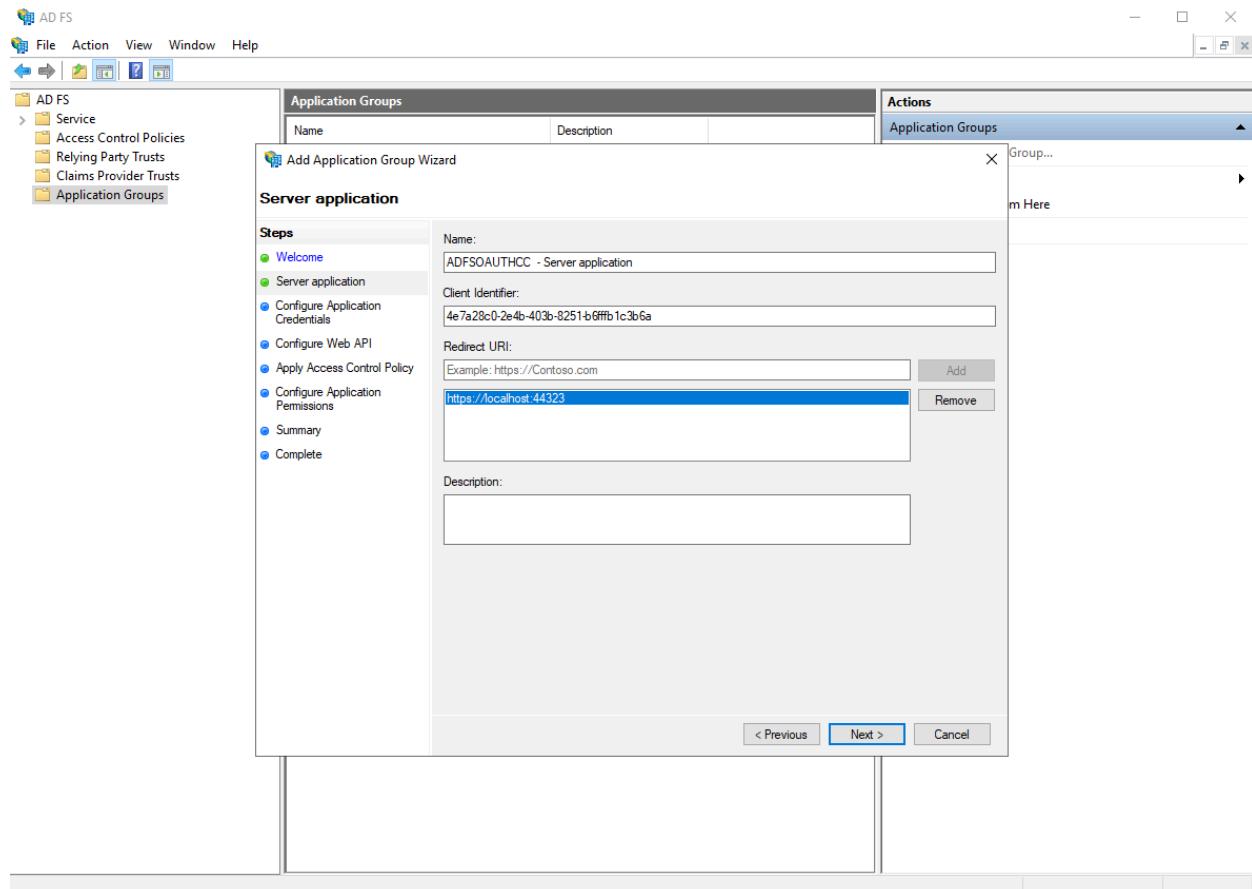
# AD FS

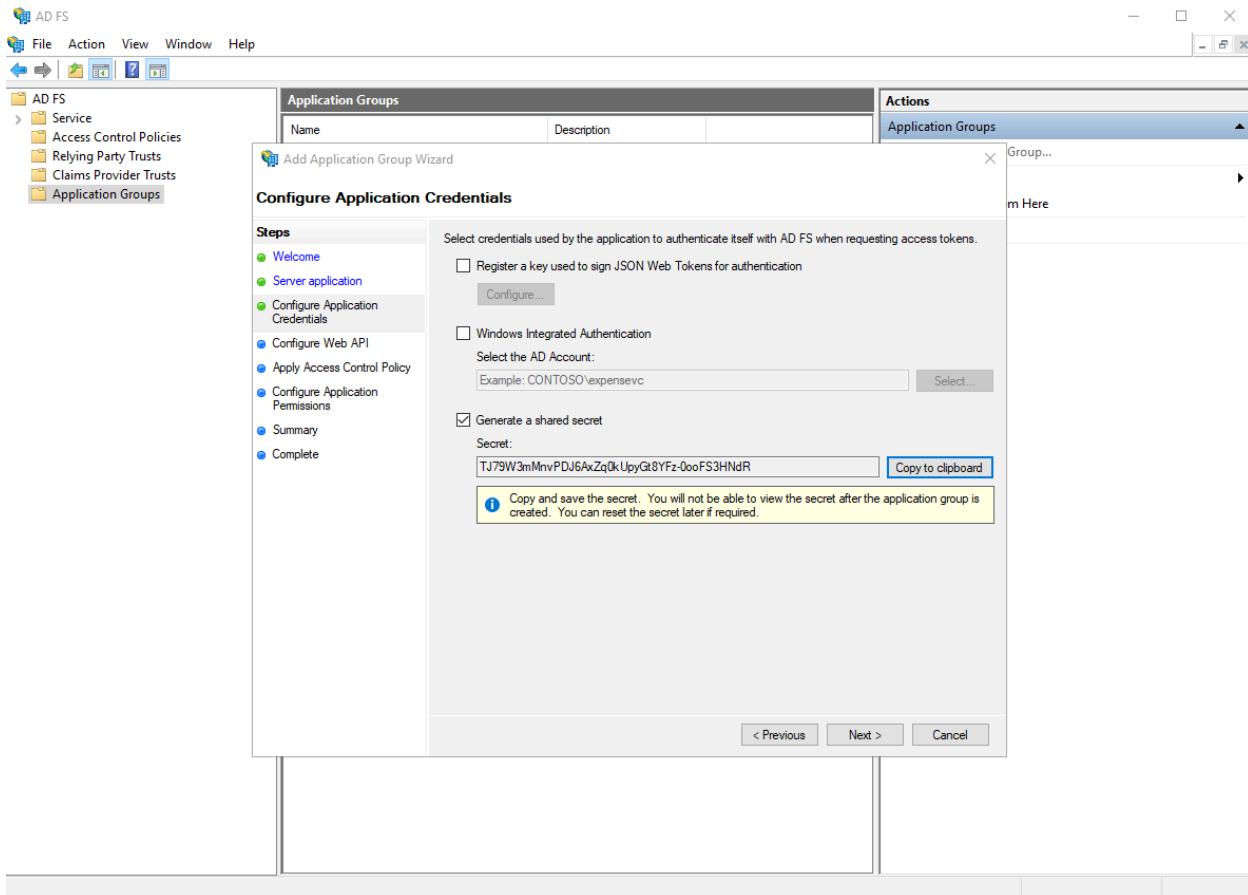
To set up Active Directory Federation Service, please read the [ADFS](#) for the basic knowledge about the ADFS and [AD FS Deployment Guide](#) for how to set up a AD FS server. Do ensure that you have a fully operational AD FS server before you move on to further steps.

## Step1 Enabling Oauth via AD FS

See [Enabling Oauth Confidential Clients with AD FS](#) for details about creating an app step by step.

By the time you finish this step, you should have acquired clientId and clientSecret like this





In which the Client Identifier in first picture and the Secret in the second picture are supposed to be clientId and clientSecret in Oauth.

## Enable Casdoor AD FS Provider

Add a AD FS provider and fill the `Client ID` and `Client Secrets` in your Casdoor.

Edit Provider Save Save & Exit

Name ? :

Display name ? :

Category ? : OAuth

Type ? : Adfs 

Client ID ? :

Client secret ? :

Domain ? :

Provider URL ? : <https://openhome.alipay.com/platform/appManage.htm#/app/2021003111697088/overview>

Save Save & Exit

# AzureAD

## Introduction

Azure Active Directory (Azure AD) simplifies application management by providing a single identity system for cloud and on-premise applications. Software as a Service (SaaS) applications, on-premise applications, and Line of Business (LOB) applications can be added to Azure AD. Users can then log in once for secure and seamless access to these applications, as well as Office 365 and other business applications provided by Microsoft.

## How to use?

The steps to register an app are shown below.

### step1. Register an application

First, [Register](#) an application. And choose an account type as needed. The demo station uses the type shown below.

Microsoft Azure Search resources, services, and docs (G+)

[Home](#) >

## Register an application

### \* Name

The user-facing display name for this application (this can be changed later).

casdoor



### 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](#)

## step2. Create a client secret

Create a `client secret` and save the value, it will be used later.

casdoor | Certificates & secrets ...

Search (Ctrl+/) Got feedback?

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.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
casdoor	1/8/2023	3Xr8Q~dFau2Hwyhg6y8Upb53PCFbuF...	f3c7d37c-1def-4e29-b75f-457fa7c081e8

## step3. Add redirect URIs

Follow the example in the picture to add the redirect URIs for Casdoor.

The screenshot shows the 'casdoor | Authentication' configuration page in the Azure portal. The left sidebar has 'Authentication' selected. The main area shows 'Platform configurations' and 'Supported account types'. On the right, under 'Redirect URIs', there is a red box around the 'http://localhost:8000/callback' entry. Below it, 'Front-channel logout URL' is set to 'https://example.com/logout'. At the bottom are 'Save', 'Discard', 'Configure', and 'Cancel' buttons.

## step4. Grant admin consent

The `user.read` API is open by default. You can add more scope according to your needs. Finally, remember to grant admin consent.

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 selected), Expose an API, App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting (Troubleshooting and New support request), and a Troubleshooting link.

The main content area shows a success message: "Successfully granted admin consent for the requested permissions." It also includes a warning about the end of user consent for newly registered multitenant apps on November 9th, 2020, and a note about the "Admin consent required" column.

The "Configured permissions" section lists Microsoft Graph permissions:

API / Permissions name	Type	Description	Admin consent requ...	Status
email	Delegated	View users' email address	No	Granted for Default Dire...
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Default Dire...
openid	Delegated	Sign users in	No	Granted for Default Dire...
profile	Delegated	View users' basic profile	No	Granted for Default Dire...
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Dire...

A red box highlights the "Grant admin consent for Default Directory" button, and another red box highlights the status column for the listed permissions, which all show "Granted".

## step5. Create AzureAD provider in casdoor

The last step, add an AzureAD OAuth provider and fill the `Client ID` and `Client Secret` in your Casdoor.

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](https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/Applications列表)

Save

Save & Exit

# Infoflow

To set up Infoflow OAuth provider, please go to [Infoflow](#) and log in using your Infoflow account.

First, please visit [Infoflow Application](#).



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

And register your Infoflow app.



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](#))

Then you can get AgentID now.

< 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

Then navigate to Setting tab, and create a new management group.

如流 Infoway 首页 通讯录 应用中心 数据统计 设置 ①

基本信息 成员加入 权限设置 ② 通讯录设置 安全设置 客户端启动页

▼ 系统管理组 普通管理组 ③ 管理员 新建下级管理组 ④

暂未设置管理员 通讯录权限 组织架构

Add your structure to the address book permissions, and give it the permissions shown below. Also add the application you just created to the following location.

## 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

Add the sensitive interface permissions as shown below:

## 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"/>

You will be able to see `CorpID` and `Secret` on the same page:

## 开发者凭据

### Client ID

CorpID

hir211...1

Secret

HgH1...NB

重置

Client Secret

Add an Infoflow OAuth provider and fill the `Client ID`, `Client Secret` and `Agent ID` in your Casdoor.

Edit Provider

Save

Save & Exit

Name ?:

Infoflow

Display name ?:

Infoflow

Category ?:

OAuth

Type ?:

Infoflow

Sub type ?:

Internal

Client ID ?

CorpID

Client secret ?

\*\*\*

Secret

Agent ID ?:

55

AgentID

Now you can use Infoflow as third party service to complete authentication!

# Okta

To set up Okta OIDC provider, first visit [Okta Developer](#) and sign up to get a developer account.

Navigate to Applications > Applications tab, click Create App Integration, select a Sign-in method of OIDC - OpenID Connect, and select an Application type of Web Application, then click Next.

## Create a new app integration

X

### 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](#)

Enter the Sign-in redirect URIs , such as `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 URIs

[Learn More](#)

Allow wildcard \* in sign-in URI redirect.

`https://door.casdoor.com/callback`

X

[+ Add URI](#)

In the **Assignments** section, define the type of Controlled access for your app, then click **Save** to create the app integration.

Now you get `Client ID`, `Client secret`, and `Okta domain`.

### Client Credentials

[Edit](#)

Client ID	Ooa4we8u8iivyscpb5d7	
	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	dev-53555475.okta.com	
-------------	-----------------------	---

Add a Okta OAuth provider in Casdoor dashboard, enter your `Client ID`, `Client secret`, and `Domain`.

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

**❗ SET DOMAIN CORRECTLY**

Note that `Domain` is not just `Okta domain`, `/oauth2/default` should be appended to it.

Visit [Okta docs on authorization servers](#) to get more details.

Now you can use Okta as third party service to complete authentication.

# Email

## Add an Email provider

1. Click [Add](#) to add a new provider.
2. Select [Email](#) in [Category](#)

Name [?](#) :

email provider

Display name [?](#) :

My Email

Category [?](#) :

Email

Type [?](#) :

Default

3. Fill [Username](#), [Password](#), [Host](#), [Port](#) of your smtp service.

Username [?](#)

no-reply@casbin.com

Password [?](#)

\*\*\*

Host [?](#) :

[🔗](#) smtp.qiye.aliyun.com

Port [?](#) :

465

4. Fill customized [Email Title](#) and [Email Content](#) and save.



# SMS

We use [casdoor/go-sms-sender](#) to send SMS for Casdoor. Now, [go-sms-sender](#) supports Aliyun, Tencent Cloud and Volc SMS APIs. You can raise an issue, or make a pull request if you want to support other SMS providers.

## Add a SMS provider

1. Click [Add](#) to add a new provider.
2. Select [SMS](#) in [Category](#)

The screenshot shows the 'Edit Provider' interface. At the top, there are two buttons: 'Edit Provider' and 'Save'. Below these are input fields for 'Name' (set to 'SMS Provider') and 'Display name' (set to 'My SMS'). A 'Category' dropdown is set to 'SMS'. A 'Type' dropdown shows 'SMS' as the selected option. Other options in the 'Type' dropdown include 'OAuth', 'Email', and 'Storage'. At the bottom left, there is a note: 'Client secret [?](#)'.

3. Select your provider type ([Aliyun SMS](#), [Tencent Cloud SMS](#) or [Volc Engine SMS](#))

The screenshot shows a dropdown menu for 'Type'. The selected item is 'Aliyun SMS'. Other options in the menu are 'Tencent Cloud SMS' and 'Volc Engine SMS'. The dropdown has a small arrow icon at the top right.

4. Get your information from Aliyun, Tencent Cloud or Volc Engine and fill them out.

# Example

## ① NOTE

Here, I use Aliyun SMS service as an example

After I logged in my Aliyun workbench, click AccessKey to create ID and Secret.



The screenshot shows the Aliyun Workbench dashboard. At the top, there's a search bar and several navigation links: 费用 (Cost), 工单 (Work Order), ICP 备案 (ICP Record Filing), 企业 (Enterprise), 支持 (Support), App, 简体 (Simplified Chinese). Below the search bar, there's a link to '短信服务操作指南' (SMS Service Operation Guide) and a '产品动态' (Product Dynamics) section with a red notification badge showing '5'. The main content area is titled '短信服务概览' (SMS Service Overview). It features a banner for a '有奖调研' (Prize Survey) about Alibaba Cloud SMS service. Below the banner, there's a section for '用户状态类型: 正常 / 个人用户' (User Status Type: Normal / Individual User). On the left, there's a '发送量数据' (Delivery Volume Data) chart and a '快速上手短信服务, 从这里开始!' (Get started with SMS service quickly, start here!) message with a progress bar indicating 20% completion. On the right, there are sections 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' (which is circled in red). Other sections include '用户监控信息' (User Monitoring Information), '国内消息' (Domestic News), and '国际/港澳台消息' (International/Hong Kong/Macau/Taiwan News). A '快速学习短信服务' (Quickly learn about SMS service) button is also visible.

By creating AccessKey, I get my AccessKey ID and AccessKey Secret:



The screenshot shows the '安全信息管理' (Security Information Management) page. At the top, there's a search bar and several navigation links: 费用 (Cost), 工单 (Work Order), ICP 备案 (ICP Record Filing), 企业 (Enterprise), 支持 (Support), App, 简体 (Simplified Chinese). Below the search bar, there's a note: '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, giving you full control over the account. Please keep them safe.). The main content area is titled '用户AccessKey' (User Access Key). It shows a table with the following data:

AccessKey ID	AccessKey Secret	状态	最后使用时间	创建时间	操作
LTAI4Fy4mVoMjAzC95mt5Wn7	显示	启用	2020年7月19日 20:24:58	2020年7月11日 17:52:50	禁用   删除

A '创建AccessKey' (Create Access Key) button is located at the top right of the table. The entire screenshot has a light gray background.

Fill the `AccessKey ID` and `AccessKey Secret` to Casdoor `Client ID` and `Client Secret`.

# Storage

## Overview

Set up a storage provider for upload files in Casdoor

## Azure Blob

Using Azure Blob as a storage provider for Casdoor

## Aliyun OSS

Using Aliyun OSS as a storage provider for Casdoor

# Overview

If you need to use file storage services such as `avatar upload`, you need to set up a storage provider and apply it in your `application`.

Casdoor supports two types of storage, Local and Cloud. In this chapter you will learn how to add a storage provider to use these services.

## Item

- `Client ID`
- `Client secret`
- `Endpoint`
- `Path prefix`: Path prefix for the file location.

 INFO

Default `Path prefix` is `/`. For example, when the `Path prefix` is empty, a default file path:

`https://cdn.casbin.com/casdoor/avatar.png`

You can fill it with `abcd/xxxx`, and then you can store your avatar in:

`https://cdn.casbin.com/abcd/xxxx/casdoor/avatar.png`

- `Bucket`
- `Domain`: The custom domain name of CDN for your cloud storage.

## Local

With Local type, the only item that you need to configure is `Domain` field. Please follow the format:

Domain/images

For example, `http://127.0.0.1:7001/images`, `http://door.casbin.org/images` are all allowed.

But `127.0.0.1:7001/images` is wrong.

The `Client ID`, `Client secret`, `Endpoint` and `Bucket` field are no longer needed, you can fill in it at will, and it cannot be empty.

## Cloud-Based

Currently, we support AWS S3, Aliyun OSS, Tencent Cloud COS, MinIO and Azure Blob cloud vendors, and are adding more Cloud storage services.

Fill in the corresponding fields with `Client ID`, `Client secret`, `Endpoint` and `Bucket` obtained from your cloud vendor console.



With `Non-local` type, you probably don't need the `Domain` field, which is used for custom domain.



# Azure Blob

 NOTE

This is an example of Azure Blob

- You must have an [Azure storage](#) account.

## Step1. Select Azure Blob

Select the Azure Blob as the storage type.

Provider Settings

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

Name <a href="#">?</a> :	provider_ftfzes
Display name <a href="#">?</a> :	New Provider - ftfzes
Category <a href="#">?</a> :	Storage
Type <a href="#">?</a> :	Azure Blob
Client ID <a href="#">?</a> :	Local File System AWS S3
Client secret <a href="#">?</a> :	Aliyun OSS Tencent Cloud COS
Endpoint <a href="#">?</a> :	Azure Blob

## Step2. Fill the necessary information in Casdoor

There are three required fields. `Client ID`, `Client secret`, `Bucket`. The relationship corresponding to the Azure Blob account is as follows:

Name	Name in Azure	is required
Client ID	AccountName	required
Client secret	AccountKey	required
Bucket	ContainerName	required
Domain	DomainName	

- AccountName

The `AccountName` is your AccountName.

- AccountKey

The `AccountKey` is your key to access Azure API.

 NOTE

You can obtain your account key from the Azure Portal under the "Access Keys" section on the left-hand pane of your storage account.

The screenshot shows the Azure Storage account 'casbin' overview page. The left sidebar contains navigation links like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, and Storage browser (preview). Under Data storage, there are links for Containers, File shares, Queues, and Tables. Under Security + networking, there are links for Networking, Azure CDN, and Access keys. The 'Access keys' link is highlighted with a red box and has a red arrow pointing to it. The main content area displays the 'Essentials' and 'Properties' tabs. The 'Properties' tab is selected, showing Blob service settings such as Hierarchical namespace (Disabled), Default access tier (Hot), Blob public access (Enabled), Blob soft delete (Enabled (7 days)), Container soft delete (Enabled (7 days)), Versioning (Disabled), Change feed (Disabled), NFS v3 (Disabled), and Allow cross-tenant replication (Enabled). It also shows File service settings for Large file share (Disabled) and Active Directory (Not configured). The status bar at the bottom right indicates '2022-04-2'.

- ContainerName

You first need to create a container. There is a default container called 'default'.

Home > casbin

## casbin | Containers

Storage account

Search (Ctrl+)

+ Container    Change access level    Restore containers    Refresh    Delete

Search containers by prefix

Name	Created
\$logs	2022-04-29
<b>default</b>	2022-04-29

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

- Domain

The custom domain name in your Azure CDN.

Home > fd-profile

## fd-profile

Front Door and CDN profiles

Search (Ctrl+)

Purge cache    Origin response timeout    Delete    Refresh

Essentials

Resource group (move) : default	Name : fd-profile
Status : Active	Pricing Tier : Azure Front Door Standard
Location : Global	Front Door ID : f2f8e27a-12ff-4412-9d21-bc583a034f8b
Subscription (move) : Visual Studio Enterprise	Origin response timeout : 60 Seconds
Subscription ID : <a href="#">Visual Studio Enterprise</a>	
Tags (edit) : Click here to add tags	

Properties    Monitoring

Endpoints

Endpoint hostname : endpoint-hth4eebgcdz2ex.z01.azurefd.net	Provision succeeded
	Enabled

Security policy

Custom domains

Domain name : cdn.casploy.com	Provision succeeded
	Validation approved

Routes

Route name (endpoint-hth4eebgcdz2ex.z01.azurefd.net) : default-route	Provision succeeded
	Enabled

Analytics

Reports

Monitoring

A red arrow points from the "Custom domains" section to the text "even section on the".

## Step3. Save your configuration

The final result is as follows:

Name <small>?</small> :	Provider_azure
Display name <small>?</small> :	Provider_azure
Category <small>?</small> :	Storage
Type <small>?</small> :	Azure Blob
Client ID <small>?</small>	casbin
Client secret <small>?</small>	***
Endpoint <small>?</small> :	
Endpoint (Intranet) <small>?</small> :	
Bucket <small>?</small> :	default
Domain <small>?</small> :	<a href="https://cdn.casploy.com/">https://cdn.casploy.com/</a>
Provider URL <small>?</small> :	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>

Then you can use Azure Blob Storage services in your application.

# Aliyun OSS

## NOTE

This is an example of Aliyun OSS.

The AccessKey is your key to access Aliyun API, with full account permissions.

So [created AccessKey](#) in Aliyun workbench.

Then create OSS service:

The screenshot shows the 'Create Bucket' page. At the top right are a help icon, a 'Create Storage Space' button, and a close button. Below is a note: '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。' (Note: After creating the bucket, the selected storage type, region, and redundancy type cannot be changed.) The form fields include: 'Bucket Name' (mycasdoor, 9/63), 'Region' (North China 2 (Beijing)), and 'Endpoint' (oss-cn-beijing.aliyuncs.com). A note below the region field says: '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。' (Products in the same region can communicate via internal network; after purchase, the region cannot be changed, please choose carefully.)

Fill the necessary information in Casdoor and save:

Name <a href="#">?</a> :	provider_storage_aliyun_oss
Display name <a href="#">?</a> :	Storage Aliyun OSS
Category <a href="#">?</a> :	Storage
Type <a href="#">?</a> :	Aliyun OSS
Client ID <a href="#">?</a>	LTAIxFoNpNAnPoiT
Client secret <a href="#">?</a>	***
Endpoint <a href="#">?</a> :	oss-cn-beijing.aliyuncs.com
Endpoint (Intranet) <a href="#">?</a> :	oss-cn-beijing-internal.aliyuncs.com
Bucket <a href="#">?</a> :	casbin
Domain <a href="#">?</a> :	<a href="https://cdn.casbin.com/casdoor/">https://cdn.casbin.com/casdoor/</a>
Provider URL <a href="#">?</a> :	<a href="https://oss.console.aliyun.com/bucket/oss-cn-beijing/casbin/object">https://oss.console.aliyun.com/bucket/oss-cn-beijing/casbin/object</a>

Then you can use Aliyun cloud storage services in your application.

# SAML

## Overview

Using identities from external identity providers that support SAML 2.0

## Aliyun IDaaS

Using Aliyun IDaaS to authenticate users

## Keycloak

Using Keycloak to authenticate users

# Overview

Casdoor can be configured to support user login to UI using identities from external identity providers that support SAML 2.0. In such a configuration, Casdoor can never store any credentials for the users.

Now, Casdoor supports many SAML application providers. Icons of providers will be shown in login page after adding to Casdoor. Here are the providers Casdoor supports:

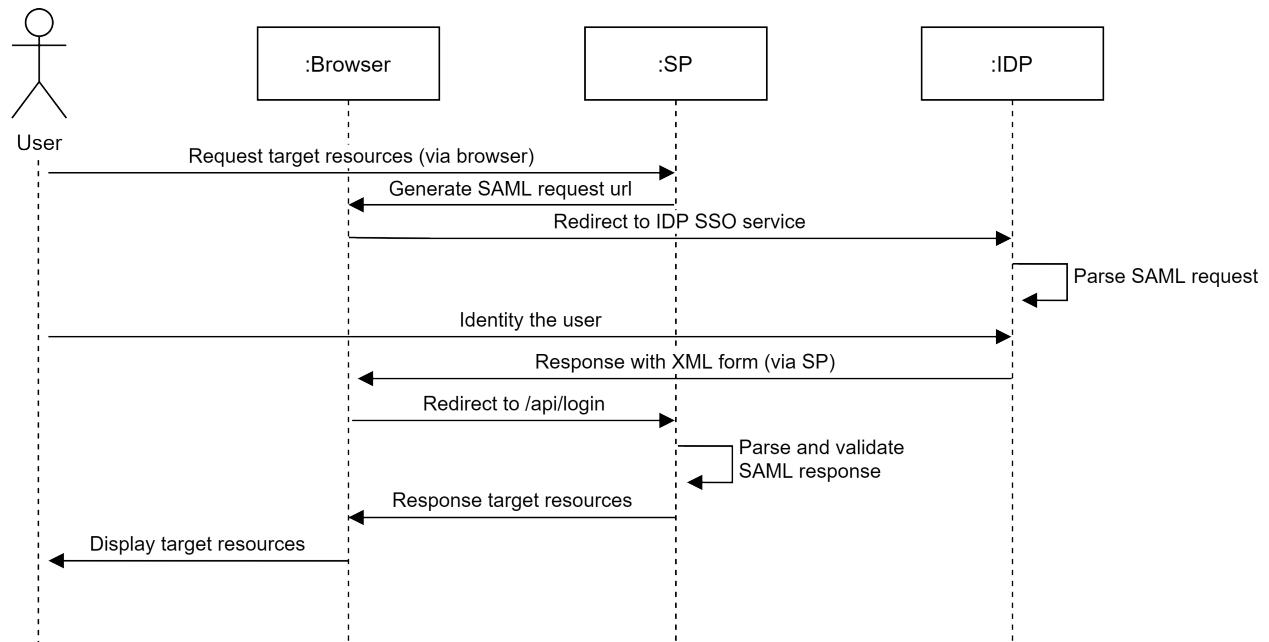
Aliyun IDaaS	Keycloak
	
✓	✓

## Terms

- Identity Provider (IDP) - The service that stores the identity database and provides identity and authentication services to Casdoor.
- Service Provider (SP) - The service providing resources to the end user, in this case, the Casdoor deployment.
- Assertion Consumer Service (ACS) - The consumer of SAML assertions generated by the Identity Provider.

# How SAML integration works

When using SAML SSO, users log into the Casdoor via the identity provider without ever passing credentials to Casdoor. The progress is shown in the following diagram.



# Aliyun IDaaS

## Create SAML application in Aliyun IDaaS

Login to the [Aliyun management console](#), search and go to the Application Identity Service (IDentity-as-a-Service, IDaaS).

The screenshot shows the Aliyun Management Console interface. On the left, there's a sidebar with navigation links like 'EIAM 实例列表' and 'CIAM 实例列表'. The main content area has a title '概览页' (Overview Page) under '应用身份服务' (Application Identity Services). A central box discusses '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). Below this, a table compares 'EIAM 不同版本区别' (Differences between EIAM versions). The table has three columns: '功能 (模块)' (Function (Module)), '标准版' (Standard Edition), and '专业版' (Professional Edition). The '专业版' column includes features like '独立集群部署, 支持灵活扩容' (Independent cluster deployment, supports flexible scaling) and '适合定制化场景, 针对使用场景提供定制化方案' (Suitable for customized scenarios, provides customized solutions for usage scenarios). To the right, there's a '阿里云售后' (Aliyun After-sales) section with a QR code and a '帮助文档' (Help Documentation) section with links to various EIAM-related documents.

Click EIAM Instance List and open the free version.

This screenshot shows the 'EIAM 实例列表' (EIAM Instance List) page. The left sidebar has a link to 'EIAM 实例列表'. The main area has a table with columns: '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), '实例开放接口域名' (Instance Open Interface Domain Name), and '操作' (Operations). A large red-bordered button labeled '开通免费版' (Launch Free Edition) is visible. At the bottom, there are navigation buttons for '上一页' (Previous Page) and '下一页' (Next Page).

An instance will be created and run automatically after opening. Click on the instance name or the Manage button to enter the IDaaS management console.

The screenshot shows the EIAM Instance List page. At the top, there is a navigation bar with tabs like '工作台' (Workbench) and '华东2 (上海)' (East China 2 (Shanghai)). Below the navigation bar is a search bar with placeholder text '搜索...'. To the right of the search bar are links for '费用' (Cost), '工单' (Ticket), 'ICP 备案' (ICP Record Filing), '企业' (Enterprise), '支持' (Support), 'App', and other icons. On the left, there is a sidebar with sections like '应用身份管理' (Application Identity Management), '概览页' (Overview Page), 'EIAM 实例列表' (EIAM Instance List), 'CIAM 实例列表' (CIAM Instance List), '安全认证' (Security Authentication), '产品文档' (Product Documentation), '联系我们' (Contact Us), and '专家服务' (Expert Services). The main content area is titled 'EIAM 实例列表' (EIAM Instance List). It contains a table with columns: 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 Users), 到期时间 (Expiration Time), 产品版本 (Product Version), 用户登录页地址 (User Login Page Address), 实例开放接口域名 (Instance Open Interface Domain Name), and 操作 (Operations). A single row is visible in the table, showing 'idaas-cn-shanghai' as the instance name, '运行中' (Running) as the status, '免费版' (Free Edition) as the specification, '100' as the max users, 'V1.9.6-GA' as the product version, and several blurred URLs as the login and interface domains. A red box highlights the '管理' (Manage) button in the operations column for this row. Below the table are navigation buttons for '上一页' (Previous Page), '下一页' (Next Page), and a page number '1'.

After entering the IDaaS management console, click Add Application, search for SAML, and click Add Application.

The screenshot shows the '添加应用' (Add Application) page. The left sidebar has sections like '概览', '快速入门', '应用' (with '添加应用' highlighted in a red box), '机构及组', '账户管理', '分类管理', '认证', '授权', '权限系统', '应用授权', '审计', '其它管理', and '设置'. The main content area has tabs for '全部' (All), '标准协议' (Standard Protocols), and '定制模板' (Custom Templates). A search bar at the top has the text 'SAML' entered. Below the search bar is a table with columns: 应用图标 (Application Icon), 应用名称 (Application Name), 应用ID (Application ID), 标签 (Tags), 描述 (Description), 应用类型 (Application Type), and 操作 (Operations). The table lists several applications: 云安全访问服务SASE (plugin\_saml\_csas), 阿里云RAM-用户SSO (plugin\_allyun), 阿里云RAM-角色SSO (plugin\_allyun\_role), 阿里邮箱 (plugin\_allymail), WordPressSaml (plugin\_wordpress\_saml), SAML (plugin\_saml), and GitLab (plugin\_saml\_gitlab). Each application entry includes a brief description and a '添加应用' (Add Application) button, which is highlighted with a red box for the 'SAML' and 'GitLab' entries.

Click Add SigningKey.

## 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					

Fill in all required information and submit.

## 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
<input type="button" value="提交"/>	<input type="button" value="取消"/>

Select the added SigningKey.

## 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>

Fill in all the required information below and submit.

- IDP IdentityId: Keep the same as Issuer URL in Casdoor.
- SP Entity ID & SP ACS URL(SSO Location): Now fill in whatever you want. After completing the configuration of Casdoor, you need to come to modify.
- Assertion Attribute: Directly fill in as username.
- Account Association Mode: Account Association

## 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)

# Account authorization & association

After the application is successfully added, an authorization prompt will pop up.  
Do not authorize it now, add an account and then authorize it.

Go to Organizations and Groups and click on New Account.

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。  
Below this, there is a section titled '组织架构' (Organization Structure) with a sub-section '查看详情' (View Details). A red box highlights the '新增账户' (Add New Account) button. To the right, there is a search bar and a table listing accounts. The table has columns: 编号 (Number), 账户名称 (Account Name), 显示名称 (Display Name), 类型 (Type), 目录 (Directory), and 操作 (Operations). One account is listed: idaas\_manager (显示名称: 默认管理员, 类型: 自建账户, 目录: /). At the bottom of the table, there are buttons for '修改' (Modify), '账户同步' (Account Sync), and '同步记录' (Sync Record). The page footer shows pagination information: 共 1 条, 1/1 页, 10 条/页, 跳至 1 页.

Fill in all required information and submit.

## 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

Go to Application Authorization, select the accounts you want to authorize and click Save.

The screenshot shows the 'Application Authorization' section of the Alibaba Cloud Management Console. On the left sidebar, under the 'Authorization' category, 'Application Authorization' is 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 'Save' button is at the bottom of the table.

Go to the Application List, click View application sub-accounts, and then click Add account association.

The screenshot shows the 'Application List' section of the Alibaba Cloud Management Console. Under the 'Application' category in the sidebar, 'Application List' is highlighted with a red box. The main panel shows a detailed view of the application 'CASDOOR-SAML'. In the 'Authorization' tab, there is a 'Details' link for the account 'casdoor', which is also highlighted with a red box. The page includes tabs for 'Application Information', 'Authentication Information', 'Account Information - Sync', and 'API'.

The screenshot shows the Alibaba Cloud application management interface. On the left, there's a sidebar with categories like Application Catalog, Add Application, Accounts, Institutions & Groups, Account Management, Classification Management, Authentication, Authentication Sources, RADIUS, Certificate Management, Authorization, System Authorization, and Application Authorization. The main area has tabs for Application Catalog and Accounts. A modal window titled 'Add Account Association' is open, with a red box highlighting the 'Add Account Association' button. The modal contains information about sub-accounts and examples of how they relate to the main account.

Fill in the primary and sub accounts that need to be associated and click Save.

The primary account exists in IDaaS, and the sub account is the ID of the user in Casdoor.

This is a screenshot of the 'Add Account Association' dialog box. It has two input fields: one for the primary account ('Primary Account') containing 'casdoor' and another for the secondary account ('Sub Account') containing '52908237-fa4c-4681-b636-a6afce22fb2e'. At the bottom are two buttons: a blue 'Save' button and a white 'Cancel' button.

## Export IDaaS Metadata

Go to the Application List, click View Application Details and click Export IDaaS SAML Metadada.

The screenshot shows the Aliyun Idaas application management interface. On the left, there is a sidebar with various management categories like Application, Account, Authentication, Authorization, Audit, and Others. 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), and 应用ID (Application ID). One row is selected, showing the icon for 'CASDOOR-SAML', the name 'CASDOOR-SAML', and the ID 'idaas-cn-shanghai-[REDACTED]\_saml'. To the right, a detailed view for '应用详情 (CASDOOR-SAML)' is displayed, containing tabs for '图标' (Icon), '应用信息' (Application Information), '认证信息' (Authentication Information), '授权信息' (Authorization Information), and '审计信息' (Audit Information). The '应用信息' tab is active, showing 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), and 'IDaaS发起地址' (IDaaS initiation address). The '认证信息' tab shows 'SigningKey' (3322747020095790430(CN=CASDOOR-TEST)), 'NameIdFormat' (urn:oasis:names:tc:SAML:2.0:nameid-format:transient), 'SP ACS URL' (http://localhost), and 'IDP IdentityId' (CASDOOR). The '授权信息' tab shows '授权' (Authorization) and '授权与人员组织的授权关系' (Authorization relationship with personnel and organization). The '审计信息' tab shows '查看日志' (View logs) and '查看同步记录' (View sync records). At the bottom of the page, there is a large red box highlighting the 'IDaaS元配置文件' (IDaaS metadata file) link under the 'IDP IdentityId' section.

# Configure in Casdoor

Create a new provider in Casdoor.

Select category as **SAML**, type as **Aliyun Idaas**. Copy the content of metadata and paste it to the **Metadata** input. The values of **Endpoint**, **IdP** and **Issuer URL** will be generated automatically after clicking the **Parse** button.

Name ⓘ :	casdoor-idaas	
Display name ⓘ :	casdoor-idaas	
Category ⓘ :	SAML	
Type ⓘ :	Aliyun IDaaS	
Client ID ⓘ :		
Client secret ⓘ :		
Metadata ⓘ :	<pre>&lt;md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aliyunidaas.com/charon/api/applications/plugin_idaas/charon"&gt;     &lt;md:SPSSOServiceBinding Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aliyunidaas.com/charon/api/applications/plugin_idaas/charon"/&gt; &lt;/md:SingleSignOnService&gt; &lt;/md:IDPSSODescriptor&gt; &lt;/md:EntityDescriptor&gt;</pre>	
<input style="margin-right: 10px;" type="button" value="Parse"/> <span style="color: green;">Success</span>		
Endpoint ⓘ :	<a href="https://dvmoykbkx.login.aliyunidaas.com/enduser/api/application/plugin_saml/idaas-cn-shanghai">https://dvmoykbkx.login.aliyunidaas.com/enduser/api/application/plugin_saml/idaas-cn-shanghai</a>	
IdP ⓘ :	MIIByzCAVcBgAwIBAgIILhzEz2NMHV4wDQYJKoZIhvNAQEFBQAwNjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTBlJlaWppbmcxFTATBgNVBAMTDENBU0RPTIItVEVTVDaeFw0yMTEyMDkwNzEyMTFaFw0yNDEyMDgwNzEyMTFaMDYxCzAJE	
Issuer URL ⓘ :	CASDOOR	
SP ACS URL ⓘ :	<a href="http://localhost:8000/api/acs">http://localhost:8000/api/acs</a>	<input type="button" value="Copy"/>
SP Entity ID ⓘ :	<a href="http://localhost:8000/api/acs">http://localhost:8000/api/acs</a>	<input type="button" value="Copy"/>
Provider URL ⓘ :	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>	

Copy the SP ACS URL and the SP Entity ID and click the Save button.

Edit the application you want to configure in Casdoor. Select the provider just added and click the button **Save**.

Providers	②
Providers	Add
Name	
casdoor-idaas	SAML
Category	Type
canSignUp	canSignIn
canUnlink	prompted
Action	
Preview	②
Test signup page.	Test signin page.

# Modify SAML application in Aliyun IDaaS

Disable the application and then click **Modify Application**.

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 'Application List' and contains a table with columns: Application Icon, Application Name, Application ID, Device Type, Status, Two-factor Authentication Status, and Operations. One row in the table is highlighted with a red box around its 'Status' column, which has a toggle switch. Below the table, there are tabs for Application Information, Authentication Information, Account Information - Sync, Account Information - Sub-account, Authorization Information, Audit Information, and API. At the bottom, there are pagination controls showing '1' of 1 page.

Fill in SP Entity ID and SP ACS URL(SSO Location) with the content copied in Casdoor. Submit and enable application.

## 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

## Validate the effect

Go to the application you just configured and you can find that there is an icon in the login page.

Click the icon and jump to the Aliyun IDaaS login page, and then successfully login to the Casdoor after authentication.



---

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.

---

# Keycloak

The JBoss [KeyCloak](#) system is a widely used and open-source identity management system that supports integration with applications via SAML and OpenID Connect. It also can operate as an identity broker between other providers such as LDAP or other SAML providers and applications that support SAML or OpenID Connect.

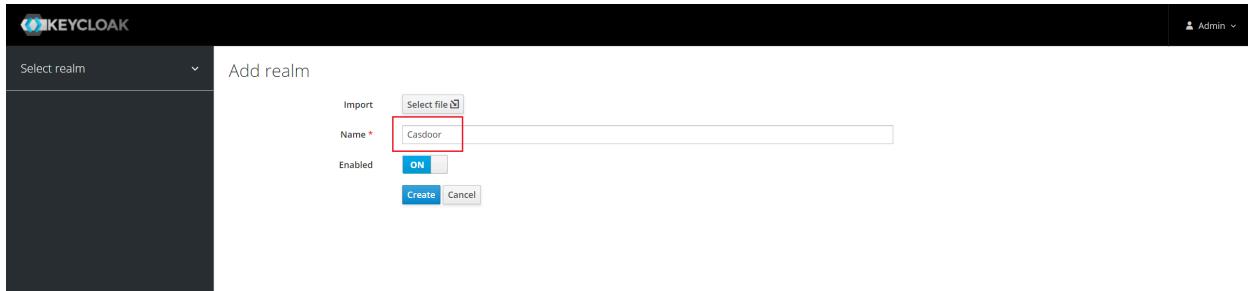
The following is an example of how to configure a new client entry in KeyCloak and configure Casdoor to use it to permit UI login by KeyCloak users that are granted access via KeyCloak configuration.

## Configure Keycloak

Some config choices and assumptions specifically for this example:

- Let's assume that you are running Casdoor as dev mode locally. Casdoor UI is available at: `http://localhost:7001` and server is available at `http://localhost:8000`. Replace with the appropriate url as needed.
- Let's assume that you are running Keycloak locally. Keycloak UI is available at: `http://localhost:8080/auth`.
- Based on that, the SP ACS URL for this deployment will be: `http://localhost:8000/api/acs`.
- Our SP Entity ID will use the same url: `http://localhost:8000/api/acs`.

Use the default realm or create a new realm.



## Add a client entry in Keycloak

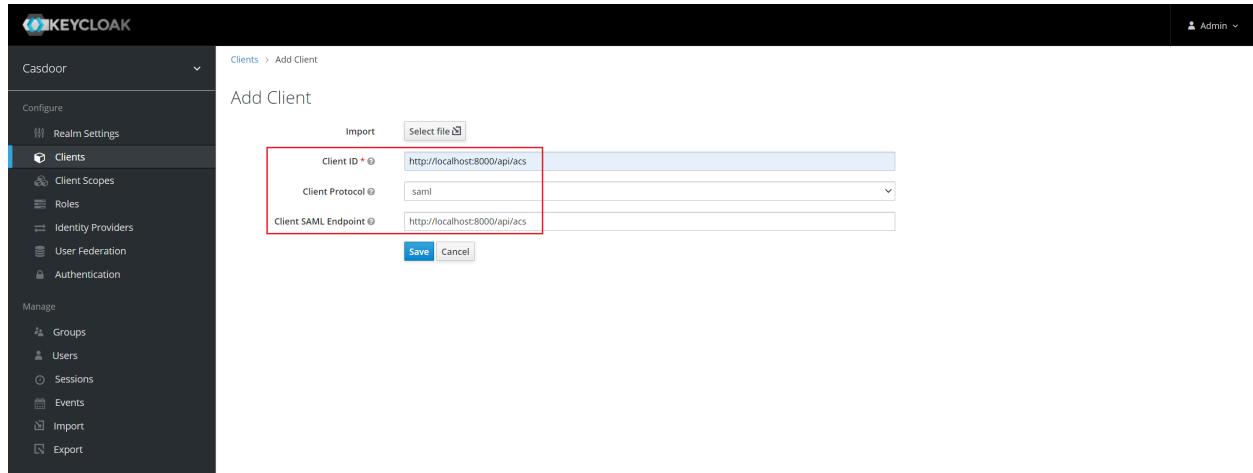


See more details about Keycloak Clients in [Keycloak documentation](#).

Click Clients in the menu and then click Create to go to the Add Client page. Fill in as below.

- Client ID: `http://localhost:8000/api/acs` - This will be the SP Entity ID used in the Casdoor configuration later.
- Client Protocol: `saml`.
- Client SAML Endpoint: `http://localhost:8000/api/acs`. - This URL is where you want the Keycloak server to send SAML requests and responses.

Generally, applications have one URL for processing SAML requests. Multiple URLs can be set in the Settings tab of the client.



The screenshot shows the Keycloak administration interface. On the left, there's a sidebar with a 'Clients' section highlighted. The main area is titled 'Add Client'. It contains three input fields: 'Client ID' (set to 'http://localhost:8000/api/acs'), 'Client Protocol' (set to 'saml'), and 'Client SAML Endpoint' (set to 'http://localhost:8000/api/acs'). Below these fields are 'Save' and 'Cancel' buttons. A red box highlights the 'Client ID' field.

Click Save. This action creates the client and brings you to the Settings tab.

The following list part of settings:

1. **Name** - Casdoor. This is only used to display a friendly name to Keycloak users in the KeyCloak UI. You can use any name you like.
2. **Enabled** - Select on.
3. **Include Authn Statement** - Select on.
4. **Sign Documents** - Select on.
5. **Sign Assertions** - Select off.
6. **Encrypt Assertions** - Select off.
7. **Client Signature Required** - Select off.
8. **Force Name ID Format** - Select on.
9. **Name ID Format** - Select username.
10. **Valid Redirect URIs** - Add http://localhost:8000/api/acs.
11. **Master SAML Processing URL** - http://localhost:8000/api/acs.
12. **Fine Grain SAML Endpoint Configuration**
  - i. **Assertion Consumer Service POST Binding URL** -

`http://localhost:8000/api/acs.`

ii. Assertion Consumer Service Redirect Binding URL -

`http://localhost:8000/api/acs.`

Save the configuration.

KEYCLOAK Admin

Clients > http://localhost:8000/api/acs

**Http://localhost:8000/api/acs**

Configure Realm Settings Clients

**Settings** Roles Client Scopes Mappers Scope Sessions Offline Access Clustering Installation

Client ID: http://localhost:8000/api/acs  
 Name: Casdoor  
 Description:  
 Enabled: ON  
 Always Display in Console: OFF  
 Consent Required: OFF  
 Login Theme:  
 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:  
 Valid Redirect URIs: http://localhost:8000/api/acs  
 Base URL:  
 Master SAML Processing URL: http://localhost:8000/api/acs  
 IDP Initiated SSO URL Name:  
 IDP Initiated SSO Relay State:  
**Fine Grain SAML Endpoint Configuration**  
 Assertion Consumer Service POST Binding URL: http://localhost:8000/api/acs  
 Assertion Consumer Service Redirect Binding URL: http://localhost:8000/api/acs  
 Logout Service POST Binding URL:  
 Logout Service Redirect Binding URL:  
 Logout Service ARTIFACT Binding URL:  
 Artifact Binding URL:  
 Artifact Resolution Service:  
**Advanced Settings**  
**Authentication Flow Overrides**

Save Cancel



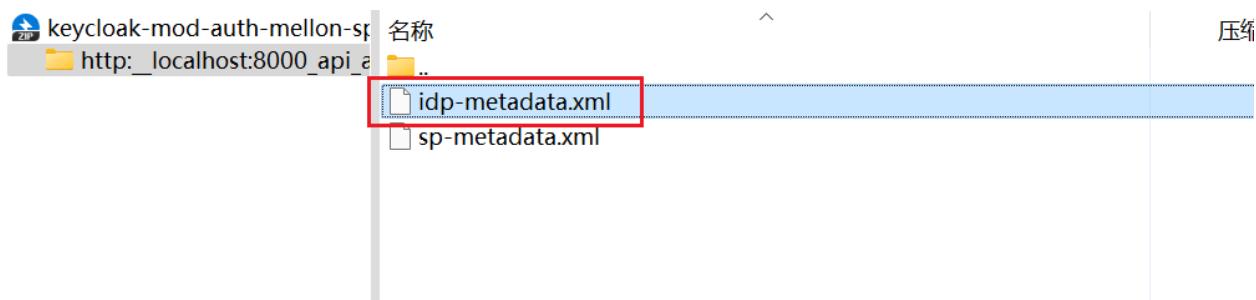
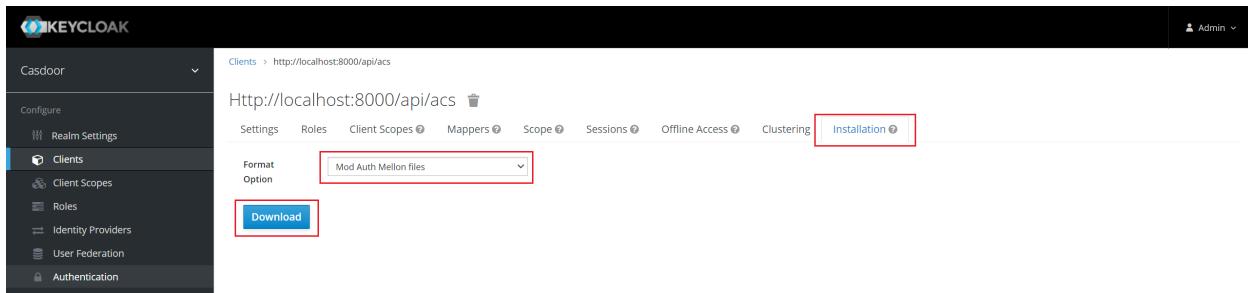
TIP

If you want to sign authn request, you need to enable the Client Signature Required option and upload the certificate generated by yourself. The private key and certificate using in Casdoor, `token_jwt_key.key` and `token_jwt_key.pem` are located in the `object` directory. In Keycloak, you need to click the Keys tab, click Import button, select Archive Format as Certificate PEM and upload the certificate.

Click Installation tab.

For the Keycloak <= 5.0.0, select Format Option - SAML Metadata IDPSSODescriptor and copy the metadata.

For Keycloak 6.0.0+, select Format Option - Mod Auth Mellon files and click Download. Unzip the downloaded.zip, locate `idp-metadata.xml` and copy the metadata.



# Configure in Casdoor

Create a new provider in Casdoor.

Select category as **SAML**, type as **Keycloak**. Copy the content of metadata and paste it to the **Metadata** input. The values of **Endpoint**, **IdP** and **Issuer URL** will be generated automatically after clicking the **Parse** button. Finally click the button **Save**.



TIP

If you enable the **Client Signature Required** option in Keycloak and upload the certificate, please enable the **Sign request** option in Casdoor.

Name ② :	keycloak-casdoor
Display name ② :	keycloak-casdoor
Category ② :	SAML
Type ② :	Keycloak
Client ID ② :	
Client secret ② :	
Sign request ② :	<input checked="" type="checkbox"/>
Metadata ② :	<pre>&lt;md:EntityDescriptor xmlns="urn:oasis.names.tc:SAML2.0:metadata" xmlns:md="urn:oasis.names.tc:SAML2.0:metadata" xmlns:saml="urn:oasis.names.tc:SAML2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realm/casdoor"&gt;&lt;md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML2.0:protocol"&gt;&lt;md:KeyDescriptor use="signing"&gt; &lt;ds:KeyInfo&gt;&lt;ds:KeyName&gt;zqpn-3k7gj-na5Zc3uPDl7bp-4wYmBwMfPzvqJHAY&lt;/ds:KeyName&gt;&lt;ds:X509Data&gt; &lt;ds:X509Certificate&gt;MIICnTCAYUCBgF9pAmxSDANBgkqhkiG9w0BAQsFADASMRawDgYDVQQDDAdjYXNkb29yMB4XDtxMTIxMDExMDg1OFoXDTMxMTIxMDExMTAxOFowEjEQMA4GA1UEAwwHY2FzZG9vcjCCASiwDQYJKoZIhvNA &lt;/ds:X509Data&gt;&lt;/ds:KeyInfo&gt;&lt;/md:KeyDescriptor&gt;&lt;/md:IDPSSODescriptor&gt;&lt;/md:EntityDescriptor&gt;</pre> <input type="button" value="Parse"/>
Endpoint ② :	http://localhost:8080/auth/realm/casdoor/protocol/saml
IdP ② :	MIICnTCAYUCBgF9pAmxSDANBgkqhkiG9w0BAQsFADASMRawDgYDVQQDDAdjYXNkb29yMB4XDtxMTIxMDExMDg1OFoXDTMxMTIxMDExMTAxOFowEjEQMA4GA1UEAwwHY2FzZG9vcjCCASiwDQYJKoZIhvNAQEBBQADggEPADCCAQ:
Issuer URL ② :	http://localhost:8080/auth/realm/casdoor
SP ACS URL ② :	http://localhost:8000/api/acs
SP Entity ID ② :	http://localhost:8000/api/acs
Provider URL ② :	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>

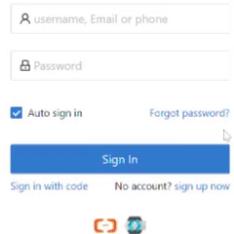
Edit the application you want to configure in Casdoor. Select the provider just added and click the button **Save**.

Providers <small>(1)</small>		Add	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
Name									
casdoor-idaas			SAML						  
keycloak-casdoor			SAML						  

## Validate the effect

Go to the application you just configured and you can find that there is a Keycloak icon in the login page.

Click the icon and jump to the Keycloak login page, and then successfully login to the Casdoor after authentication.



The screenshot shows the Casdoor login interface. At the top, there is a search bar labeled "username, Email or phone" and a password field labeled "Password". Below these fields are two buttons: "Auto sign in" (with a checked checkbox) and "Forgot password?". In the center is a large blue "Sign In" button. Below the button, there are links for "Sign in with code" and "No account? sign up now". At the bottom right of the form, there are icons for SAML and OpenID Connect.

# Payment



Add Wechat OAuth provider to your application



> Providers > Payment >

Alipay

# Alipay

# WeChatPay

## Step1. Deploy Casdoor

Firstly, the 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, you need to ensure:

- Open your favorite browser and visit <http://localhost:8000>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2. Configure payment callback notification address

Before that, please log in to the WeChat Pay Merchant Platform. In order for Casdoor to receive payment result notifications, you need to set a callback notification address in the WeChat Pay Merchant Platform.

- In Merchant Dashboard, go to `Development Configuration` → `Payment Configuration`.
- Find the `Callback Notification Address` setting, and click the `Modify`

button.

- Fill in the payment callback notification address of the Casdoor instance. For example:

```
https://your-casdoor-instance.com/api/wechat-payment-callback
```

## Step3. Configure API Security

### Get APIv3 key

To ensure the security of API calls, you need to configure API security settings in the WeChat Pay Merchant Platform.

Log in the [WeChat merchant platform](#) → [Account center](#) → [Account settings](#) → [API security](#) → [APIv3 key](#) → [set up](#)

### Get the serial number of the merchant certificate

It is also necessary to obtain the serial number of the merchant certificate. The following are the steps to obtain it.

Log in the [WeChat merchant platform](#) → [Account center](#) → [Account settings](#) → [API security](#) → [API certificate management](#) → copy the serial number.

You can refer to the [WeChat payment merchant ID query guide](#), [APIv3 key settings](#) and [How to view the certificate serial number](#) for help.

## Step4. Add payment provider

Select the WeChat Pay as the Payment type.

New Provider    Save    Save & Exit    Cancel

Name ? : wechat-provider

Display name ? : New wechat-provider

Organization ? : admin (Shared)

Category ? : **Payment**

Type ? : WeChat Pay

Client ID ? : Alipay  
GC

Client secret ? : PayPal  
**WeChat Pay**

Provider URL ? : <https://github.com/organizations/xxx/settings/applications/123456/>

## Get Payment URL

Log in the [WeChat merchant platform](#) → [Commodity centered](#) → [Development arrangement](#) → [payment arrangements](#) → [Payment URL](#) → [copy](#)

## Fill the necessary information in Casdoor

There are four required fields, `Client ID`, `Client secret`, `appId`, `Provider URL`. The relationship corresponding to the Azure Blob account is as follows:

Name	Name in WeChat Pay	is required
Client ID	merchant ID	required
Client secret	APIv3 key	required
appId	appId	required
Provider URL	Payment URL	required

The acquisition of `merchant ID` and `APIv3 key` is as mentioned before. For `appId`, see [here](#) for more help.

Edit Provider Save Save & Exit

Name ? : wechat-provider

Display name ? : New wechat-provider

Organization ? : admin (Shared)

Category ? : Payment

Type ? : WeChat Pay

Client ID ? e75c5c9f0056d80849a7 Your merchant ID

Client secret ? \*\*\* Your APIv3 key

appId ? appldadaasdaffafgaass Your appId

Provider URL ? https://api.mch.weixin.qq.com/pay/unifiedorder Your Payment URL

Save Save & Exit

## Step5. Add WeChat Cert

In this step, you need two required fields, `serial number`, `private key`.

How to obtain the serial number has been stated in the third step.

To get `private key`, click [here](#) for help.

Edit Cert Save Save & Exit

Name ? : cert\_wechat  
x509

Display name ? : New Cert - wechat

Scope ? : JWT

Type ? : x509

Crypto algorithm ? : RS256

Bit size ? : 4096

Expire in years ? : 20

Your merchant certificate serial number

Certificate ? : Copy certificate Download certificate

```
-----BEGIN CERTIFICATE-----
MIIE2TCAsGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMCYxDjAMBg
NVBAoTBWFk
bWluMRQwEgYDVQQDAjZXJ0X2dmamRqZzAeFw0yMzA0MTAxMTEy
NTIaFw00MzA0
-----END CERTIFICATE-----
```

Private key ? : Your private key Copy private key Download private key

```
-----BEGIN RSA PRIVATE KEY-----
MIJKgIBAAKCAgEA4Fn+yt0cUCUlrMx/zXd0JnEbRCxBqo8weFf1LgBKi2h
6R1vD
cZfFRRvlHA/Oktl5nKXQPuQzwuxHy6Cz2HRoAR0ayNVDcASJTWOtOF/
z0vYRKT/
-----END RSA PRIVATE KEY-----
```

## Step6. Add WeChat Payment Provider in Products

Currency ? : USD

Price ? : 300

Quantity ? : 99

Sold ? : 10

Payment providers ? : wechat-provider x

The payment provider you just add

wechat-provider

Return URL ? : ↲

The payment callback notification address same in WeChat merchant platform

State ? : Published

Preview ? : Test buy page..

Final effect:

Buy Product					
Name	New Product - 4emdrq				
Detail		Tag	Casdoor Summit 2022	SKU	product_4emdrq
Image	 Casdoor				
Price	\$300 (USD)	Quantity	99	Sold	10
Pay	 WeChat Pay				

## What's more

You can explore the following projects/docs to learn more about WeChat Pay.

- [wechatpay-apiv3-go-sdk](#)
- [Wechat payment development document](#)

# Captcha

## Overview

Add a captcha to your application

## Default

Using Casdoor default captcha in your application

## reCAPTCHA

Add reCAPTCHA to your application

## hCaptcha

Add hCaptcha to your application

 **Aliyun Captcha**

Add Aliyun Captcha to your application

 **Cloudflare Turnstile**

Add Cloudflare Turnstile to your application

# Overview

Casdoor can be configured to support different captchas to check whether the operation is made by human. If you add a captcha provider and applied it in the application, when the user logins, registers or forgets password and needs to send a code, then a captcha check dialog will appear to check whether the operation is made by human.

Now, Casdoor supports many captcha providers. Here are the providers Casdoor supporting:

Default	reCAPTCHA	hCaptcha	Aliyun Captcha	Cloudflare Turnstile

We will show you how to apply a captcha and add it to Casdoor.

## Add a captcha provider

1. Navigate to your Casdoor index page
2. Click [Providers](#) in the top bar
3. Click [Add](#), then you can see a new provider in the list top
4. Click the new provider to modify it
5. Select [Captcha](#) in [Category](#)

6. Choose the Captcha provider you need in `Type`
7. Fill the most important information, different captcha providers have different information that needs to be filled in

## Applied in application

1. Click `Applicaton` in the top bar and choose one application to edit.
2. Click provider add button, and select the provider you just added.
3. Done!

# Default

Default captcha implements generation and verification of image. A default captcha image is the sequence of digits 0-9 with the defined length(5).

## Configure in Casdoor

Create a new provider in Casdoor.

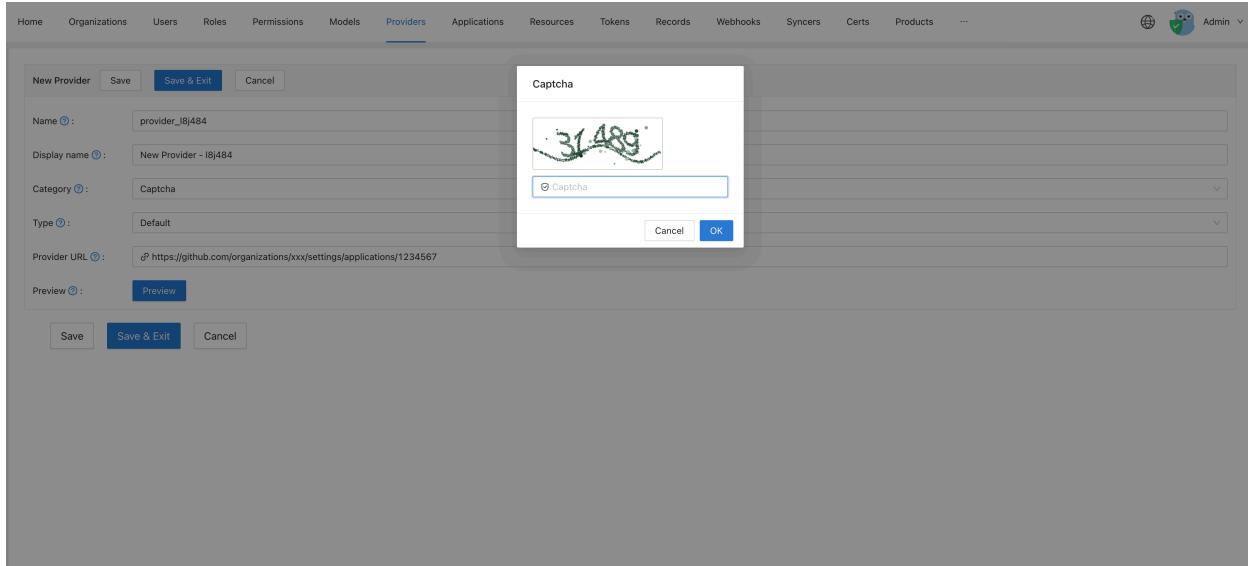
Select category as Captcha , type as Default .

The screenshot shows the Casdoor web interface with the 'Providers' tab selected. A modal window is open for creating a new provider, titled 'New Provider'. The form fields are as follows:

Name	Value
Name (必填)	provider_I8j484
Display name (必填)	New Provider - I8j484
Category (必填)	Captcha
Type (必填)	Default
Provider URL (可选)	<a href="https://github.com/organizations/xxx/settings/applications/1234567">https://github.com/organizations/xxx/settings/applications/1234567</a>
Preview (必填)	Preview

At the bottom of the modal, there are three buttons: 'Save' (gray), 'Save & Exit' (blue), and 'Cancel' (gray). Above the modal, there are buttons for 'New Provider' (gray), 'Save' (gray), 'Save & Exit' (blue), and 'Cancel' (gray). The top navigation bar includes links for Home, Organizations, Users, Roles, Permissions, Models, Applications, Resources, Tokens, Records, Webhooks, Syncers, Certs, Products, and Admin.

And you can click Preview button to preview the style of this captcha.



## Applied in application

Edit the application you want to configure in Casdoor. Select the provider just added. There are three kinds of rules:

- **Always** Always turned on human-machine verification when login.
- **None** Never require human-machine verification, the account will be blocked when it attempted to login into the same application with wrong password for the 5th time within 15 minutes. And it will be unblocked after 15 minutes.
- **Dynamic** After 5 failed login attempts, the account will not be blocked but instead, human-machine verification will be required.

Providers		Add	Name	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Rule	Action
provider_4olfdm	Captcha		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Always	
provider_casdoor_github	OAuth		<input checked="" type="checkbox"/>								
provider_casdoor_google	OAuth		<input checked="" type="checkbox"/>								

We also provide a demo video to demonstrate the differences in rules, which we hope will be helpful to you



# reCAPTCHA

reCAPTCHA is provided by Google. And we use reCAPTCHA v2 Checkbox . You can see more details from this [link](#).

## Create an API key pair

To start using reCAPTCHA, you need to [sign up for an API key pair](#) for your site. The key pair consists of a site key and secret key. The site key is used to invoke reCAPTCHA service on your site or mobile application. The secret key authorizes communication between your application backend and the reCAPTCHA server to [verify the user's response](#).

First, choose the [type of reCAPTCHA](#) and then fill in authorized domains or [package names](#). After you have accepted the terms of service, click [Register](#) to get a new API key pair.

The screenshot shows the Google reCAPTCHA registration interface. At the top, there's a blue header bar with the text "Google reCAPTCHA". Below it, a light blue bar says "← Register a new site". A yellow bar at the top of the main content area says "Get unlimited assessments using reCAPTCHA Enterprise". The main form has sections for "Label" (set to "reCaptcha"), "reCAPTCHA type" (set to "reCAPTCHA v2"), "Domains" (set to "casdoor.org"), and "Owners" (set to "resultlee@gmail.com"). There's also a checked checkbox for "Accept the reCAPTCHA Terms of Service".

Then you can get a site key and a secret key.

The screenshot shows the "Adding reCAPTCHA to your site" page. It displays a message that "'reCaptcha' has been registered." Below this, there are two sections: "Use this site key in the HTML code your site serves to users." and "Use this secret key for communication between your site and reCAPTCHA.". Each section contains a "COPY SITE KEY" button and a text input field containing a long string of characters. At the bottom, there are "GO TO SETTINGS" and "GO TO ANALYTICS" buttons.

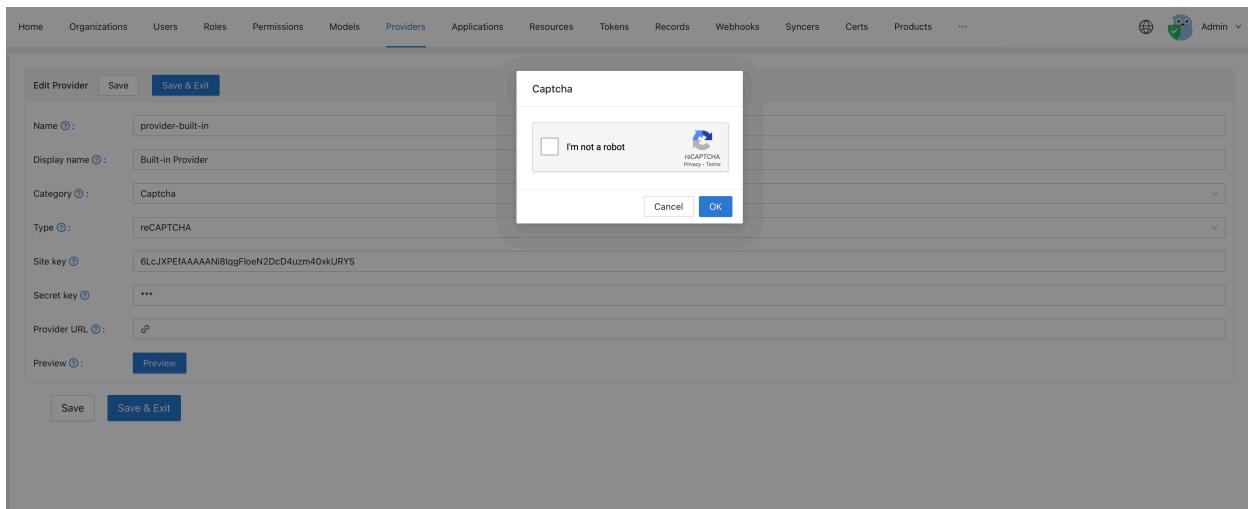
## Configure in Casdoor

Create a new provider in Casdoor.

Select category as **Captcha** , type as **reCAPTCHA** . And you need to fulfill the site key and the secret key which is created by last step.

The screenshot shows the 'New Provider' configuration page for reCaptcha. The provider type is set to 'reCAPTCHA'. The 'Site key' and 'Secret key' fields are filled with placeholder values. A 'Provider URL' field contains a link to GitHub's organization settings. A 'Preview' button is visible at the bottom. The interface includes standard save and cancel buttons.

And you can click Preview button to preview the style of this captcha.



## Applied in application

Edit the application you want to configure in Casdoor. Select the provider just added and click the button Save.

The screenshot shows the application configuration page where the 'reCaptcha' provider is selected from a list. The table columns include Name, Category, Type, canSignUp, canSignIn, canUnlink, prompted, and Action. The 'reCaptcha' row is highlighted with a blue border.

# hCaptcha

hCaptcha is a captcha service provider which is similar to reCAPTCHA. You can see more details from this [link](#).

## Create an API key pair

To start using hCaptcha, you need to [sign up for an API key pair](#) for your site. You can find your site key on your [profile page](#).

Then you can get a site key and a secret key.

## Configure in Casdoor

Create a new provider in Casdoor.

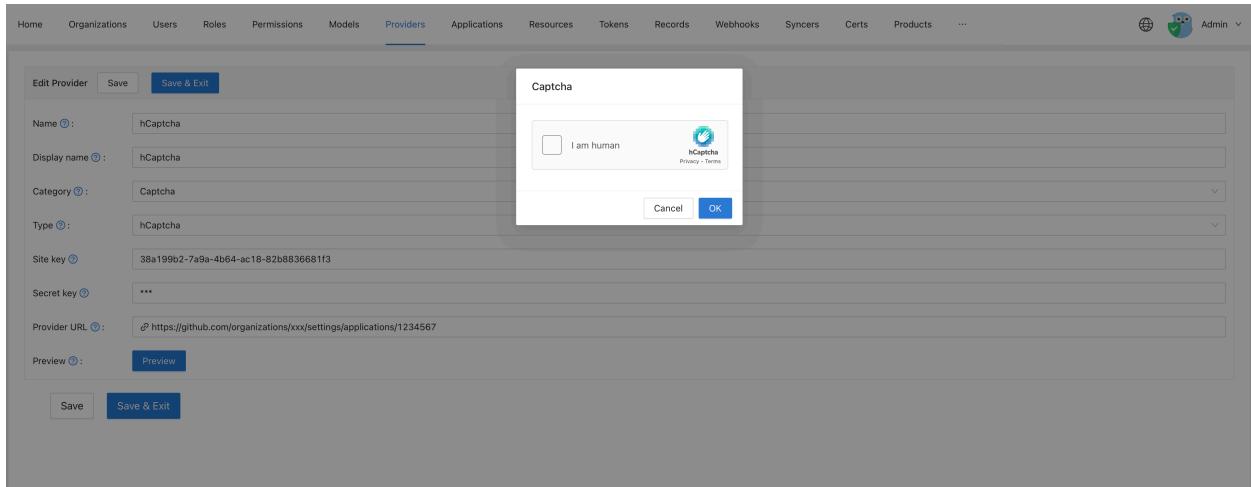
Select category as **Captcha** , type as **hCaptcha** . And you need to fulfill the site key and the secret key which is created by last step.

The screenshot shows the Casdoor web interface with the 'Providers' tab selected. A new provider is being created with the following details:

- 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/xx/settings/applications/1234567

At the bottom, there are buttons for **Save**, **Save & Exit**, and **Cancel**.

And you can click Preview button to preview the style of this captcha.



## Applied in application

Edit the application you want to configure in Casdoor. Select the provider just added and click the button Save.

Providers :	Add	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
Name	hCaptcha	Captcha						

# Aliyun Captcha

Aliyun Captcha is a captcha service provided by Aliyun. It includes two ways to verify captcha: [Sliding Validation](#) and [Intelligent Validation](#). You can see more details from this [link](#).

## Add Captcha configuration in Aliyun

Login to the [Aliyun management console](#), search and go to the Captcha Service. And click Confirm Open to enable Captcha Service.



After entering the captcha agement console, click Add configuration.

公告: 2021年3月18日起, 人机验证产品统一更名为验证码。

配置名称	appkey	scene	验证方式	业务类型	使用场景	最后更新	操作
测试验证码	F [REDACTED] B	nc_other	滑动验证	PC	其它	2022-06-20 23:47:37	自定义样式 系统代码集成
测试智能验证码	FF [REDACTED] B	lc_other	智能验证	PC	其它	2022-06-21 00:44:08	自定义样式 系统代码集成

共有2条 < 1 >

Fill in all required information and submit.

① 配置服务内容

② 系统代码集成&测试

③ 完成

配置名称:

高峰期QPS:

业务类型:  PC网页  H5 (移动端WAP + APP)

验证方式:  滑动验证  智能验证  无痕验证

使用场景:  登录  注册  活动  论坛  短信  其它

产品形态预览:

下一步

Then you can see your **Scene** and **App key** in your console.

配置名称	appkey	scene	验证方式	业务类型	使用场景	最后更新	操作
测试验证码	XXXXXXXXXXXXXXXXXXXX8B	nc_other	滑动验证	PC	其它	2022-06-20 23:47:37	自定义样式   系统代码集成
测试智能验证码	XXXXXXXXXXXXXXXXXXXX8B	lc_other	智能验证	PC	其它	2022-06-21 00:44:08	自定义样式   系统代码集成

And `Access key`, `Secret access key` is in your profile.

## Configure in Casdoor

Create a new provider in Casdoor.

Select category as `Captcha`, type as `hCaptcha`. Then select sub type: `Sliding Validation` or `Intelligent Validation`. And you need to fulfill the `Access key`, `Secret access key`, `Scene` and `App key` which are created by last step.

New Provider Save Save & Exit Cancel

Name : Aliyun\_Captcha

Display name : Aliyun\_Captcha

Category : Captcha

Type : Aliyun Captcha

Sub type : Sliding Validation

Access key : LTAI4G7CngW2Pp5pE4yS7gF

Secret access key : 3IPXXXXXXXXXXN

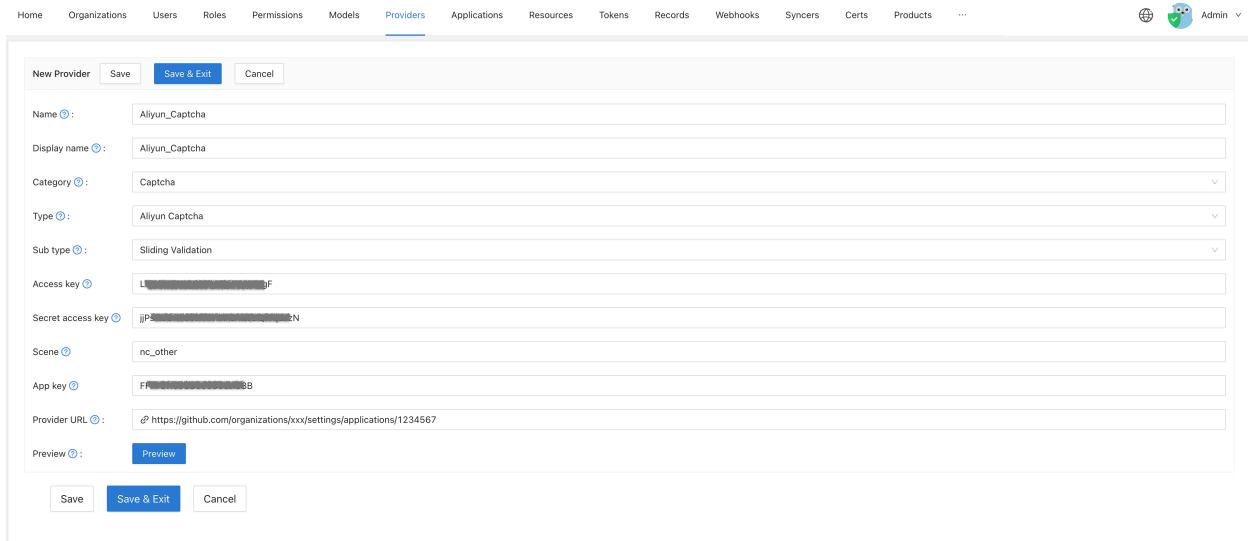
Scene : nc\_other

App key : FXXXXXXXXXXXXX8

Provider URL : <https://github.com/organizations/xxx/settings/applications/1234567>

Preview : Preview

Save Save & Exit Cancel



And you can click **Preview** button to preview the style of this captcha.

The following image is **Sliding Validation** preview:

Edit Provider Save Save & Exit

Name : Aliyun\_Captcha

Display name : Aliyun\_Captcha

Category : Captcha

Type : Aliyun Captcha

Sub type : Sliding Validation

Access key : LTAI4G7CngW2Pp5pE4yS7gF

Secret access key : \*\*\*

Scene : nc\_other

App key : \*\*\*

Provider URL : <https://github.com/organizations/xxx/settings/applications/1234567>

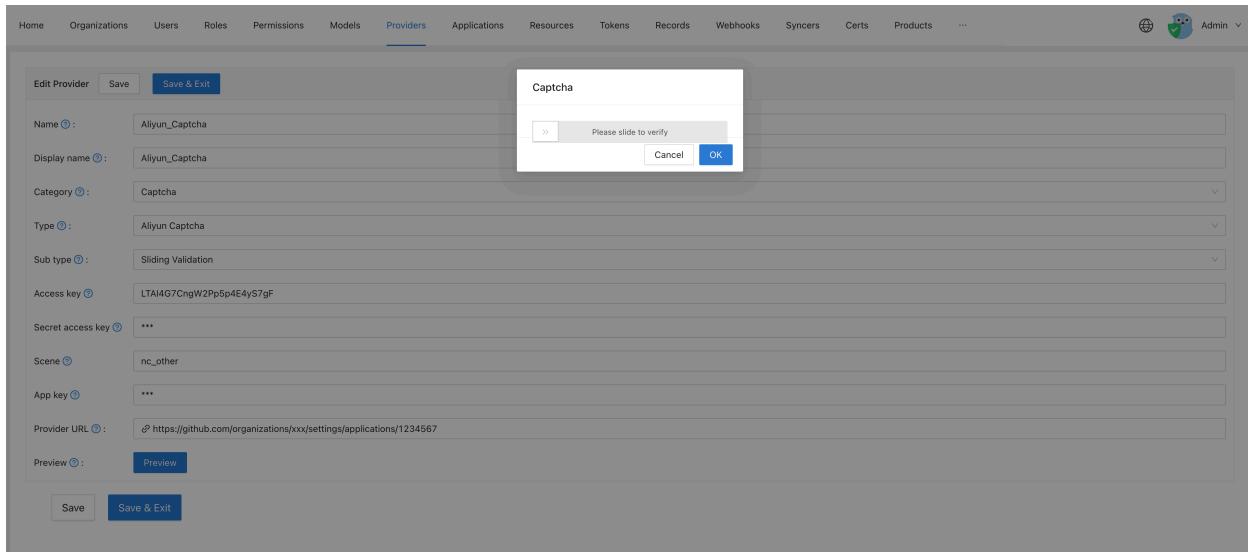
Preview : Preview

Save Save & Exit

Captcha

Please slide to verify

Cancel OK



The following image is **Intelligent Validation** preview:

The screenshot shows the Casdoor provider configuration interface. A modal window titled "Captcha" is open, prompting the user to "Click the button to start". The main configuration form contains the following fields:

- Name: Aliyun\_Captcha
- Display name: Aliyun\_Captcha
- Category: Captcha
- Type: Aliyun Captcha
- Sub type: Intelligent Validation
- Access key: LTAI4G7CngW2Pp5p4E4yS7gF
- Secret access key: ...
- Scene: ic\_other
- App key: ...
- Provider URL: https://github.com/organizations/xxx/settings/applications/1234567
- Preview: Preview

At the bottom of the configuration form are "Save" and "Save & Exit" buttons.

# Applied in application

Edit the application you want to configure in Casdoor. Select the provider just added and click the button **Save**.

The screenshot shows the Casdoor provider list table. A single row is selected, highlighting the "Name" column which contains "Aliyun\_Captcha". The table has columns for Name, Category, Type, canSignUp, canSignIn, canUnlink, prompted, and Action.

Providers	Add	Name	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
		Aliyun_Captcha	Captcha	Intelligent Validation					Up, Down, Delete

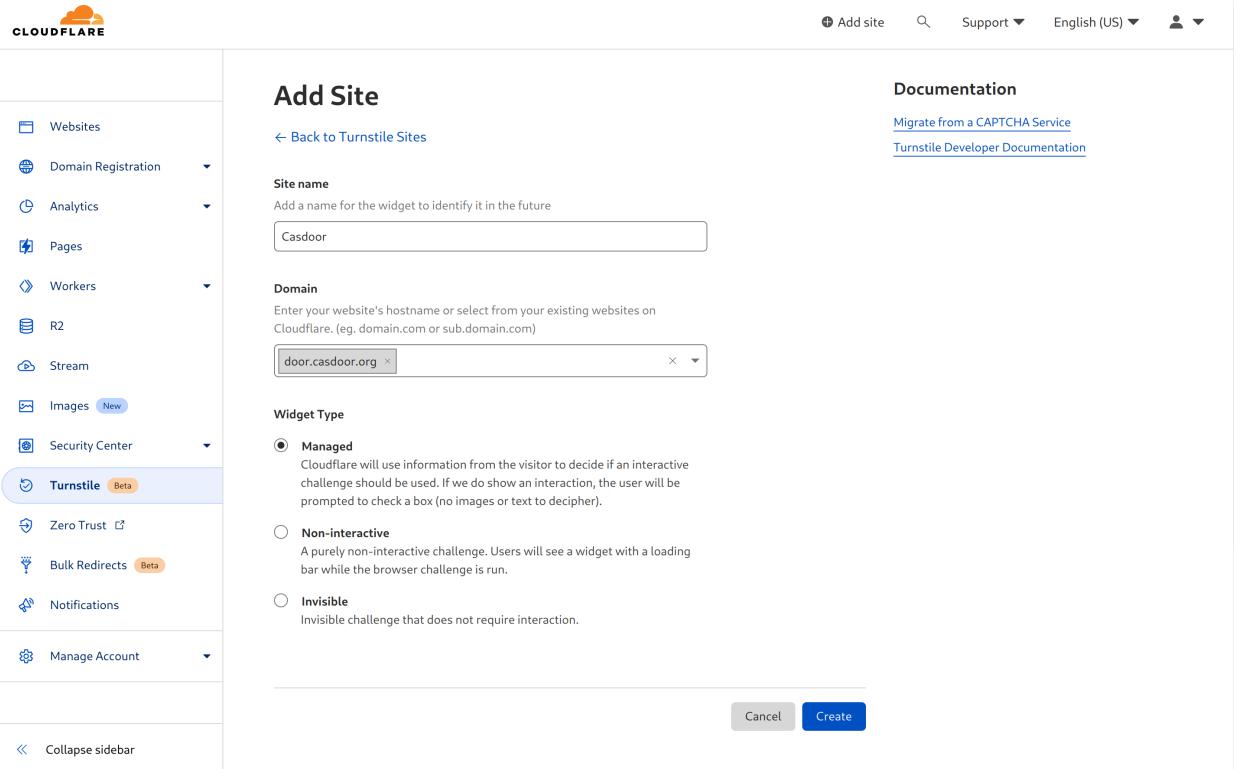
# Cloudflare Turnstile

Cloudflare Turnstile is a captcha service provided by Cloudflare, which is a user-friendly, privacy preserving alternative to captcha. You can see more details from [Turnstile Docs](#).

## Create an API key pair

To start using Cloudflare Turnstile, you need to [Create a Cloudflare account](#), navigate to the [Turnstile](#) tab on the navigation bar, and get the Site Key and Secret Key.

First, add a name for the widget to identify it in the future and enter your website's hostname. Then choose the widget type. [Managed](#) is recommended. Click [Create](#).



The screenshot shows the Cloudflare dashboard with the sidebar open. The sidebar includes options like Websites, Domain Registration, Analytics, Pages, Workers, R2, Stream, Images (New), Security Center, Turnstile (Beta), Zero Trust, Bulk Redirects (Beta), Notifications, and Manage Account. The Turnstile option is selected and highlighted with a blue border. The main content area is titled "Add Site" and shows a "Site name" field containing "Casdoor". A "Domain" field contains "door.casdoor.org". Under "Widget Type", the "Managed" option is selected. At the bottom right are "Cancel" and "Create" buttons.

**Add Site**

[← Back to Turnstile Sites](#)

**Site name**  
Add a name for the widget to identify it in the future

**Domain**  
Enter your website's hostname or select from your existing websites on Cloudflare. (eg. domain.com or sub.domain.com)

**Widget Type**

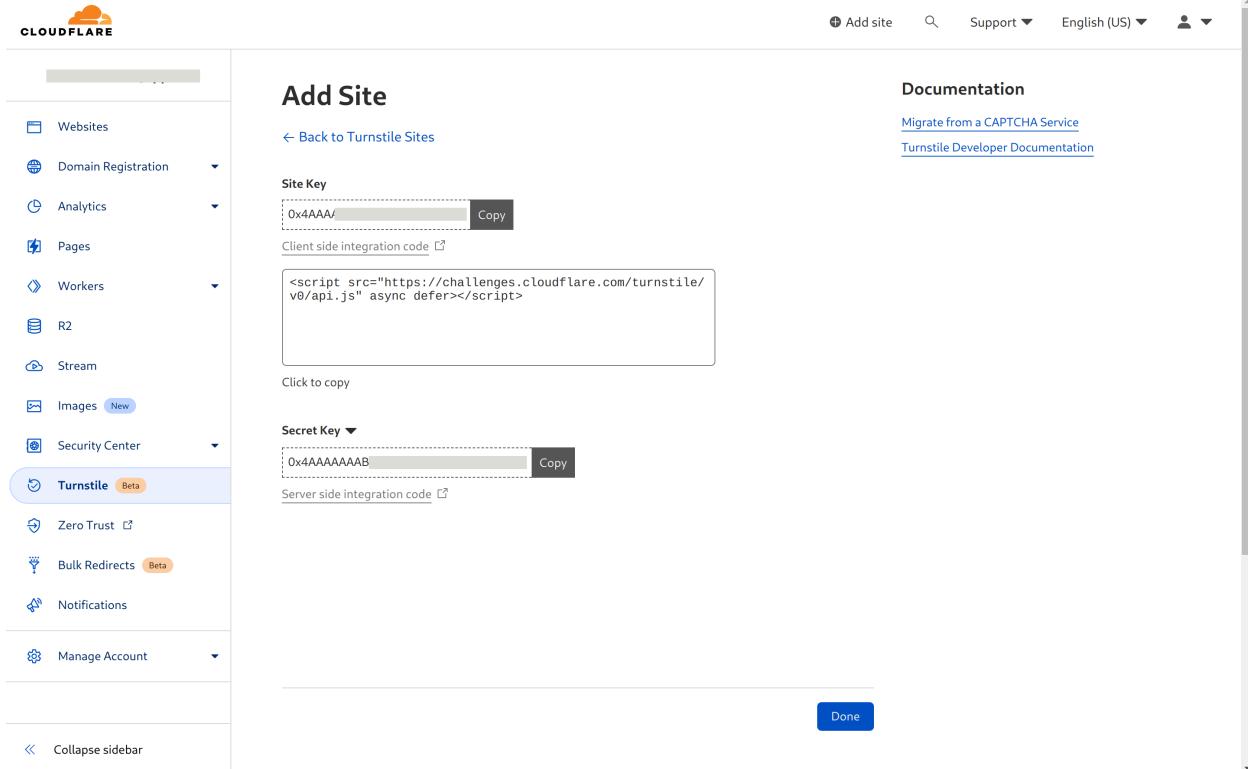
**Managed**  
Cloudflare will use information from the visitor to decide if an interactive challenge should be used. If we do show an interaction, the user will be prompted to check a box (no images or text to decipher).

**Non-interactive**  
A purely non-interactive challenge. Users will see a widget with a loading bar while the browser challenge is run.

**Invisible**  
Invisible challenge that does not require interaction.

[Cancel](#) [Create](#)

Then you can get a site key and a secret key.



The screenshot shows the Cloudflare dashboard with the sidebar expanded. The 'Turnstile' option under the 'Security Center' section is selected, indicated by a blue background and a 'Beta' badge. The main content area is titled 'Add Site' and shows the configuration for a Turnstile site. It includes fields for 'Site Key' (containing '0x4AAA/...' with a 'Copy' button) and 'Secret Key' (containing '0xAAAAAAAB...' with a 'Copy' button). Below these are sections for 'Client side integration code' (containing a script tag) and 'Server side integration code'. A 'Done' button is at the bottom right. The top navigation bar includes links for 'Add site', 'Support', 'English (US)', and user profile.

# Configure in Casdoor

Create a new provider in Casdoor.

Select category as **Captcha** , type as **Cloudflare Turnstile** . And you need to fulfill the site key and the secret key which is created by last step.

 Casdoor Home Organizations Users Roles Permissions Models Adapters Applications Providers Resources ... Admin

Edit Provider

Name ②: Cloudflare Turnstile

Display name ②: Cloudflare Turnstile

Organization ②: admin (share)

Category ②: Captcha

Type ②: Cloudflare Turnstile

Site key ②: 0x4AAAAAAABXhq3vOlgpUTmk

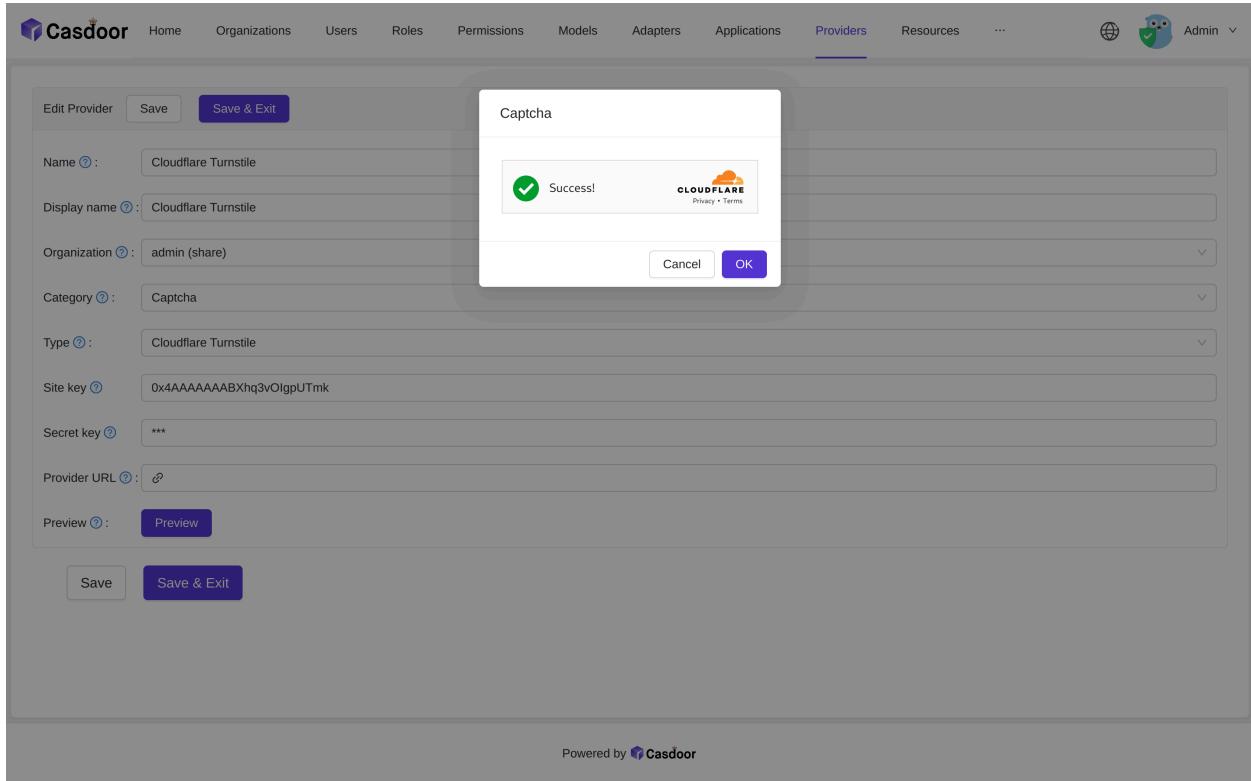
Secret key ②: \*\*\*

Provider URL ②:

Preview ②:

Powered by  Casdoor

And you can click the **Preview** button to preview the style of this captcha.



## Applied in application

Edit the application you want to configure in Casdoor. Select the provider just added and click the button Save.

Providers								
Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action
Cloudflare Turnstile	Captcha						None	



&gt;

Resources

# Resources



## Overview

Upload resources in Casdoor

# Overview

You can upload resources in casdoor. Before upload resources, you need to configure a storage provider. Please see [Storage Provider](#)

You have now configured at least one storage provider and added that provider to your application.

Providers <a href="#">?</a>			
Providers	Add		
Name	Category	Type	Config
Provider_azure	Storage	A	
Github_1	OAuth		
provider_Alipay	Payment		

All right! Let's see an example of how to upload and delete resources.

## Upload Resources

Users can upload resources such as files and images to the previously configured [cloud storage](#).

Resources [Upload a file...](#)

Provider	Created time	Tag
provider_storage_aliyun_oss	source/casbin/leo220yuyaodog/2022_ICM_Problem_D.pdf	2022-05-18 17:25:21
provider_storage_aliyun_oss	source/built-in/admin/美的2021&22Q1交流.pdf	2022-05-18 12:28:01
provider_storage_aliyun_oss	source/casbin/admin/solo.svg	2022-05-17 16:25:39

## Delete Resources

If you no longer need the resource, you can choose to delete it by clicking the "Delete" button.

Created time	Tag	Type	Format	File size	Preview	URL	Action
2022-05-19 23:16:55	custom	image	.jpg	70.3 KB		<a href="#">Copy Link</a>	<a href="#">Delete</a>



&gt;

Products

# Products



## Products

Add products that you want to sell



## Payment

View the transaction information of the products in Payment

# Products

You can add the product (or service) you want to sell. The following will tell you how to add a product.

## Configuring Products Attributes

First, you need to understand the basic properties of the product: [Tag](#) [Detail](#)

[Currency](#) [Price](#) [Quantity](#) [Sold](#)

Tag [?](#) : Casdoor Summit 2022

Detail [?](#) : This is a description

Currency [?](#) : USD

Price [?](#) : 19

Quantity [?](#) : 100

Sold [?](#) : 10

## Payment Provider

Of course, in addition to setting these properties, you also need to add payment

providers to the product, and multiple payment providers can be added to a product.

To learn how to configure a payment provider, see [Payment Provider](#)

Payment providers  [X](#)

[?](#) :

provider\_Alipay

Return URL [?](#) : <http://localhost:8000/products/callback>

Finally, fill in the Return URL. This is the url to jump from the payment provider page when the payment is completed.

## Preview the Product

You're done. See the review and save:

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	<a href="#">Alipay</a>				

# Payment

After the payment is successful, you can see the transaction information of the products in Payment, such as organization, user, purchase time, product name, etc.

## Invoice

You can enter the edit screen to issue an invoice

Type	Product	Price	Curren	Action
	A notebook computer	300	USD	<a href="#">Result</a> <a href="#" style="background-color: blue; color: white; border-radius: 5px;">Edit</a> <a href="#" style="background-color: red; color: white; border-radius: 5px;">Delete</a>

Fill in invoice information, invoice types are [individual](#) and [organization](#).

Message [?](#) :

Person name [?](#) :

Person ID card [?](#) :

Person Email [?](#) :

Person phone [?](#) :

Invoice type [?](#) :

Invoice title [?](#) :

Invoice tax ID [?](#) :

Invoice remark [?](#) :

Invoice URL [?](#) :

Invoice actions [?](#) : [Issue Invoice](#) [Return to Website](#)

Finally, click the "issue invoice" button.



&gt;

Pricing

# Pricing



## Overview

Casdoor pricing overview



## Plan

Casdoor plan overview



## Pricing

Casdoor pricing overview



## Subscription

Casdoor subscription overview

# Overview

Casdoor can be used as subscription management system via [plan](#), [pricing](#) and [subscription](#).

You can choose which plans to include in your price list like on pictures below:

**Pricing**

Casdoor + Casbin SaaS hosting services provided by Casbin Inc.

BASIC	PREMIUM	ENTERPRISE
<b>\$ 9</b> per month	<b>\$ 25</b> per month	<b>\$ 59</b> per month
For small teams, with limited technical support (via Tickets)	For fast growing start-ups, with full technical support (8x5)	For large & medium-sized enterprise, with full technical support (8x5)
<ul style="list-style-type: none"><li>✓ 10 Applications</li><li>✓ 10 Providers</li><li>✓ 100 login requests per second</li><li>✓ 10K Users</li><li>✓ 5 Organizations</li></ul>	<ul style="list-style-type: none"><li>✓ 100 Organizations</li><li>✓ 5K login requests per second</li><li>✓ 99.9% SLA</li><li>✓ Anti-bot security protection</li><li>✓ Custom domain</li></ul>	<ul style="list-style-type: none"><li>✓ 1K Organizations</li><li>✓ 300 Providers</li><li>✓ 99.9% SLA</li><li>✓ Anti-bot security protection</li><li>✓ Custom domain</li><li>✓ UNLIMITED login requests per second</li></ul>
<a href="#">Getting started</a>	<a href="#">Getting started</a>	<a href="#">Getting started</a>

*Free 14-days trial available!*

Each [pricing list](#) belong to [application](#) and has own url that allow sign up new users with selected plan.

General user flow looks like:

- Get [pricing](#) url
- Choose [plan](#)

- Signup to application
- **Subscription** will be auto created

# Plan

Plan - describe list of application's features with own name and price.

Plan features depends on Casdoor role with set of permissions.

That allow to describe plan's features independ on naming and price. For example: plan may has diffrent prices depends on county or date.

Picture below describes relation between Plan and role.

## Plan

- Display Name
  - Price per month
- ...

## Role

permission 1  
permission 2  
...  
permission N

# Plan properties

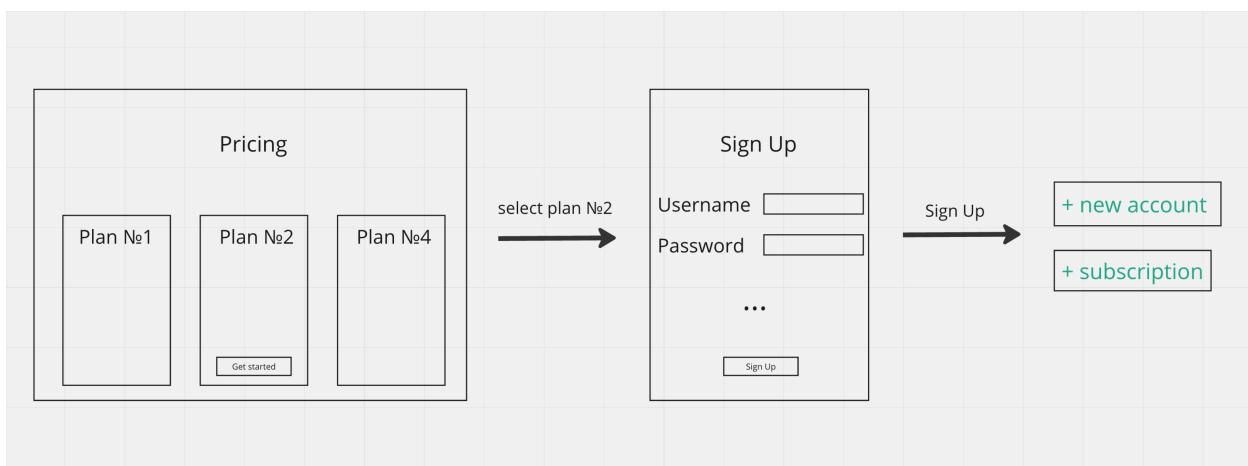
Every plan has these properties:

- Owner
- Name
- CreatedTime
- DisplayName
- IsEnabled
- PricePerMonth
- PricePerYear
- Role

# Pricing

Pricing contains one or more plan and provide ability to sing up to application with selected plan.

General flow might looks like on picture below:



## Pricing properties

Every Pricing has these properties:

- Owner
- Name
- CreatedTime
- DisplayName
- Description
- Plans - Array of plans
- IsEnabled

- `Has trial` - any payments will not be required for sign up in case of true
- `TrialDuration` - impact on subscription end days
- `Application`
- `Submitter`
- `Approver`
- `ApproveTime`
- `State`

# Subscription

**Subscription** - helps to manage user's selected plan that make easy to control application's features access.



Since each plan based on `casdoor role` you can assign plan's role to user and use enforce API for permission checking.

**Subscription** can be created in thee ways:

- Manually by admin
- After sign up from pricing page
- Via API.

## Subscription properties

Every Subscription has these properties:

- `Owner`
- `Name`
- `CreatedTime`
- `DisplayName`
- `Duration`
- `Description`
- `Plan`
- `StartDate`

- EndDate
- User
- IsEnabled
- Submitter
- Approver
- ApproveTime
- State



&gt;

Users

# Users



## Overview

Manage users in Casdoor



## MFA / 2FA

Config adapter and basic CRUD to policy



## Roles

the user's roles



## Permissions

the user's permissions

# Overview

## User properties

As an authentication platform, Casdoor is able to manage users. Every user has these properties:

- `Owner` Owner organization of the user
- `Name` User name, unique
- `CreatedTime`
- `UpdatedTime`
- `Id` Unique for every user
- `Type`
- `Password`
- `PasswordSalt`
- `PasswordOptions` Password complexity options
- `DisplayName` Shown in UI
- `FirstName`
- `LastName`
- `Avatar` A link to user's avatar
- `PermanentAvatar`
- `Email`
- `Phone`
- `Location`
- `Address`

- `Affiliation`
- `Title`
- `IdCardType`
- `IdCard`
- `Homepage`
- `Bio`
- `Tag`
- `Region`
- `Language`
- `Gender`
- `Birthday`
- `Education`
- `Score`
- `Karma`
- `Ranking`
- `IsDefaultAvatar`
- `IsOnline`
- `IsAdmin` Is the user the admin of his organization
- `IsGlobalAdmin` Does the user have the permission to manage the Casdoor
- `IsForbidden`
- `IsDeleted`
- `SignupApplication`
- `Hash`
- `PreHash`
- `CreatedIp`
- `LastSigninTime`

- `LastSigninIp`
- `Roles` Array of the user's roles
- `Permissions` Array of the user's permissions

unique Id of the platform:

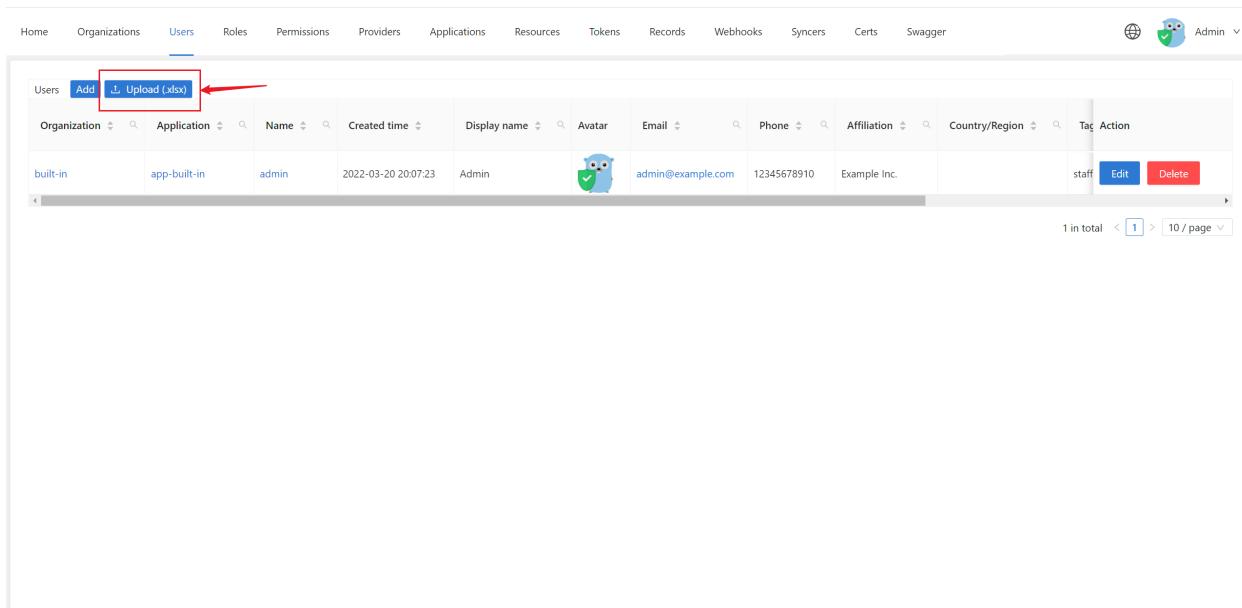
- `Github`
- `Google`
- `QQ`
- `WeChat`
- `Facebook`
- `DingTalk`
- `Weibo`
- `Gitee`
- `LinkedIn`
- `Wecom`
- `Lark`
- `Gitlab`
- `Adfs`
- `Baidu`
- `Casdoor`
- `Infoflow`
- `Apple`
- `AzureAD`
- `Slack`
- `Steam`
- `Ldap`

- **Properties** This is a string → string map, stored all other properties may need.

## Import users from XLSX file

You can add new users or update existing Casdoor users by uploading a XLSX file of user information.

In the Admin Console, go to Users and click **Upload(.xlsx)** button.



The screenshot shows the Casdoor Admin Console interface. The top navigation bar includes links for Home, Organizations, Users (which is selected), Roles, Permissions, Providers, Applications, Resources, Tokens, Records, Webhooks, Syncers, Certs, and Swagger. On the far right, there's a globe icon, a user profile icon, and the word "Admin". Below the navigation is a search bar with placeholder text "Search users, roles, organizations...". The main content area is titled "Users" and contains a table with columns: Organization, Application, Name, Created time, Display name, Avatar, Email, Phone, Affiliation, Country/Region, Tag, and Action. A single user row is shown with values: built-in, app-built-in, admin, 2022-03-20 20:07:23, Admin, an owl icon, admin@example.com, 12345678910, Example Inc., staff, and buttons for Edit and Delete. At the bottom of the table are pagination controls showing "1 in total" and "10 / page". Above the table, there are buttons for "Add" and "Upload (.xlsx)" with a red arrow pointing to the upload button. The footer of the page says "Made with ❤ by Casdoor".

Select your XLSX file and click Open, the users will be imported.

We provide a [template XLSX file](#) named `user_test.xlsx` in the `xlsx` folder. The template includes 5 users for test and headers for some required user properties.

Home   Organizations   **Users**   Roles   Permissions   Providers   Applications   Users uploaded successfully, refreshing the page   Syncers   Certs   Swagger    Admin

**user\_test.xlsx**

Organization	Application	Name	Created time	Display name	Avatar	Email	Phone	Affiliation	Country/Region	Tag	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	sciencist	<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	galileleo	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		3dzw4@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>

6 in total < 1 > | 10 / page ▾

Made with ❤ by **Casdoor**

# MFA / 2FA

## About multi-factor authentication

MFA (Multi-Factor Authentication) is a security measure that can improve the security of users and systems. It requires users to provide two or more factors of authentication to verify their identity when logging in or performing sensitive operations.

For Casdoor, the second form of authentication is a code that's sent as a text message or email. After you enable MFA, Casdoor generates an authentication code any time someone attempts to sign in your account. The only way someone can sign in your account is if they know both your password and have access to the authentication code.

## Config MFA

1. In user profile page, you can see the configuration of multi-factor authentication. If you can't see it, make sure the organization has added multi-factor authentication item in the account items table.

Managed accounts [Add](#)

Application	Username	Password	Action
		No data	

Multi-factor authentication [②](#):

Multi-factor methods

Type : sms	<a href="#">Setup</a>
Type : email	<a href="#">Setup</a>

ID card [②](#):

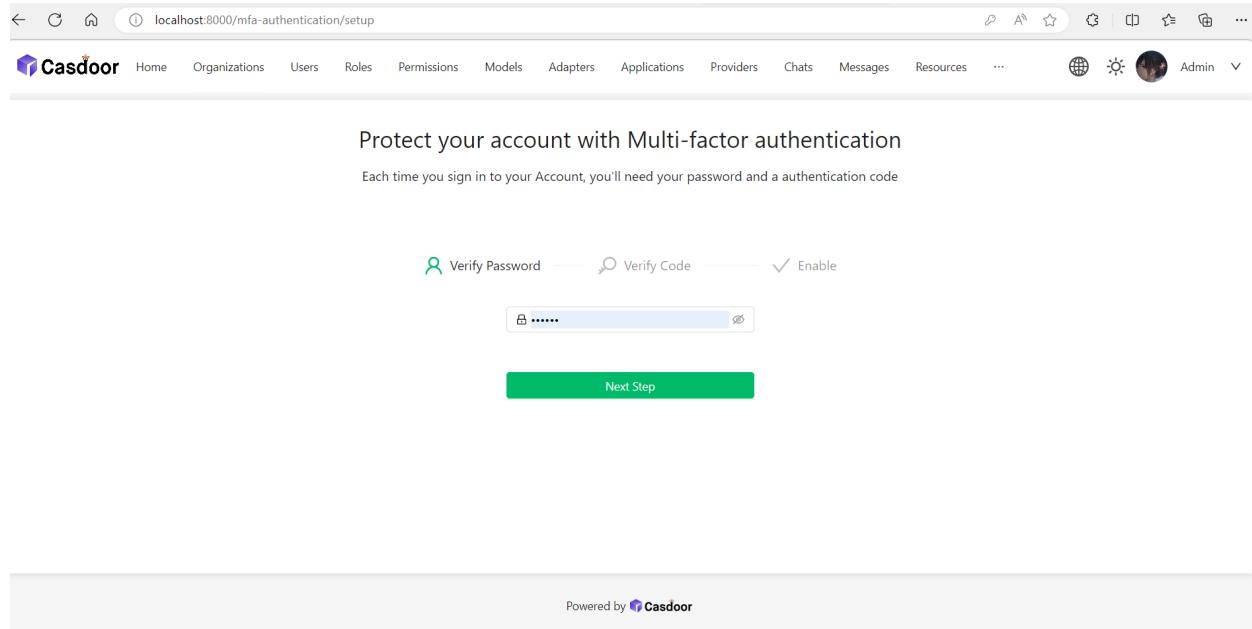
2. Click the "setup" button.

Multi-factor authentication [②](#):

Multi-factor methods

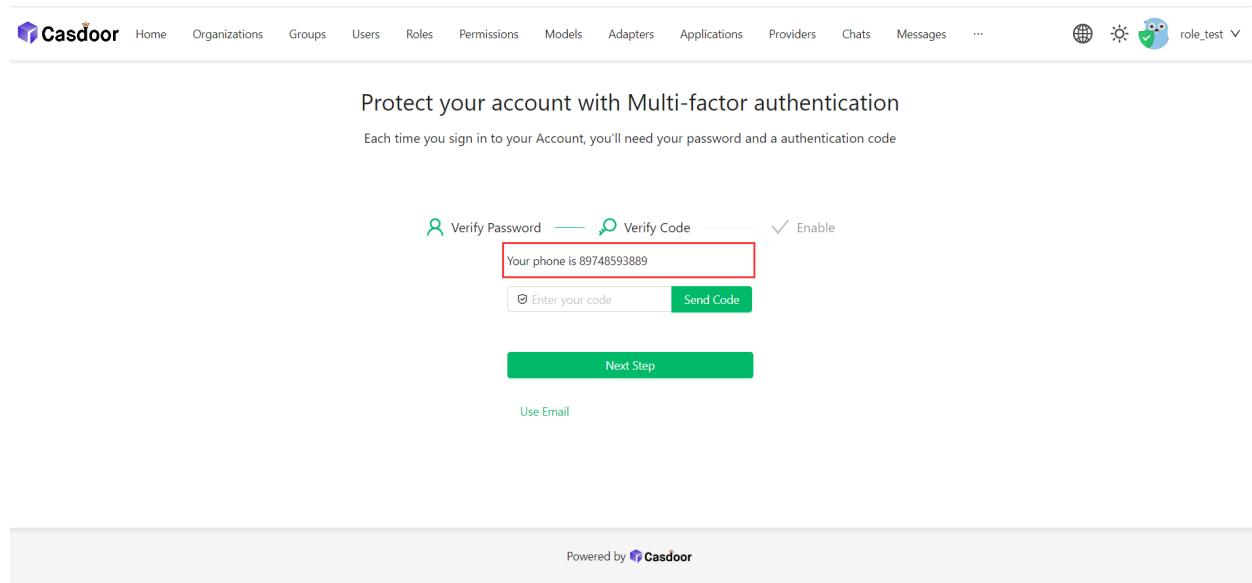
Type : sms	<a href="#">Setup</a>
Type : email	<a href="#">Setup</a>

3. Type your password and click "Next Step".

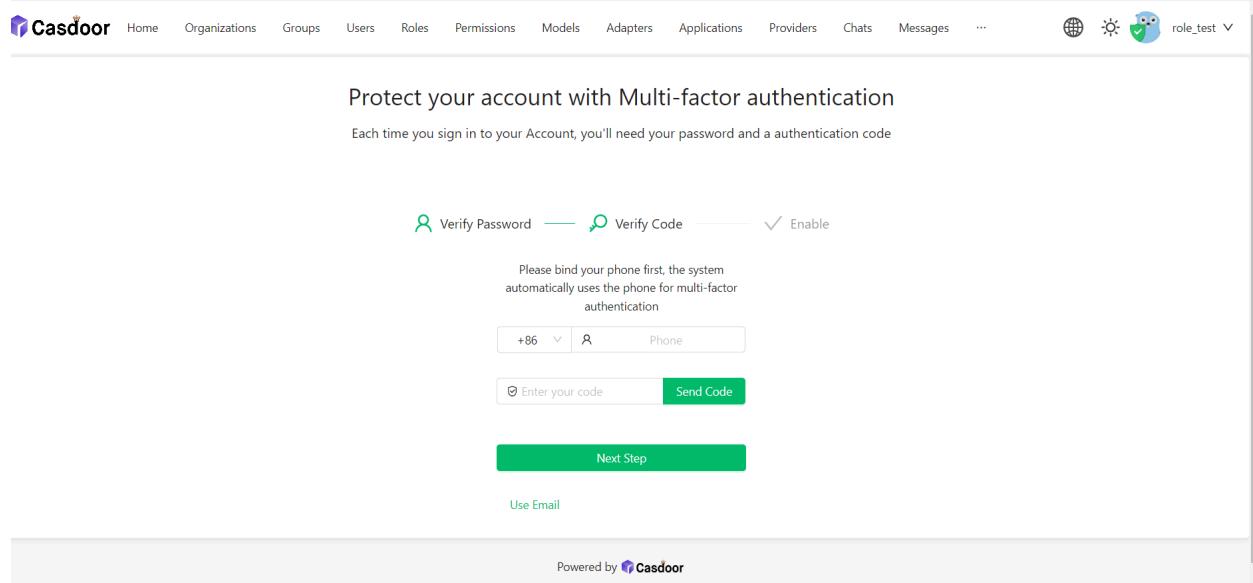


## Configuring multi-factor authentication using text messages

If you have bound your mobile phone number, Casdoor will use it to send you a text message.



If not, you need to bind your mobile phone number first.



1. Select your country code and type your mobile phone number.
2. Check your information is correct, click "Send Code".
3. You'll receive a text message with a security code. Then type the code into the field "Enter your code" and click "Next Step".

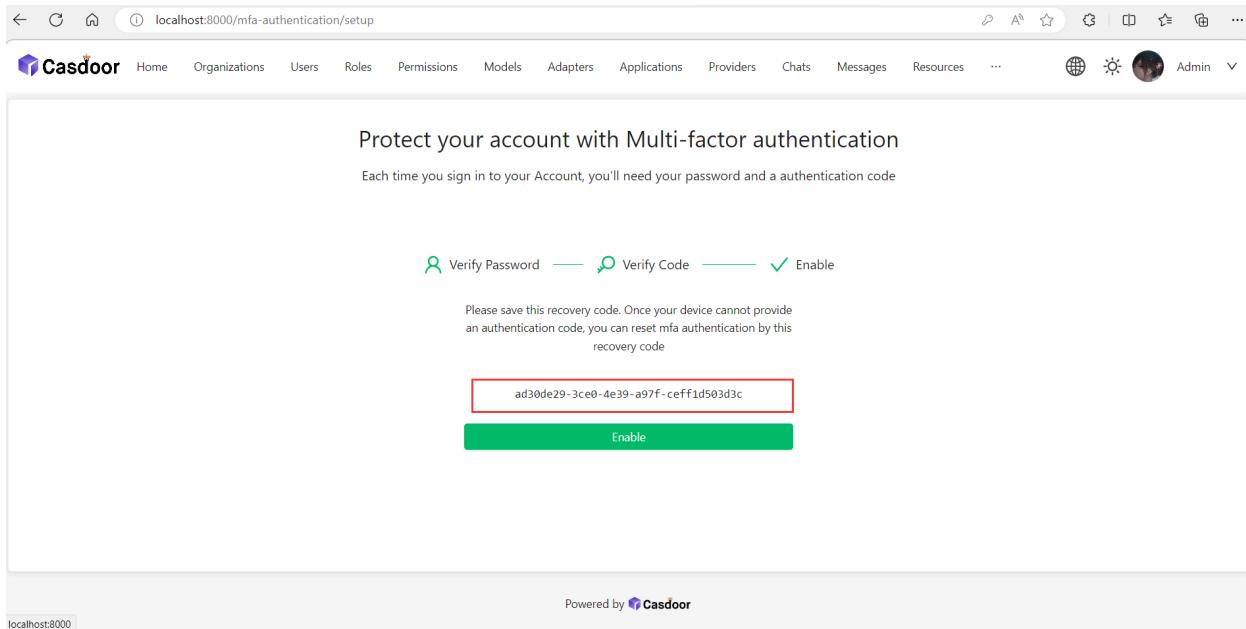
## Configuring multi-factor authentication using email

Config email as your multi-factor authentication method is similar to text messages.

1. Use your current email or type your email address and click "Send Code".
2. Then type the code into the field "Enter your code" and click "Next Step".

# Enable multi-factor authentication and save recovery codes

Above "Enable" button, copy your recovery codes and save to your device. Save them to a secure location because your recovery codes can help you get back into your account if you lose access.



## ⚠ CAUTION

One recovery code can only be used once. If you use a recovery code to sign in, it will be invalid.

# Changing your preferred MFA method

You can add multiple MFA methods. Only the preferred method will be used when you sign in.

If you want to set a preferred MFA method, click the "Set preferred" button.

The screenshot shows a user interface for managing multi-factor authentication methods. At the top, there's a section for "Multi-factor authentication" with a "Disable" button. Below it, there's a table for "Multi-factor methods".  
The first row shows "Type : sms 132\*\*\*\*0885" with an "Enabled" status and a "Set preferred" button.  
The second row shows "Type : email 2\*\*\*\*\*4@qq.com" with an "Enabled" status and a "Set preferred" button, which is highlighted with a red border.  
At the bottom, there's a section for "ID card" with a dropdown menu.

A "Preferred" label is displayed on your preferred method.

## Disable multi-factor authentication

If you want to disable multi-factor authentication, click the "Disable" button. All your multi-factor authentication config will be deleted.

The screenshot shows the same user interface as the previous one, but with a different configuration. The "Disable" button at the top is now highlighted with a red border.  
In the "Multi-factor methods" section:  
- The first row for "sms" has an "Enabled" status and a "Set preferred" button.  
- The second row for "email" has an "Enabled" status and a "Set preferred" button.  
Both rows have their "Enabled" status boxes checked.  
The "ID card" section at the bottom is also present.

# Roles

Each user may have multiple roles. You can see the user's roles on the user's profile.

Bio [?](#) :

Tag [?](#) :

Signup application [?](#) :

Roles [?](#) :   (highlighted)

Permissions [?](#) :

3rd-party logins [?](#) :

Is admin [?](#) :

Is global admin [?](#) :

Is forbidden [?](#) :

Is deleted [?](#) :

## Role properties

Every role has these properties:

- `Owner`
- `Name`
- `CreatedTime`
- `DisplayName`
- `.IsEnabled`
- `Users` Array of this role's sub users

- Roles Array of this role's sub roles

# Permissions

Each user may have multiple permissions. You can see the user's permissions on the user's profile.

Bio [?](#) :

Tag [?](#) :

Signup application [?](#) :

Roles [?](#) :

Permissions [?](#) :  (The permission\_test button is highlighted with a red border)

3rd-party logins [?](#) :

Is admin [?](#) :

Is global admin [?](#) :

Is forbidden [?](#) :

Is deleted [?](#) :

## Permission properties

Permission has these properties:

- 
- 
- 
- 
- 
-

- `Users` Array of this role's sub users
- `Roles` Array of this role's sub roles
- `ResourceType`
- `Resources` Array of the resources
- `Actions` Array of the actions
- `Effect`



&gt;

Syncer

# Syncer



## Overview

Synchronize users in Casdoor



## Database

Using Database Syncer to synchronize database



## Keycloak

Using Keycloak Syncer to synchronize Keycloak

# Overview

As an authentication platform, Casdoor can easily manipulate users stored in databases.

## Syncer

Casdoor stores users in `user` table. Don't worry about migrating your application user data into Casdoor, when you plan to use Casdoor as an authentication platform. Casdoor provides `syncer` to quickly help you sync user data to Casdoor.

Specify the database and user table that you want to synchronize to Casdoor. And the syncer will sync the data after the specified interval. For details, see [database syncer](#).

## Synchronization hash

Casdoor use hash to determine how to update a user. Casdoor would calculate the hash value of each user in the table, which is generated using users' information, such as password or mobile phone number.

If the calculated hash value of a user with a specific `Id` changed compared with the original value, Casdoor would affirm which user table has been updated. Then the database would update the old information, realize the **bilateral synchronization** between Casdoor user table and origin user table.

# Database

## Database Syncer

The users table we created as a demo are imported from the [template XLSX file](#).

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			<a href="https://casbin.org">https://casbin.org</a>	z6mive@
built-in	euler	2022-03-20T20:47:08+08:00		bb7831b4-0d24-4e96-b043-f8fd8d15eb	normal-user	123		Leonhard Euler			<a href="https://casbin.org">https://casbin.org</a>	3dw4j@
built-in	galileo	2022-03-20T20:47:58+08:00		7920eb6c-f9f5-40ef-8e18-3ac99f49bd15	normal-user	123		Galileo Galilei			<a href="https://casbin.org">https://casbin.org</a>	8pf438@
built-in	gauss	2022-03-20T20:48:33+08:00		f0c28816-2c0d-479b-b545-cb4cf96db36	normal-user	123		Carl Friedrich Gauß			<a href="https://casbin.org">https://casbin.org</a>	vqdsan@
built-in	tesla	2022-03-20T20:49:03+08:00		687c3068-fd21-4d32-b2ba-e13e8b369a	normal-user	123		Nikola Tesla			<a href="https://casbin.org">https://casbin.org</a>	9v73hn@

Click the Syncers tab and create a new syncer. Fill in all the required information as below and save.

Organization [?](#):

Name [?](#):

Type [?](#):

Host [?](#):

Port [?](#):

User [?](#):

Password [?](#):

Database type [?](#):

Database [?](#):

Table [?](#):

Table primary key [?](#):

Table columns [?](#):

Table columns	Add	Column name	Column type	Casdoor column	Is hashed	Action
		name	string	Name	<input checked="" type="checkbox"/>	
		create_time	string	CreatedTime	<input checked="" type="checkbox"/>	
		id	string	Id	<input checked="" type="checkbox"/>	
		password	string	Password	<input checked="" type="checkbox"/>	

Affiliation table [?](#):

Avatar base URL [?](#):

Sync interval [?](#):



### TIP

In general, you need to fill in at least the `ID` and `Name` in Casdoor Columns.  
And others important fields like `createdTime`, `Password`, `DisplayName`.

The following are the required fields.

- `Organization`: The organization that the user will import
- `Name`: The syncer name
- `Type`: Select database
- `Host`: The original database host
- `Port`: The original database port
- `User`: The original database username
- `Password`: The original database password
- `Database type`: All Xorm supported databases, like: MySQL, PostgreSQL, SQL Server, Oracle, Sqlite
- `Database`: The original database name
- `Table`: The original user table name
- `Table columns`
- `Column name`: The original user column name
- `Column type`: The original user column type
- `Casdoor Column`: The casdoor user column name

Optional fields

- `Is hashed`: Whether to calculate hash value. When enable "Is hashed", if the field of user in origin table updated, the syncer will sync this user. Disable "Is hashed", meaning if only the field update, the syncer need not sync the user. In short, the user does not synchronize until the fields involved in the hash calculation(enable "Is hashed") are updated.

- **Avatar base URL**: When sync users, if **Avatar base URL** is not empty and origin **user.avatar** not hasPrefix "http", new **user.avatar** will be replaced by **Avatar base URL + user.avatar**.
- **Affiliation table**: It is used to sync the affiliation of user from this table in database. Because the affiliation may be code of int type in "Affiliation table", so we need to map the int to a string. See [getAffiliationMap\(\)](#) . Because Casdoor has some redundant fields to borrow, [here](#) we use **score** to map the int code to a string name.

Then you can turn on the **Is enable** button and save, the syncer will start to work.

Users												
												Action
Organization	Organization	Application	Name	Created time	Display name	Avatar	Email	Phone	Affiliation	Country/Region		
built-in			euler	2022-04-08 10:10:45							<button>Edit</button>	<button>Delete</button>
built-in			gauss	2022-04-08 10:10:45							<button>Edit</button>	<button>Delete</button>
built-in			tesla	2022-04-08 10:10:45							<button>Edit</button>	<button>Delete</button>
built-in			einstein	2022-04-08 10:10:45							<button>Edit</button>	<button>Delete</button>
built-in			galileleo	2022-04-08 10:10:45							<button>Edit</button>	<button>Delete</button>

# Keycloak

## Keycloak Syncer

The Keycloak syncer is basically the same as the [database syncer](#), except that the [Table](#) and [Table columns](#) can be configured automatically for Keycloak.

In addition, the Keycloak syncer will query [credential](#) table, [keycloak\\_group](#) table and [user\\_group\\_membership](#) table because the user information in Keycloak is stored in multiple tables.

Column name	Column type	Casdoor column	Is hashed	Action		
ID	string	Id	<input checked="" type="checkbox"/>			
USERNAME	string	Name	<input checked="" type="checkbox"/>			
EMAIL	string	DisplayName	<input checked="" type="checkbox"/>			
EMAIL_VERIFIED	boolean	Email	<input checked="" type="checkbox"/>			
FIRST_NAME	string	EmailVerified	<input checked="" type="checkbox"/>			
LAST_NAME	string	FirstName	<input checked="" type="checkbox"/>			
CREATED_TIMESTAMP	string	LastName	<input checked="" type="checkbox"/>			
ENABLED	boolean	CreatedTime	<input checked="" type="checkbox"/>			
		IsForbidden	<input checked="" type="checkbox"/>			



&gt;

Tokens

# Tokens



## Overview

Introduction to tokens in Casdoor

# Overview

Casdoor is based on OAuth. Tokens are users' OAuth token.

- Owner
- Name
- CreatedTime
- Application
- Organization
- User
- Code
- AccessToken
- ExpireIn Tokens will expire in hours
- Scope Scope of authorization
- TokenType E.g. type Bear

There are two options to generate a JWT Token after logging into the application:

- JWT
- JWT-Empty

The JWT option will create a token with all User fields. The JWT-Empty will create a token with all non-empty values for the user.



&gt;

Webhooks

# Webhooks



## Overview

Add webhooks in Casdoor

# Overview

## Overview

Event systems allow you to build integrations, which subscribe to certain events on Casdoor. When one of those event is triggered, we'll send a POST json payload to the configured URL. The application parsed the json payload and carry out the hooked function. Events consist of signup, login, logout, update users, which are stored in the action field of the record. Event systems can be used to update an external issue from users.



&gt;

Deploy

# Deploy

## Nginx

use Nginx to reverse proxy your backend Go program, quickly start the Casdoor service

## k8s

Deploy Casdoor in k8s

# Nginx

Although Casdoor is a front-end back-end separation architecture, in the production environment, the back-end program still provides static file services for front-end files. Therefore, you can use reverse proxy software such as [Nginx](#) to proxy all traffic for the Casdoor domain and redirect it to the port monitored by the backend go program.

In this chapter you will learn how to use Nginx to reverse proxy your backend Go program, and quickly start the Casdoor service.

## 1. Build front end static files

Now assume that you have downloaded Casdoor and completed the necessary configuration. If not, go to [Get started](#) section.

You only needs to build static files, like this:

[Yarn](#)    [npm](#)

---

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

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

## 2. Run the back end program

```
go run main.go
```

Or build first:

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

## 3. Configure and run Nginx

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

Add a server:

```
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;
    }
}
```

Then restart your nginx process, run:

```
nginx -s reload
```

## 4. Test

Visit `http://YOUR_DOMAIN_NAME` in your favorite browser.

# k8s

## Deploy Casdoor in k8s

We have given a basic example of deploying Casdoor into k8s. In the root folder of casdoor, there exists a file named "k8s.yaml", which includes an example minimum configuration to be used in deploying casdoor in k8s, a deployment and a service.

First, make sure that you have modified the conf/app.conf so that the casdoor can successfully connect to the database, and the database is running. Second, make sure k8s is able to pull the necessary images.

Run

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

And soon you can see the result via command `kubectl get pods`

The content of k8s.yaml is as follow

```
# 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
```

This file is merely an example. For example, you can choose to use a namespace other than default, use a service type instead of nodeport to expose the casdoor, or use a use config map in k8s to mount the configuration file, which is a more recommended way in k8s.





LDAP

# LDAP



## Overview

Casdoor cooperates with a ldap server



## Config and Sync LDAP Users

LDAP configuration in Casdoor



## LDAP Server

How to connect ldap client in Casdoor

# Overview

Support for Ldap server currently has been introduced into Casdoor. Casdoor is able to synchronize users from Ldap servers to Casdoor to use them as user accounts to log in, and authenticate them using the Ldap servers. Casdoor also supports setting up cron job to synchronize users automatically on a regular basis.

## Detail about Casdoor-Ldap synchronization mechanism

How Casdoor cooperates with a Ldap server is described as follows:

1. Synchronization: Casdoor can connect to Ldap server fetch users' information, reads all users' information (include `uidNumber`, `uid`, `cn`, `gidNumber`, `mail`, `email`, `emailAddress`, `telephoneNumber`, `mobile`, `mobileTelephoneNumber`, `registeredAddress`, `postalAddress`), and creates Casdoor accounts for each user in Ldap, and stores the accounts in database.
2. Authentication: As we have seen, Casdoor doesn't fetch Ldap users' passwords to Casdoor. Thus, when the account which is synchronized from Ldap server tries to log in through Casdoor, instead of checking password stored in casdoor's database, Casdoor connects to Ldap server and verifies whether the user's password is correct.
3. User distinguished: Casdoor uses `uid` to exclusively identify a user, thus please make sure every Ldap user has a different uid.

Once a user is synchronized into Casdoor, that user's information is detached with the Ldap user, which means, if you modify the user's information in Casdoor, the

user's information in ldap won't be modified and vice versa (except ldap user's password, we rely on it to authenticate a user)

# Config and Sync LDAP Users

Ldap configurations belong to an organization, which Ldap users will be synchronized into.

You are supposed to use a global admin user to modify the configuration. You need to enter the following information of the LDAP user synchronization in the "organization" page.

LDAP		添加	服务器	基本DN	自动同步	最近同步	操作
LDAP服务器	Example LDAP Server	example.com:389	ou=People,dc=example,dc=com	Disable			同步 编辑 删除

# Config to connect LDAP server

		<a href="#">Edit LDAP</a>	<a href="#">Save</a>	<a href="#">Save &amp; Exit</a>	<a href="#">Sync LDAP</a>
Organization <small>?</small> :	built-in				
ID <small>?</small> :	691edec0-f1ab-4e23-8f9f-a824a383032f				
Server name <small>?</small> :	Example LDAP Server				
Server host <small>?</small> :	example.com				
Server port <small>?</small> :	389				
Enable SSL <small>?</small> :	<input checked="" type="checkbox"/>				
Base DN <small>?</small> :	ou=built-in,dc=example,dc=com				
Search Filter <small>?</small> :	(objectClass=posixAccount)				
Filter fields <small>?</small> :	<input type="button" value="uid"/> <input type="button" value="Email"/>				
Admin <small>?</small> :	cn=admin,dc=example,dc=com				
Admin Password <small>?</small> :	.....				
Auto Sync <small>?</small> :	0	mins			

## Server Name

A friendly name is used by managers to identify different servers.

e.g: Example LDAP Server

## Server Host

LDAP server's host or IP address.

e.g: example.com

## Server Port

LDAP server's ports, only allow numbers.

e.g: 389

## Base DN

Casdoor uses Sub search mode by default when searching in LDAP. Base DN is the basic distinguished name of the search. Casdoor will return all users under the current base DN.

The admin account configured in casdoor should have at least read-only permissions at base DN.

e.g: ou=Example,dc=example,dc=com

## Search filter

Casdoor uses search filter to query ldap users.

e.g: (objectClass=posixAccount)

## Filter fields

Filter fields are the identifier of the user in LDAP server, When you log in to Casdoor as an LDAP user. Casdoor regards the entered login username as the uid of LDAP user. You can also config other filed, such as mail, mobile.

localhost:8000/ldap/built-in/691edec0-f1ab-4e23-8f9f-a824a383032f

ExPhysLab 计算机 工作台·语音 Kristin英语课堂 Google Email International Jour... Learn English Onli... Understanding IE... DeepL Translate...

Other bookmarks

**Casdoor** Home Organizations Users Roles Permissions Models Adapters Applications Providers Chats Messages Resources ... Admin

Edit LDAP Save Save & Exit Sync LDAP

Organization : built-in

ID : 691edec0-f1ab-4e23-8f9f-a824a383032f

Server name : Example LDAP Server

Server host : 1

Server port : 389

Enable SSL :

Base DN : ou=built-in,dc=example,dc=com

Search Filter : (objectClass=inetOrgPerson)

Filter fields :

Admin : cn=admin,dc=example,dc=com

Admin Password : \*\*\*\*\*

## Admin

An account that can log in to the specified LDAP server.

Login with DN or ID depends on the LDAP server settings you want to connect.

e.g: `cn=manager,dc=example,dc=com`

## Admin Password

Password of LDAP server Admin account.

## Auto Sync

Set `0` to disable auto sync, other value means Sync every few minutes.

# Sync users

The sync table displays all users get from the LDAP server in the specific `ou`. If

the users have been synced, the checkbox will be disabled. You can check the box to select users, then sync the selected users from the LDAP server.

Example LDAP Server		Sync	Edit LDAP			
<input type="checkbox"/>	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			

< 1 > 10 / page ▾

### **⚠ CAUTION**

If the **uid** of the user in LDAP server is same as the **name** of a user existed in the organization of Casdoor, Casdoor will create a new user that the **name** include the **uid** and a random string. But the user may not be able to login, because the name of the new synced user does not exist in LDAP server. So try to avoid that.

# LDAP Server

Many systems like [Nexus](#) support [ldap](#) authentication. A simple Idap server is also implemented in Casdoor, which supports bind and search operations.

The following describes how to connect to the Idap server in Casdoor and implement simple login authentication.

## LDAP Server Port

The LDAP server listens on port [389](#) by default, you can change the default port by changing [ldapServerPort](#) in [conf/app.conf](#).

## How it works

Similar to the Idap client in Casdoor, the users in the Idap server are all subclasses of [poxisAccount](#).

When the server receives a set of data transmitted by the Idap, it will parse the [cn](#) and [ou](#), where [cn](#) represents the username, [ou](#) represents the organization name. It doesn't matter what [dc](#) is.

If it is a bind operation, the server will use Casdoor to verify the username and password and give the user permission in Casdoor.

If it is a search operation, the server will check whether the Search operation is legal according to the permissions given to the client by the bind operation and return a response.

## INFO

We only support [Simple Authentication](#).

## How to bind

In Casdoor Ldapserver, we only recognize `DN` similar to this: `cn=admin, ou=buil-`  
`in, dc=example, dc=com.`

So please set the `DN` of the admin user to the above form. Then you can use this `DN` to bind to Ldap server with the user's password to log in to casdoor for verification. If the server verification is passed, the user will be granted the authority in Casdoor.

## How to search

Once the bind operation completes successfully, you can perform the correct search operation. There are some differences between search and bind.

- If you want to search for a certain user, such as `Alice` under the `built-in` organization, you should use `DN` like this : `ou=buil-`  
`in, dc=example, dc=com,` and add `cn=Alice` in the Filter field.
- If you want to search for all users under a certain organization, such as all users in `built-in`, you should use `DN` like this : `ou=buil-`  
`in, dc=example, dc=com,` and add `cn=*` in the Filter field.
- If you want to search for all users for all organizations (the premise is that the user has sufficient permissions), you should use `DN` like this  
`:ou=*, dc=example, dc=com,` and add `cn=*` in the Filter field.



&gt;

Integrations

# Integrations



Go

8 items



Java

17 items



JavaScript

1 items



Lua

1 items



PHP

4 items



Ruby

1 items



Haskell

1 items



Python

1 items

# Go

## Kubernetes

Using Casdoor for authentication in Kubernetes

## OpenShift

Using Casdoor for authentication in openshift

## BookStack

Using Casdoor for authentication in BookStack

## Bytebase

Using OAuth2 to connect various applications, like Bytebase

 **ELK**

Overview of casdoor/elk-auth-casdoor

 **Gitea**

Using Casdoor for authentication in Gitea

 **Grafana**

Using Casdoor for authentication in Grafana

 **MinIO**

Configuring Casdoor as identity provider to support with MinIO

# Kubernetes

According to the [Kubernetes documentation](#), the API Server of Kubernetes can be authenticated using OpenID Connect (OIDC). This article will guide you on how to configure authentication in Kubernetes using Casdoor.

## Environment Requirements

Before starting, please make sure that you have the following environment:

- A Kubernetes cluster.
- A Casdoor application like this [demo website](#)
- kubectl command tool (optional)

 NOTE

Kubernetes oidc-issuer-url only accepts URLs which use the https:// prefix.  
So your Casdoor application should be deployed on an HTTPS website.

## Step 1: Creating an Casdoor App and User Account for Authentication

Go to your Casdoor and add your new application Kubernetes. Please remember the `Name`, `Organization`, `client ID`, `client Secret` and add some grant type in this APP.

Name [?](#):  Kubernetes

Display name [?](#):

Logo [?](#):  URL [?](#):  https://cdn.casbin.org/img/casdoor-logo\_1185x256.png

Preview:  Casdoor

Home [?](#):

Description [?](#):

Organization [?](#):  casbin

Client ID [?](#):  Kubernetes

Client secret [?](#):  72c65c3912aec24a9f3ec41b65a7577114ed2bae

Cert [?](#):

Grant types [?](#): Authorization Code Password ID Token Refresh Token Client Credentials Token

Next, we will add a new user to the application that we just created. Please note that the `organization` and `Signup application` used here should correspond to the APP registered earlier.

Organization <a href="#">?</a> :	casbin
ID <a href="#">?</a> :	202e02e9-9128-496a-a209-fdb336448f56
Name <a href="#">?</a> :	user_pnvm5i
Display name <a href="#">?</a> :	New User - pnvm5i
Avatar <a href="#">?</a> :	<p>Preview:</p>  <p>Upload a photo...</p>
User type <a href="#">?</a> :	normal-user
Password <a href="#">?</a> :	<a href="#">Modify password...</a>
Email <a href="#">?</a> :	pnvm5i@example.com
Phone <a href="#">?</a> :	+1 <input type="button" value="▼"/> 78005961394
Country/Region <a href="#">?</a> :	Please select country/region
Location <a href="#">?</a> :	
Affiliation <a href="#">?</a> :	Example Inc.
Title <a href="#">?</a> :	
Homepage <a href="#">?</a> :	
Bio <a href="#">?</a> :	
Tag <a href="#">?</a> :	staff
Signup application <a href="#">?</a> :	Kubernetes

# Step 2: Configure Kubernetes API Server with OIDC Authentication

To enable the OIDC plugin, at least configure the following flags on the API server:

- `--oidc-issuer-url` : URL of the provider which allows the API server to discover public signing keys.
- `--oidc-client-id` : A client id that all tokens must be issued for.

This article use of minikube for demonstration. We can configure the OIDC plugin for the minikube's API server using the following command at startup:

```
minikube start --extra-config=apiserver.oidc-issuer-
url=https://demo.casdoor.com --extra-config=apiserver.oidc-client-
id=294b09fbc17f95daf2fe
```

# Step 3: Test OIDC Authentication

## Obtain Authentication Information

Due to the lack of a frontend in kubectl, authentication can be performed by sending a POST request to the Casdoor server. Here is the code in Python which sends a POST request to the Casdoor server and retrieves the `id_token` and `refresh_token`:

```
import requests
import json
```

After executing this code, you should receive a response similar to the following:

```
{  
  "access_token": "xxx",  
  "id_token": "yyy",  
  "refresh_token": "zzz",  
  "token_type": "Bearer",  
  "expires_in": 72000,  
  "scope": ""  
}
```

Now, we can use the `id_token` that we just obtained to authenticate with Kubernetes API server.

## HTTP Request-Based Authentication

Add the token to the request header.

```
curl https://www.xxx.com -k -H "Authorization: Bearer $(id_token)"
```

- <https://www.xxx.com> is the Kubernetes API server deployment address.

## Kubectl Client-Based Authentication

### Configuration File Method

Write the following configuration to the `~/.kube/config` file. You should replace each configuration item in the configuration file above with the values you obtained earlier.

```
users:
```

Now you can directly access your API server using kubectl. Try running a test command.

```
kubectl cluster-info
```

### Command Line Argument Method

Alternatively, you can authenticate by directly adding the id\_token to the command line parameters of kubectl.

```
kubectl --token=$(id_token) cluster-info
```

# OpenShift

OpenShift supports OIDC, so we can integrate Casdoor with OpenShift. The following steps demonstrate how to integrate Casdoor with OpenShift Local using [the online demo of Casdoor](#).

## Step1. Create an Casdoor application

Add a new application in Casdoor, note following points.

- Remember the `Client ID` and `Client secret` for the next step.
- The format of the Redirect URL is `https://oauth-openshift.apps.<cluster_name>.<cluster_domain/*`, Fill it in depending your situation

Name [?](#) :

Display name [?](#) :

Logo [?](#) :   
URL [?](#) : 

Home [?](#) :

Description [?](#) :

Organization [?](#) :

Client ID [?](#) :

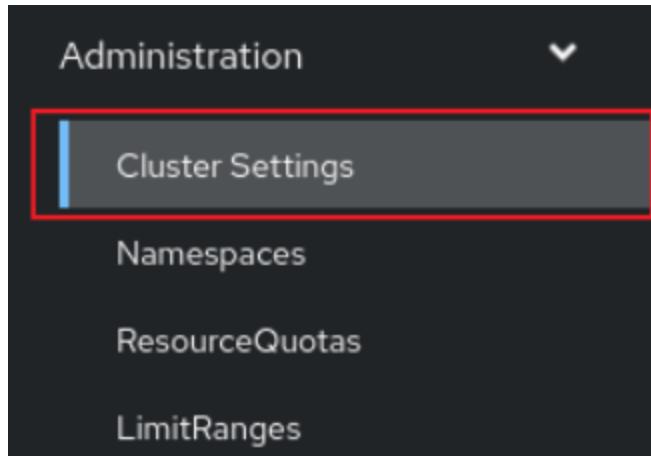
Client secret [?](#) :

Cert [?](#) :

Redirect URLs [?](#) :   
Redirect URLs [Add](#)

## Step2. Openshift Oauth Configuration

Now, login into the Openshift Console as Kubeadmin. Once you are logged In. Browse to the side menu, locate the Cluster settings



Under Global Configuration You will see Oauth

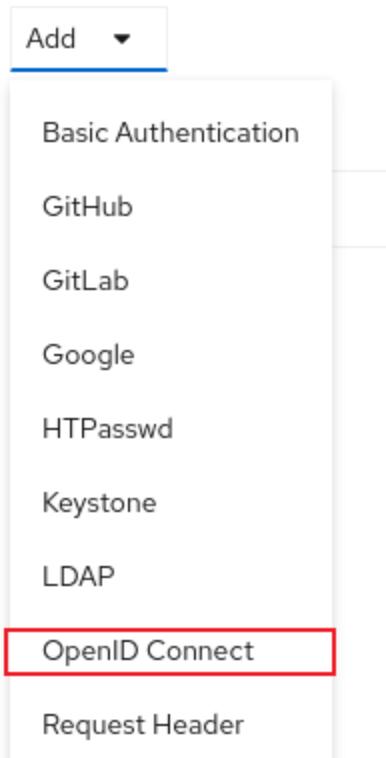
OAuth

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).

You will see the Identity Provider section. In ADD section, select the OpenID Connect from options.

## Identity providers

Identity providers determine ho



Configure OIDC, note following points.

- Fill in the `Client ID` and `Client Secret` remembered in the previous step.
- The Issuer URL must use https, with the form `https://<casdoor-host>`, again depending on your situation

## 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 \*

\*\*\*\*\*

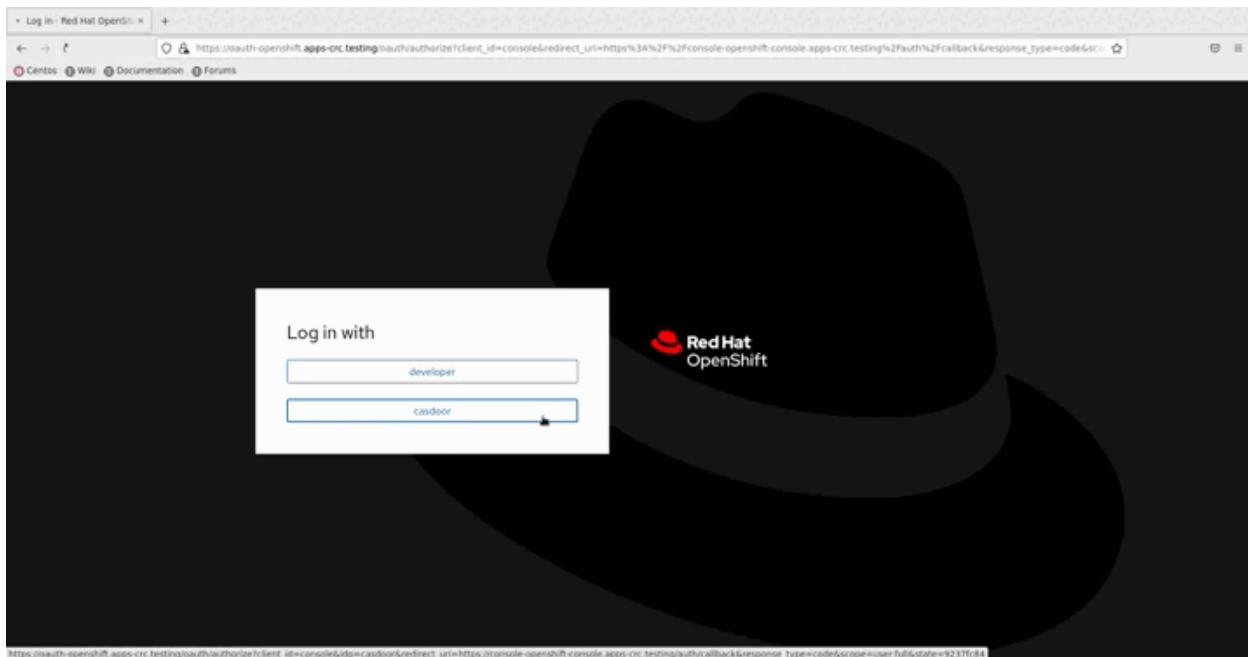
Issuer URL \*

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.

## Step3. Test OIDC Authentication

Access the Openshift console in the browser. You will see casdoor (The Name you configured in the previous step). Click on the casdoor login option. You will get redirected to the Casdoor login page.



# BookStack

## Using Casdoor for authentication in BookStack

[BookStack](#) is an open source book and document sharing site, as well as an open source application developed using the Go language to help you better achieve document reading management.

Bookstack-casdoor has been integrated with Casdoor, and you can now start quickly with a simple configuration.

### Step1. Create an Casdoor application

Go to your Casdoor and add your new application BookStack. Here is an example of creating the BookStack application in Casdoor.

Edit Application Save Save & Exit

Name ? : bookstack

Display name ? : bookstack

Logo ? : URL ? : [https://cdn.casdoor.com/logo/casdoor-logo\\_1185x256.png](https://cdn.casdoor.com/logo/casdoor-logo_1185x256.png)

Preview: 

Home ? :

Description ? :

Organization ? : [REDACTED]

Client ID ? : [REDACTED]

Client secret ? : [REDACTED]

Please remember the Name, Organization, client ID, and client Secret. You will use them in the next step.

## Step2. Configure Casdoor Login

Now, please move to the BookStack. Find the file: oauth.conf.example.

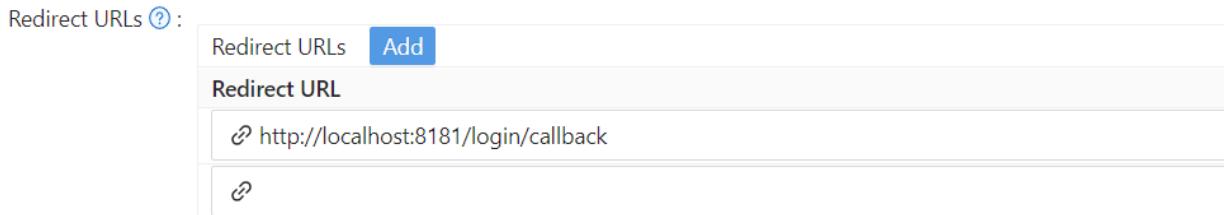
Rename oauth.conf.example to oauth.conf and modify the configuration. The content of which by default is:

```
[oauth]
```

```
casdoorOrganization = <"Organization">
casdoorApplication = "bookstack"
casdoorEndpoint = http://localhost:8000
clientId = <client ID>
clientSecret = <client Secret>
redirectUrl = http://localhost:8181/login/callback
```

## Step3. Fill in the `redirectUrl` in Casdoor

The last step, go back to the page where you added the BookStack application, and fill in the `Redirect URLs`. Make sure the `Redirect URL` is the same as the `redirectUrl` in the file `oauth.conf`.



The screenshot shows a configuration interface for 'Redirect URLs'. At the top, there's a header 'Redirect URLs ?' with a question mark icon. Below it is a button labeled 'Add'. A table follows, with a single row containing a column labeled 'Redirect URL' and a value cell containing the URL 'http://localhost:8181/login/callback'. There is also a small link icon next to the URL.

Now that you've done all the configuration for Casdoor!

You can go back to your BookStack and experience using Casdoor for login authentication once the BookStack has been successfully deployed.

# Bytebase

Casdoor can use OAuth2 to connect various applications. Here we will use Bytebase as an example to show you how to use OAuth2 to connect to your applications.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Bytebase_HOSTNAME`: Domain name or IP where Bytebase is deployed.

## Step1. Deploy Casdoor and Bytebase

Firstly, the Casdoor and Bytebase should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. You can set `CASDOOR_HOSTNAME = http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find a redirect url: `<CASDOOR_HOSTNAME>/oauth/callback`
3. Add your redirect url to casdoor application:

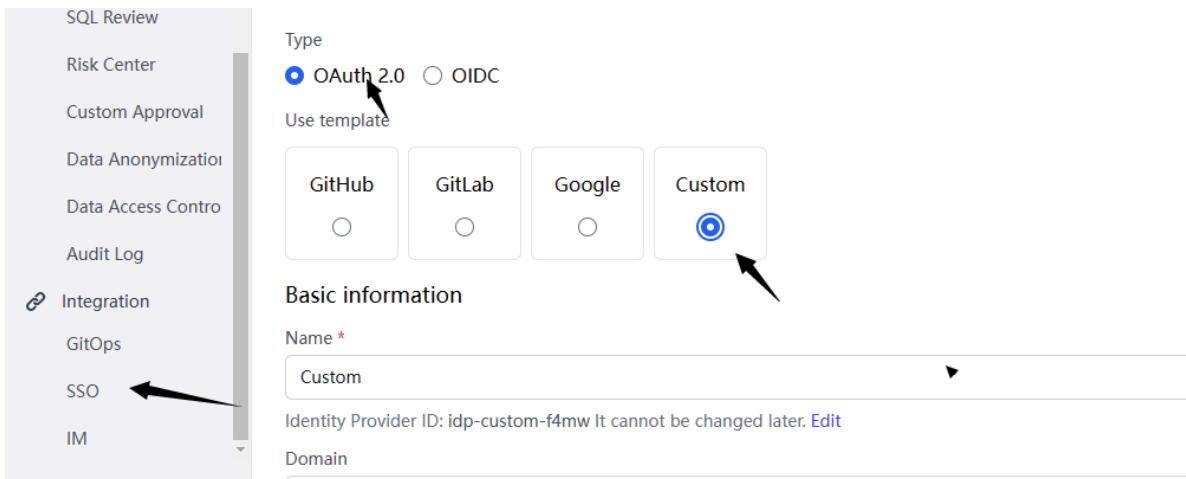
The screenshot shows the Casdoor application settings page. It includes fields for Client ID (e828fd6922f4292b979e), Client secret (bab9f6c2fad67471e1bd81e074ea192e4f46dd), Cert (cert-built-in), and Redirect URLs (Redirect URLs: <CASDOOR\_HOSTNAME>/oauth/callback). There is also a table for Redirect URLs with one entry: <CASDOOR\_HOSTNAME>/oauth/callback.

Not surprisingly, you can get two values on the application settings page: `Client ID` and `Client secret` like the picture above, we will use them in the next step.

Open your favorite browser and visit: `http://<CASDOOR_HOSTNAME>/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure Bytebase

1. You should find sso and use OAuth 2.0



2. You should config this app

The screenshot shows the Casdoor application interface. On the left, there's a sidebar with various navigation items like 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. Under the SSO section, there's a sub-menu for 'SSO > casdoor'. The main area displays 'Basic Information' for the 'casdoor' provider, including fields for Name (set to 'casdoor'), Identity Provider ID (set to 'idp-casdoor-mels'), Domain (set to 'http://101.43.192.216:8000'), and Client ID (set to 'e828fd992342926979e'). Below these are sections for 'Identity provider information' (Auth URL: 'http://101.43.192.216:8000/login/oauth/authorize', Scopes: 'openid profile email'), 'Token URL' (set to 'http://101.43.192.216:8000/api/login/oauth/access\_token'), and 'User information URL' (set to 'http://101.43.192.216:8000/api/get-account'). There's also a 'User information mapping' section where field names from the user API are mapped to Bytebase user fields. At the bottom, there are buttons for 'Test Connection', 'Archive this SSO', 'Discard changes', and 'Update'.

3. You can find Client Id and Client Secret in Casdoor application page.

- 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`

Log out of Bytebase, and test SSO.

The screenshot shows the Bytebase login page. On the left, there's a large, colorful illustration of a rocket ship launching from a platform, with two cartoonish characters (one holding a flag) watching. On the right, the Bytebase logo is at the top, followed by input fields for 'Email' (containing 'jim@example.com') and 'Password'. Below the password field is a 'Forgot your password?' link. A large blue 'Sign In' button is centered. Below it, there's a 'New to Bytebase? Sign up' link and a 'Sign in with casdoor' button with a Casdoor icon. At the bottom, there are language links for 'English' and '简体中文' (Simplified Chinese), and a copyright notice: '© 2023 Bytebase. All rights reserved.'

# ELK

## Overview of casdoor/elk-auth-casdoor

One of the biggest drawbacks of ELK (Elasticsearch, Logstash and Kibana) is that originally, these products have no authentication mechanism, so that everyone can visit the kibana dashboard as long as he has the url of kibana, or ES urls. Later ELK integrated an embedded authentication system "Xpack", whose all advanced functions are not free (eg. Oauth, OIDC, LDAP, SAML), and only plain authentication (setting a set of accounts and passwords) is free of charge, which is quite inconvenient. We cannot just provide a unique account for everyone in a corporation.

Therefore, we have developed a elk authentication solution based on Casdoor, free of charge, open source and under maintenance, supporting lots of advanced features. Casdoor is a centralized authentication/ Single-Sign-On platform based on Oauth2.0/OIDC, and casdoor/elk-auth-casdoor is actually a reverse proxy, which is designed to intercept all http data flow toward the elk/kibana, and guides the users who haven't logged in to log in. This reverse proxy is completely transparent as long as the user has logged in.

If this user hasn't been correctly authenticated, the request will be temporally cached, and the user will be redirected to Casdoor login page. After user logs in through casdoor, the cached request will be restored and sent to kibana. So it's ok if a POST request (or something other than GET) is intercepted, and user won't need to refill the form and resend the request. The reverse proxy will remember it for you.

Location of casdoor/elk-auth-casdoor repository <https://github.com/casdoor/elk-auth-casdoor>

auth-casdoor

## How to run it?

0. have golang environment installed
1. go to [casdoor/elk-auth-casdoor](#) and fetch the code
2. register your proxy as an app of Casdoor.
3. modify the configuration

The configuration file locates in "conf/app.conf". Here is an example, and you should customize changes according to your real demands.

```
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. visit <http://localhost:8080> (in the example above), and log in following the guidance of redirection, and you shall see kibana protected and authenticated by casdoor.
5. If everything works well, don't forget to block the visits of original kibana's port coming from outside by configurating your firewall(or something else), so that outsiders can only visit kibana via this reverse proxy.

# Gitea

## Using Casdoor for authentication in Gitea

Gitea is a community managed lightweight code hosting solution written in Go. It is published under the MIT license.

Gitea supports 3rd-party authentication including Oauth, which makes it possible to use Casdoor to authenticate it. Here is the tutorial for achieving this.

### Preparations

To configure Gitea to use Casdoor as identification provider, you need to have Gitea installed as well as access to administrator account.

For more information about how to download, install and run Gitea see <https://docs.gitea.io/en-us/install-from-binary/>

You are supposed to create an administrator account during installation. If you didn't, the administrator will be the first registered user. Please use this account proceed the following procedures.

### 1. Create an Casdoor application

Like this

Edit Application

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 ⓘ: 3416238e1edf915eac08b8fe345b2b95cdba7e04

Cert ⓘ: cert-built-in

Redirect URLs

Action
Add
Redirect URL
http://localhost:3000/user/oauth2/Casdoor/callback
Actions: Up, Down, Delete

Please remember the client ID and client Secret for the next step.

Please don't fill in the callback url in this step. The url depends on the configurations on gitea in the next step. Later we will come back to set a correct callback url.

## 2. Configure Gitea to use Casdoor

Log in as administrator. Go to 'Site Administration' page via drop-down menu in the upper right corner. Then Switch to "Authentication Source" Page.

You are supposed to see something like this.

The screenshot shows the GitHub 'Authentication Sources' management interface. At the top, there's a navigation bar with links for Issues, Pull Requests, Milestones, Explore, and a notifications icon. Below that is a secondary navigation bar with links for Dashboard, User Accounts, Organizations, Repositories, Webhooks, Authentication Sources (which is underlined to indicate it's the active tab), User Emails, Configuration, System Notices, and Monitoring. The main content area is titled 'Authentication Source Management (Total: 0)' and contains a table with the following columns: ID, Name, Type, Enabled, Updated, Created, and Edit. A blue 'Add Authentication Source' button is located at the top right of the table area.

Press the "Add Authentication Source" Button, and fill in the form like this.

The screenshot shows the 'Add Authentication Source' form on GitHub. The form has the following fields:

- Authentication Type: OAuth2
- Authentication Name: Casdoor
- OAuth2 Provider: OpenID Connect
- Client ID (Key): 7ceb9b7fda4a9061ec1c
- Client Secret: 3416238e1edf915eac08b8fe345b2b95cdba7e04
- Icon URL: (empty)
- 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: (empty)

Please choose the authentication type as "oauth2".

Please input a name for this authentication source and remember this name. This name will be used for the callback\_url in the next step.

Please choose the `OpenID Connect` Oauth2 Provider.

Fill in the Client ID and Client Secret remembered in the previous step.

Fill in the openid connect auto discovery url, which is supposed to be `<your endpoint of casdoor>/.well-known/openid-configuration`.

Fill in the other optional configuration items as you wish. And then submit it.

Submit the form.

### 3. Configure the callback url in casdoor

Go back to the application edit page in step 2, and add the following callback url:

`<endpoint of gitea>/user/oauth2/<authentication source name>/callback`

The `<authentication source name>` is the name for authentication source in Gitea in the previous step.

### 4. Have a try on Gitea

Logout the current administrator account.

You are supposed to see this in login page:

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

Press the 'sign in with openid' button and you will be redirected to casdoor login page.

After login you will see this:

Explore   Help   [\[←\] Sign In](#)

Register New Account   [Link to Existing Account](#)

Complete New Account

Username \*

Email Address \*

admin@example.com

**Complete Account**

Follow the instructions and bind the casdoor account with a new gitea account or

existing account.

Then everything will be working correctly.

# Grafana

## Using Casdoor for authentication in Grafana

[Grafana](#) supports authentication via Oauth. Therefore it is extremely easy for users to use casdoor to log in in Grafana. Only several steps and simple configurations can achieve that.

Here is a tutorial to use Casdoor for authentication in Grafana. Before you proceed, please ensure that you have grafana installed and running.

### Step 1 Create an app for Grafana in Casdoor

Here is an example of creating an app in Casdoor

Edit Application Save Save & Exit

Name ⓘ: application\_9p7eai

Display name ⓘ: New Application - 9p7eai

Logo ⓘ:  URL ⓘ: [https://cdn.casbin.com/logo/logo\\_1024x256.png](https://cdn.casbin.com/logo/logo_1024x256.png)

Preview:



casbin

Home ⓘ: [/](#)

Description ⓘ:

Organization ⓘ: built-in

Client ID ⓘ: 7ceb9b7fda4a9061ec1c

Client secret ⓘ: 3416238e1edf915eac08b8fe345b2b95cd8a7e04

Cert ⓘ: cert-built-in

Redirect URLs ⓘ:

Action	Redirect URL
	<a href="http://localhost:3000/login/generic_oauth">http://localhost:3000/login/generic_oauth</a>

Please copy the client secret and client id for the next step.

Please add the callback url of Grafana. By default, Grafana's oauth callback is [/login/generic\\_oauth](/login/generic_oauth). So please concatenate this url correctly.

## Step 2: Modify the configuration of Grafana

By default the configuration file for oauth locates at `conf/defaults.ini` in the workdir of Grafana.

Please find the section `auth.generic_oauth` and modify the following field:

```
[auth.generic_oauth]
name = Casdoor
```

## About HTTPS

If you don't want HTTPS enabled for casdoor or if you deploy grafana without HTTPS enabled, please also set `tls_skip_verify_insecure = true`

## About redirectURI after Sign In With Casdoor

If the redirect uri is not right after Sign In with Casdoor in Grafana, you may want to configure [root\\_url](#)

```
[server]
http_port = 3000
# The public facing domain name used to access grafana from a
browser
domain = <your ip here>
# The full public facing url
root_url = %(protocol)s://%(domain)s:%(http_port)s/
```

related links:

1. [Grafana doc](#)
2. [Grafana defaults.ini](#)

## About Role Mapping:

You may want to configure role\_attribute\_path to map your user's role to Grafana via [role\\_attribute\\_path](#)

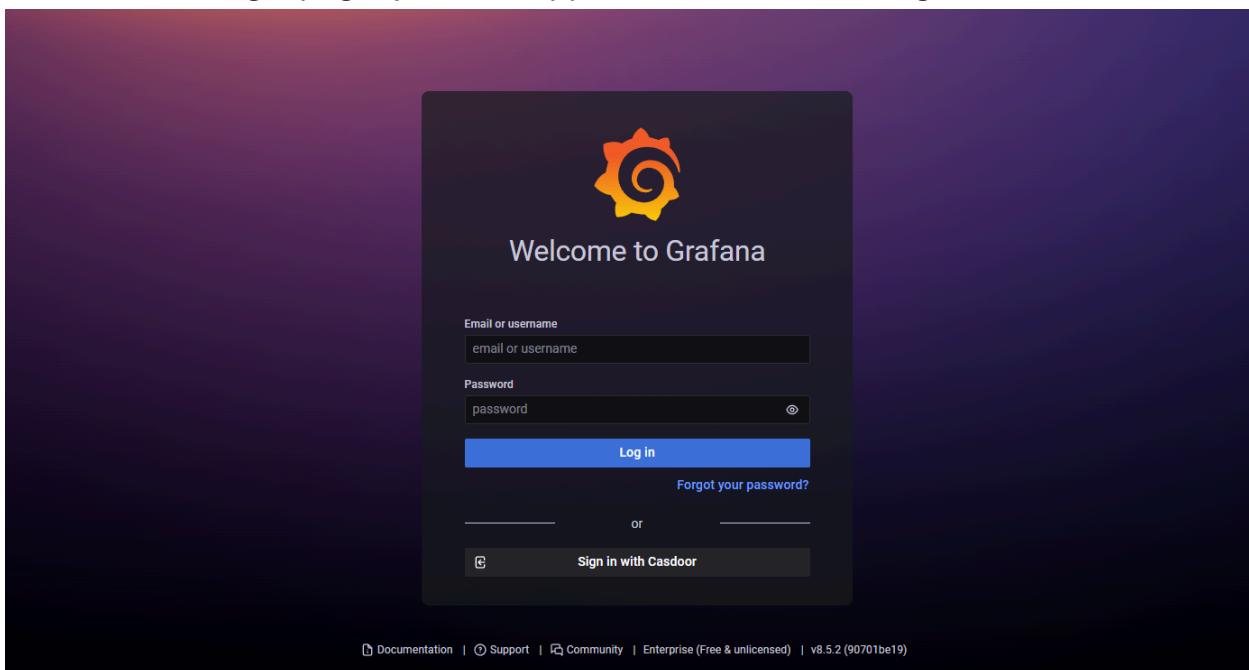
```
[auth.generic_oauth]
role_attribute_path = contains(roles[*].name, 'admin') && 'Admin'
```

the JMESPath expression after role\_attribute\_path is very important here. read grafana doc please

## Step3: See whether it works

Shutdown grafana and restart it.

Go to see the login page, you are supposed to see something like this



# MinIO

MinIO supports external identity management using an OpenID Connect (OIDC)-compatible provider. This document covers configuring Casdoor as identity provider to support with MinIO.

## Step1. Deploy Casdoor & MinIO

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

You can refer to [here](#) to deploy your MinIO server and [here](#) for MinIO client called `mc`.

## Step2. Configure Casdoor Application

1. Create or use an existing Casdoor application.

## 2. Add Your redirect url

The screenshot shows the Casdoor application settings interface. It includes fields for 'Client ID' (24a25ea0714d92e78595) and 'Client secret' (155...). Below these, there's a section for 'Redirect URLs' with a sub-section for 'Redirect URLs'. A button labeled 'Add' is visible, and a link to 'Add a redirect URL for spring security' is provided. A specific URL entry is shown: http://localhost:8082/ui-one/login/oauth2/code/custom.

Client ID	24a25ea0714d92e78595	Client ID
Client secret	155...	Client Secret
Redirect URLs	Add	Add a redirect URL for spring security
http://localhost:8082/ui-one/login/oauth2/code/custom		

## 3. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: `client ID` and `client secret` like the picture above, we will use them in next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## 4. This step is necessary for MinIO. As MinIO needs to use a claim attribute in JWT for its policy, you should configure it in casdoor as well. Currently, casdoor uses `tag` as a workaround for configuring MinIO's policy.

Tag ? : **readwrite**

You can find all supported policies [here](#).

## Step3. Configure MinIO

You can start a MinIO server by following commands:

```
export MINIO_ROOT_USER=minio  
export MINIO_ROOT_PASSWORD=minio123  
minio server /mnt/export
```

You can use parameter `--console-address` to configure the address and port.

Then you can add a service alias by MinIO client `mc`.

```
mc alias set myminio <You console address> minio minio123
```

Now, you can configure OpenID connect of MinIO. For Casdoor, the command is like the following:

```
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"
```

You can refer to [official document](#) for more detailed parameters.

Once successfully set, restart the MinIO instance.

```
mc admin service restart myminio
```

## Step4. Try the demo!

Now, you can open your MinIO console in the browser and click on `Login with SSO`.

You will be redirected to the casdoor user login page. Upon successful login you

will be redirected to MinIO page and logged in automatically and you should see now the buckets and objects they have access to.

 CAUTION

If you deploy frontend and backend of casdoor in different ports, the login page you are redirected to will be backend port and it will display `404 not found`. You can modify the port to the frontend one. Then you can access to casdoor login page successfully.

# Java

## Spring Boot

Using Casdoor in Spring Boot project

## Spring Cloud

Using Casdoor in Spring Cloud

## Spring Cloud Gateway

Using Casdoor in Spring Cloud Gateway

## Spring Security

2 items

 Jenkins Plugin

Using Casdoor plugin for your Jenkins security

 Jenkins OIDC

Using OIDC protocol as IDP to connect various applications, like Jenkins

 Jira

2 items

 Confluence

Using OIDC protocol as IDP to connect various applications, like Confluence

 RuoYi

Using Casdoor in RuoYi-Cloud



## Pulsar-manager

Using Casdoor in Pulsar-manager



## ShenYu

Using Casdoor in ShenYu



## ShardingSphere

Using Casdoor in ShardingSphere



## Apache IoTDB

Using Casdoor Apache IoTDB



## Apache DolphinScheduler

Using Casdoor for DolphinScheduler SSO login

 **FireZone**

Using OIDC protocol as IDP to connect various applications, like FireZone

 **CloudFoundry**

Learn how to integrate Casdoor with CloudFoundry to secure your applications

 **Thingsboard**

Learn how to integrate Casdoor with Thingsboard to secure your applications

# Spring Boot

[casdoor-spring-boot-example](#) is an example of how to use [casdoor-spring-boot-starter](#) in SpringBoot project. We will show you the steps below.

## Step1. Deploy Casdoor

Firstly, the 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, you need to ensure:

- Open your favorite browser and visit <http://localhost:8000>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor-based login page in your own app with the following steps.

## Step2. Import casdoor-spring-boot-starter

You can import the casdoor-spring-boot-starter with maven or gradle.

Maven      Gradle

```
<!-- 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>
```

```
// https://mvnrepository.com/artifact/org.casbin/casdoor-spring-boot-starter
```

```
implementation group: 'org.casbin', name: 'casdoor-spring-boot-starter', version: '1.x.y'
```

## Step3. Init Config

Initialization requires 6 parameters, which are all string type.

Name (in order)	Must	Description
endpoint	Yes	Casdoor Server Url, such as <code>http://localhost:8000</code>
clientId	Yes	Application.client_id
clientSecret	Yes	Application.client_secret
certificate	Yes	Application.certificate

Name (in order)	Must	Description
organizationName	Yes	Application.organization
applicationName	No	Application.name

You can use Java properties or YAML files to init as below.

[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
```

### ⚠ CAUTION

You should replace the configuration with your own Casdoor instance, especially the `clientId`, `clientSecret` and the `jwtPublicKey`.

## Step4. Redirect to the login page

When you need the authentication who access your app, you can send the target url and redirect to the login page provided by Casdoor.

Please be sure that you have added the callback url (e.g. `http://localhost:8080/login`) in application configuration in advance.

```
@Resource  
private CasdoorAuthService casdoorAuthService;  
  
@RequestMapping("toLogin")  
public String toLogin() {  
    return "redirect:" +  
casdoorAuthService.getSigninUrl("http://localhost:8080/login");  
}
```

## Step5. Get token and parse

After Casdoor verification passed, it will be redirected to your application with code and state.

You can get the code and call `getOAuthToken` method, then parse out jwt token.

`CasdoorUser` contains the basic information about the user provided by Casdoor. You can use it as a keyword to set the session in your application.

```
@RequestMapping("login")  
public String login(String code, String state, HttpServletRequest  
request) {
```

# Service

Examples of APIs are shown below.

- 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());
```

## What's more

You can explore the following projects/docs to learn more about the integration of Java with Casdoor.

- [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

Under the Spring Cloud microservice system, general authentication occurs at the gateway. Please refer to [casdoor-springcloud-gateway-example](#).

If you want to use Casdoor in a single service, you can refer to [casdoor-spring-boot-example](#).

No matter in the gateway layer or in the single service, both use [casdoor-spring-boot-starter](#).

## What's more

You can explore the following projects/docs to learn more about the integration of Java with Casdoor.

- [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](#) is an example on how to use [casdoor-spring-boot-starter](#) as a OAuth2 plugin in Spring Cloud Gateway. We will show you the steps below.

## Step1. Deploy Casdoor

Firstly, the 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, you need to ensure:

- Open your favorite browser and visit <http://localhost:8000>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2: Init a Spring Cloud Gateway

You can use the code of this example directly or combine your own business code.

We need a gateway service and at least one business service.

In this example, `casdoor-gateway` as the gateway service and `casdoor-api` as the business service.

## Step3: Include the dependency

Add `casdoor-spring-boot-starter` to the Spring Cloud Gateway project.

For 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>
```

For Gradle:

```
// https://mvnrepository.com/artifact/org.casbin/casdoor-spring-boot-starter
implementation group: 'org.casbin', name: 'casdoor-spring-boot-starter', version: '1.x.y'
```

## Step4: Configure your properties

Initialization requires 6 parameters, which are all string type.

Name (in order)	Must	Description
endpoint	Yes	Casdoor Server Url, such as <code>http://localhost:8000</code>
clientId	Yes	Application.client_id
clientSecret	Yes	Application.client_secret
certificate	Yes	Application.certificate
organizationName	Yes	Application.organization
applicationName	No	Application.name

You can use Java properties or YAML files to init as below.

For properties:

```
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
```

For yaml:

```
casdoor:
  endpoint: http://localhost:8000
  client-id: <client-id>
```

In addition, you need to configure Gateway Routing. For yaml:

```
spring:
  application:
    name: casdoor-gateway
  cloud:
    gateway:
      routes:
        - id: api-route
          uri: http://localhost:9091
          predicates:
            - Path=/api/**
```

## Step5: Add the CasdoorAuthFilter

Add an implementation class of GlobalFilter to the gateway for identity verification, such as CasdoorAuthFilter in this example.

If the authentication fails, it returns to the front end 401 to jump to the login interface.

```
@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) {
```

# Step6: Get the Service and use

Now provide 5 services: `CasdoorAuthService`, `CasdoorUserService`, `CasdoorEmailService`, `CasdoorSmsService` and `CasdoorResourceService`.

You can create them as below in Gateway project.

```
@Resource  
private CasdoorAuthService casdoorAuthService;
```

When you need the authentication who access your app, you can send the target url and redirect to the login page provided by Casdoor.

Please be sure that you have added the callback url (e.g. `http://localhost:9090/callback`) in application configuration in advance.

```
@RequestMapping("login")  
public Mono<String> login() {  
    return Mono.just("redirect:" +  
        casdoorAuthService.getSigninUrl("http://localhost:9090/callback"));  
}
```

After Casdoor verification passed, it will be redirected to your application with code and state.

You can get the code and call `getOAuthToken` method, then parse out jwt token.

`CasdoorUser` contains the basic information about the user provided by Casdoor, you can use it as a keyword to set the session in your application.

```

@RequestMapping("callback")
public Mono<String> callback(String code, String
state, ServerWebExchange exchange) {
    String token = "";
    CasdoorUser user = null;
    try {
        token = casdoorAuthService.getOAuthToken(code, state);
        user = casdoorAuthService.parseJwtToken(token);
    } catch(CasdoorAuthException e) {
        e.printStackTrace();
    }
    CasdoorUser finalUser = user;
    return exchange.getSession().flatMap(session -> {
        session.getAttributes().put("casdoorUser", finalUser);
        return Mono.just("redirect:/");
    });
}

```

Examples of APIs are shown below.

- 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());

## Step7: Restart project

After start, open your favorite browser and visit <http://localhost:9090>, then click any button which can request resources from casdoor-api.



# Casdoor

[Get Resource](#)

[Update Resource](#)

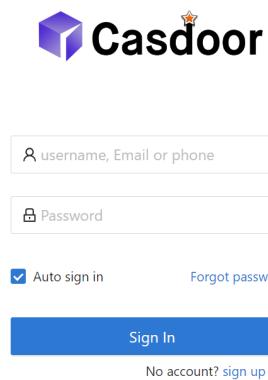
The gateway authentication logic will be triggered. Since you are not logged in, you will jump to the login interface. Click Login Button.



# Click to login

[Login](#)

You can see the unified login platform of Casdoor.



After successful login, it will jump to the main interface. Then you can click any button.



"success get resource1"

## What's more

You can explore the following projects/docs to learn more about the integration of Java with Casdoor.

- [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 Security

## Spring Security OAuth

Using Spring Security as an example to show how to use OIDC to connect to your applications

## Spring Security Filter

Based on Spring Security Filter, how to use OIDC to connect your application.



# Spring Security OAuth

Casdoor can use OIDC protocol as IDP to connect various applications. Here we will use Spring Security as an example to show you how to use OIDC to connect to your applications.

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add Your redirect url (You can see more details about how to get redirect url in the next section)

Client ID <a href="#">?</a> :	24a25ea0714d92e78595	Client ID
Client secret <a href="#">?</a> :	155 [REDACTED]	Client Secret
Redirect URLs <a href="#">?</a> :	Redirect URLs	Add
	Redirect URL	Add a redirect URL for spring security
	🔗 http://localhost:8082/ui-one/login/oauth2/code/custom	

3. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: Client ID and Client secret like the picture above. We will use them in next step.

Open your favorite browser and visit: [http://CASDOOR\\_HOSTNAME/.well-known/openid-configuration](http://CASDOOR_HOSTNAME/.well-known/openid-configuration), you will see the OIDC configure of Casdoor.

# Step3. Configure Spring Security

Spring Security natively support OIDC.

You can customize the settings of Spring Security OAuth2 Client:

**CAUTION**

You should replace the configuration with your own Casdoor instance, especially the <Client ID> and others.

## application.yml      application.properties

spring:

```
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
```

#### CAUTION

For default situation of Spring Security, the <Redirect URL> should be like `http://<Your Spring Boot Application Endpoint>/<Servlet Prefix if it is configured>/login/oauth2/code/custom`. For example, in the following demo, the redirect URL should be `http://localhost:8080/login/oauth2/code/custom`.

You should also configure this in `casdoor` application.

You can also customize the settings by `ClientRegistration` in your code. You can find the mapping [here](#)

# Step4. Get Started with A Demo

1. We can create a Spring Boot application.
2. We can add a configuration which protects all endpoints except `/` and `/login**` for users to log in.

```
@EnableWebSecurity
public class UiSecurityConfig extends WebSecurityConfigurerAdapter {

    @Override
    protected void configure(HttpSecurity http) throws Exception {
        http.authorizeRequests().antMatchers("/", "/login**").permitAll().anyRequest().authenticated().and()
            .oauth2Login();

    }
}
```

3. We can add a naive page for user to log in.

```
<!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">
```

When user clicks the `login` button, he will be redirected to `casdoor`.

4. Next, we can define our protected resources. We can export an endpoint called `/foos` and a web page for display.

## Data Model

```
public class FooModel {  
    private Long id;  
    private String name;  
  
    public FooModel(Long id, String name) {  
        super();  
        this.id = id;  
        this.name = name;  
    }  
    public Long getId() {  
        return id;  
    }  
    public void setId(Long id) {  
        this.id = id;  
    }  
    public String getName() {  
        return name;  
    }  
    public void setName(String name) {  
        this.name = name;  
    }  
}
```

## Controller

```
@Controller  
public class FooClientController {  
    @GetMapping("/foos")  
    public String getFoos(Model model) {
```

## Web page

```
<!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>
                <tr>
                    <td>ID</td>
                    <td>Name</td>
                </tr>
            </thead>
            <tbody>
                <tr th:if="${foos.empty}">
                    <td colspan="4">No foos</td>
                </tr>
                <tr th:each="foo : ${foos}">
```

**⚠ CAUTION**

All the web page template should be put under `resources/templates`.

## Step5. Try the demo!

Firstly, you can try to open your favorite browser and directly visit `/foos`. It will automatically redirect to casdoor's login page. You can log in here or from the root page.

If you visit your root page,

Spring OAuth Client Thymeleaf - 1

Welcome !  
[Login](#)

Click the `login` button and the page will redirect to casdoor's login page.



username, Email or phone

Password

Auto sign in      [Forgot password?](#)

[Sign In](#)

[Sign in with code](#)    No account? [sign up now](#)

After you log in, the page will redirect to </foos>.

Spring OAuth Client Thymeleaf -1

Hi, [user](#)

Your Username

### All Foos:

ID	Name
1	a
2	b
3	c

# Spring Security Filter

Casdoor can use OIDC protocol as IDP to connect various applications. Here, we will use the filter in spring security to integrate casdoor and show you how to connect to the application using oidc.

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add Your redirect url (You can see more details about how to get redirect url in the next section).

Name [?](#) : application\_a6ftas → your application name

Display name [?](#) : New Application - a6ftas

Logo [?](#) : URL [?](#) : [https://cdn.casbin.org/img/casdoor-logo\\_1185x256.png](https://cdn.casbin.org/img/casdoor-logo_1185x256.png)

Preview: 

Home [?](#) :

Description [?](#) :

Organization [?](#) : organization\_carg1b → your organization name

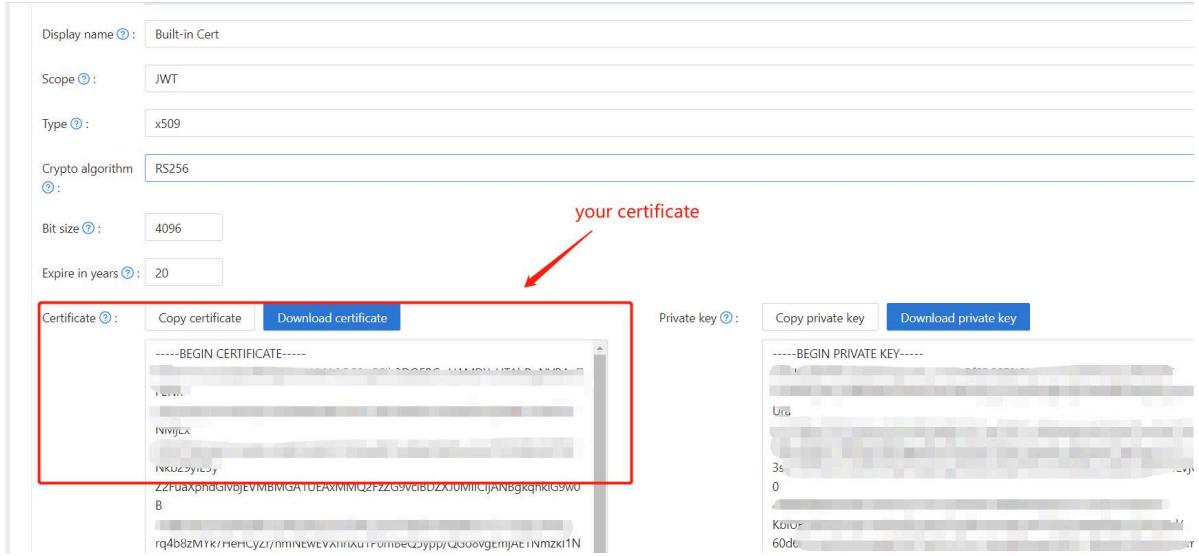
Client ID [?](#) : 3ed7314825ecf955cb19 → your client id

Client secret [?](#) : ee9314ea228... → your client secret

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

Redirect URLs [?](#) : Redirect URLs Add  
Redirect URL → your redirect url  
<http://localhost:3000/callback>

3. On the certificate editing page, you can see your Certificate.



#### 4. Add provider you want and supplement other settings.

Not surprisingly, you can get these values on the application settings page:

`Application Name`, `Organization Name`, `Redirect URL`, `Client ID`, `Client Secret`, `Certification`. As shown above, we will use them in the next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure Spring Security

You can customize the settings of spring security filters to process tokens:

### ⚠ CAUTION

You should replace the configuration with your own Casdoor instance especially the `<Client ID>` and others.

```
server:  
port: 8080
```

### CAUTION

For frontend applications, the default value of `<FRONTEND_HOSTNAME>` is `localhost:3000`.

For example, in the following demo, the redirect URL should be `http://localhost:3000/callback`.

You should also configure this in `casdoor` application.

## Step4. Configure Frontend

You need to install `casdoor-js-sdk` and configure `SDK`.

1. Install `casdoor-js-sdk`.

```
npm i casdoor-js-sdk
# or
yarn add casdoor-js-sdk
```

2. Set up `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",
```

# Step5. Get Started with A Demo

1. We can create a Spring Boot application.
2. We can add some configurations to handle JWT.

```
@EnableWebSecurity
public class SecurityConfig {

    private final JwtTokenFilter jwtTokenFilter;

    public SecurityConfig(JwtTokenFilter jwtTokenFilter) {
        this.jwtTokenFilter = jwtTokenFilter;
    }

    @Bean
    public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {
        // enable CORS and disable CSRF
        http = http.cors(corsConfig -> corsConfig
            .configurationSource(configurationSource())
            .csrf().disable());

        // set session management to stateless
        http = http
            .sessionManagement()

        .sessionCreationPolicy(SessionCreationPolicy.STATELESS)
            .and();

        // set permissions on endpoints
        http.authorizeHttpRequests(authorize -> authorize
            .mvcMatchers("/api/redirect-url", "/api/
signin").permitAll()
            .mvcMatchers("/api/**").authenticated()
        );
    }
}
```

3. We can add a simple JWT filter to intercept requests that need to verify tokens.

```
@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 {
        // get authorization header and validate
        final String header =
request.getHeader(HttpHeaders.AUTHORIZATION);
        if (!StringUtils.hasText(header) ||
header.startsWith("Bearer ")) {
            chain.doFilter(request, response);
            return;
        }

        // get jwt token and validate
        final String token = header.split(" ")[1].trim();

        // get user identity and set it on the spring security
        context
        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;
        }
    }
}
```

When the user accesses the interface requiring authentication, `JwtTokenFilter` will obtain the token from the request header `Authorization` and verify it.

4. Next, we need to define a `Controller` to handle that when the user login to the `casdoor`, it will be redirected to the server and carry the `code` and `state`. The server needs to verify the user's identity from the `casdoor` and obtain the `token` through these two parameters.

```
@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());
        }
    }

    // ...
}
```

## Step6. Try the demo!

First, you can try to access the frontend application through the browser. If you have not logged in, it will display a login button. Click the login button, and you will be redirected to the `casdoor` login page.

If you visit your root page,

---

`Casdoor Login`

Click the `Casdoor Login` button and the page will redirect to casdoor's login page.



username, Email or phone

Password

Auto sign in      [Forgot password?](#)

[Sign In](#)

No account? [sign up now](#)

---

Made with ❤ by **Casdoor**

After you log in, the page will redirect to [/](#).

---



New User - rtsbx4

[Logout](#)

# Jenkins Plugin

Casdoor provides a plugin for users to login Jenkins. Here we will show you how to use Casdoor plugin for your Jenkins security.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`JENKINS_HOSTNAME`: Domain name or IP where Jenkins is deployed.

## Step1. Deploy Casdoor and Jenkins

Firstly, the [Casdoor](#) and [Jenkins](#) should be deployed.

After a successful deployment, you need to ensure:

1. Set Jenkins URL([Manage Jenkins](#) → [Configure System](#) → [Jenkins Location](#)) to `JENKINS_HOSTNAME`.

The screenshot shows the Jenkins 'Dashboard' > 'configuration' page. 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. Casdoor can be logged in and used normally.
3. Set Casdoor's `origin` value (conf/app.conf) to `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
```

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://JENKINS_HOSTNAME/securityRealm/finishLogin`

The screenshot shows the Casdoor application settings page. It includes fields for:

- Description: Casdoor for Jenkins
- Organization: built-in
- Client ID: bbd0bd66696e504dec59
- Client secret: d2de01b01...110b47465c
- Redirect URLs:
  - Redirect URLs: Add
  - Redirect URL: http://10.144.125.123:6780/securityRealm/finishLogin (with a note: Add a redirect url for Jenkins JENKINS\_HOSTNAME)

3. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: Client

`ID` and `Client secret` like the picture above, we will use them in next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure Jenkins

Now, you can install Casdoor plugin from the market or by uploading its `.jar` file.

After completing the installation, go to Manage Jenkins → Configure Global Security.

Suggestion: Back up the Jenkins `config.xml` file, and use it to recover in case of setup errors.

The screenshot shows the Jenkins 'Configure Global Security' page. Under the 'Authentication' section, there is a checkbox for 'Disable remember me'. In the 'Security Realm' section, a radio button is selected for 'Casdoor Authentication Plugin'. The 'Casdoor Endpoint' field is filled with a placeholder URL. Below it, error messages indicate that 'Casdoor Endpoint is required.' and 'Client Id is required.' The 'Client ID' and 'Client Secret' fields are empty, with corresponding error messages: 'Client Id is required.' and 'Client Secret is required.'. The 'JWT Public Key' field is also empty, with the error message 'Jwt Public Key is required.' The 'Organization Name' and 'Application Name' fields are empty. At the bottom, there are 'Save' and 'Apply' buttons, and an 'Advanced...' link.

1. In Security Realm, select "Casdoor Authentication Plugin".
2. In Casdoor Endpoint, specify the `CASDOOR_HOSTNAME` noted above.

3. In Client ID, specify the `Client ID` noted above.
4. In Client secret, specify the `Client secret` noted above.
5. In JWT Public Key, specify the public key used to validate JWT token. You can find the public key in Casdoor by clicking `Cert` at the top. After clicking `edit` your application, you can copy your public key in the following page.

The screenshot shows the Casdoor interface with the 'Certs' tab selected. On the left, there's a form for editing a certificate named 'cert-built-in'. The 'Scope' is set to 'JWT'. The 'Type' is 'x509' and 'Crypto algorithm' is 'RSA'. The 'Bit size' is 4096 and 'Expire in years' is 20. Below the form, there are two large text areas representing the public and private keys, each with a 'Copy private key' or 'Download private key' button. A red arrow labeled '1' points to the 'Certs' tab in the top navigation. A red arrow labeled '2' points to the 'Copy public key' button.

6. Organization Name and Application Name is optional. You can specify your organization and application to verify users in other organizations and applications. If they are empty, the plugin will use the default organization and application.
7. In the Authorization section, check “Logged-in users can do anything”. Disable “Allow anonymous read access”.
8. Click `save`.

Now, Jenkins will automatically redirect you to Casdoor for authentication.

# Jenkins OIDC

Casdoor can use OIDC protocol as IDP to connect various applications. Here we will use Jenkins as an example to show you how to use OIDC to connect to your applications.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`JENKINS_HOSTNAME`: Domain name or IP where Jenkins is deployed.

## Step1. Deploy Casdoor and Jenkins

Firstly, the [Casdoor](#) and [Jenkins](#) should be deployed.

After a successful deployment, you need to ensure:

1. Set Jenkins URL([Manage Jenkins](#) → [Configure System](#) → Jenkins Location) to `JENKINS_HOSTNAME`.

Dashboard > configuration

**Jenkins Location**

Jenkins URL  
 ?

JENKINS\_HOSTNAME  
 ?

**Serve resource files from another domain**

Resource Root URL  
 ?

Without a resource root URL, resources will be served from the Jenkins URL with Content-Security-Policy set.

**Global properties**

Environment variables

**Save** **Apply**

2. Casdoor can be logged in and used normally.
3. Set Casdoor's `origin` value (conf/app.conf) to `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
```

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://JENKINS_HOSTNAME/securityRealm/finishLogin`

Description [?](#): Casdoor for Jenkins

Organization [?](#): built-in

Client ID [?](#): bbd0bd66696e504dec59 Client ID

Client secret [?](#): d2de01b01 [REDACTED] 110b47465c Client secret

Redirect URLs [?](#):

Redirect URLs	Add
Redirect URL	<a href="http://10.144.125.123:6780/securityRealm/finishLogin">http://10.144.125.123:6780/securityRealm/finishLogin</a> <span style="color: red;">Add a redirect url for Jenkins</span>
	JENKINS_HOSTNAME

3. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: Client ID and Client secret like the picture above, we will use them in the next step.

Open your favorite browser and visit: [http://CASDOOR\\_HOSTNAME/.well-known/openid-configuration](http://CASDOOR_HOSTNAME/.well-known/openid-configuration), you will see the OIDC configure of Casdoor.

## Step3. Configure Jenkins

First, we need to install [OpenId Connect Authentication](#), Jenkins does not natively support OIDC.

After completing the installation, go to [Manage Jenkins → Configure Global Security](#).

The screenshot shows the Jenkins 'Manage Jenkins' interface. In the top left, there are links for 'User List', 'Build History', and 'Manage Jenkins'. A red box highlights the 'Manage Jenkins' link. Below it are 'My Views' and '构建队列' (Build Queue) which shows '队列中没有构建任务' (No builds in queue). Under '构建执行状态' (Build Execution Status), it shows '1 空闲' (1 idle) and '2 空闲' (2 idle). The main area is titled 'System Configuration' and contains several sections: 'Configure System' (Configure global settings and paths), 'Global Tool Configuration' (Configure tools, their locations and automatic installers), 'Manage Nodes and Clouds' (Add, remove, control and monitor the various nodes that Jenkins runs jobs on), 'Manage Plugins' (Add, remove, disable or enable plugins that can extend the functionality of Jenkins), 'Security' (Configure Global Security, Manage Credentials, Configure Credential Providers), and a 'TIP' section.

### TIP

Back up the Jenkins `config.xml` file, and use it to recover in case of setup errors.

1. In Access Control, Security Realm select `Login with Openid Connect`.
2. In Client ID, specify the `Client ID` noted above.
3. In Client secret, specify the `Client secret` noted above.
4. In Configuration mode, select `Automatic configuration` and fill in `http://CASDOOR_HOSTNAME/well-known/openid-configuration` into Well-known configuration endpoint.

**Security Realm**

Delegate to servlet container  
 Jenkins' own user database  
 Login with Openid Connect Select this

**Client id**

bbd0bd66696e504dec59	<b>Input your Client ID</b>	<span style="color:red">?</span>
----------------------	-----------------------------	----------------------------------

**Client secret**

Concealed	<b>Input your Client secret</b>	<span style="color:red">?</span>
-----------	---------------------------------	----------------------------------

**Change Password**

**Configuration mode**

Automatic configuration  
 Well-known configuration endpoint  
 Manual configuration

**CASDOOR HOSTNAME**

**http://10.144.1.2:8000/.well-known/openid-configuration**

If your casdoor is deployed locally, you may need to select **Manual configuration** and input some information:

- 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**

**Configuration mode**

Automatic configuration  
 Manual configuration

**Token server url**

<b>http://10.144.1.2:8000/api/login/oauth/access_token</b>	<span style="color:red">?</span>
--	----------------------------------

**CASDOOR HOSTNAME**

**Authorization server url**

<b>http://10.144.1.2:8000/login/oauth/authorize</b>	<span style="color:red">?</span>
---	----------------------------------

**UserInfo server url**

<b>http://10.144.1.2:8000/api/get-account</b>	<span style="color:red">?</span>
---	----------------------------------

**Scopes**

<b>address phone openid profile offline_access email</b>	<span style="color:red">?</span>
--	----------------------------------

## 5. Click Advanced setting, fill in the following:

- In User name field, specify **name**

- In Full name field, specify `displayName`
- In Email field, specify `email`

User name field name

Full name field name

Email field name

Groups field name ?

Token Field Key To Check ?

6. In the Authorization section, check “Logged-in users can do anything”. Disable “Allow anonymous read access”. You can configure more complex authorization later, for now check if OpenID actually works.

Log out of Jenkins, it should now redirect you to Casdoor for authentication.



Auto sign in      [Forgot password?](#)  
  
[Sign in with code](#)    [No account? sign up now](#)

---

G

# Jira

## Via Built-in SSO

Using OIDC protocol as IDP to connect various applications, like Jira

## Via miniOrange Plugin

Using OIDC protocol as IDP to connect various applications, like Jira

# Via Built-in SSO

This is a free method to connect casdoor, but your website must use https;

Casdoor can use OIDC protocol as IDP to connect various applications. Here is a [Jira](#) tutorial.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Jira_HOSTNAME`: Domain name or IP where Jira is deployed.

## Step1. Deploy Casdoor and Jira

Firstly, the [Casdoor](#) and [Jira](#) should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. You can set `CASDOOR_HOSTNAME = http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find Authentication methods:

The screenshot shows the Jira Software Administration interface. The left sidebar has sections like Applications, Projects, Issues, Manage apps, User management, and System (which is selected). The main content area is titled "Authentication methods". It includes a warning about making authentication safer, a table of login options (Username and password, casdoor), and a section for "Authentication on API calls". A red box highlights the "Authentication methods" link in the sidebar, and another red box highlights the "System" tab in the top navigation bar.

### 3. Add a Configure and choose OpenId Connection signle sign-on in Authentication method

#### 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. Find the redirect url:

Give these URLs to your identity provider

Redirect URL

<https://test.v2tl.com/plugins/servlet/oidc/callback>



Location where the client is sent to after successful account authentication.

## 5. Add a redirect url:

The screenshot shows the Casdoor application settings page. It includes fields for Client ID (642ec5d6779a2f0e879d), Client secret (26cb47985c47ae3844580536ce2f59872969e109), Cert (cert-built-in), and a Redirect URLs section. The Redirect URLs section contains an 'Add' button and a table with one row: https://test.v2tl.com/plugins/servlet/oidc/callback. There are also Action buttons for sorting and deleting.

Not surprisingly, you can get two values on the application settings page: `Client ID` and `Client secret` like the picture above, we will use them in the next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure Jira

1. We need continue to config our Configure in jira

## 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. You can configure more complex authorization later, for now check if OpenID actually works.

⚠ You have temporary access to administrative functions. [Drop access](#) if you no longer require it. For more information, refer to the [documentation](#).



Dashboards ▼ Projects ▼ Issues ▼ Boards ▼ Plans ▼ Create

Search



## Administration

Search Jira admin

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

Add configuration

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"/>	<span style="font-size: small;">...</span>
casdoor	OpenID Connect	26 April 2023 7:20 PM	<input checked="" type="checkbox"/>	<span style="font-size: small;">...</span>

#### 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](#).

# Via miniOrange Plugin

This is a tutorial on using [miniOrange](#) to connect casdoor and jira

[Casdoor](#) can use OIDC protocol as IDP to connect various applications. Here is a [Jira](#) tutorial.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Jira_HOSTNAME`: Domain name or IP where Jira is deployed.

## Step1. Deploy Casdoor and Jira

Firstly, the [Casdoor](#) and [Jira](#) should be deployed.

After a successful deployment, you need to ensure:

1. Set Jira URL(Plans → Administration → System → General configuration) to

`Jira_HOSTNAME`.

The screenshot shows the Jira General configuration settings page. On the left sidebar, under 'General configuration', there is a 'Base URL' field containing 'http://localhost:8080'. A red arrow points from the text 'Jira\_HOSTNAME' in the previous step description to this 'Base URL' field. The main panel displays general settings like Title (JIRA), Mode (Private), Maximum Authentication Attempts Allowed (3), CAPTCHA on signup (OFF), and Email from (\$fullname) (Jira). The 'System' tab is selected at the top.

2. Casdoor can be logged in and used normally.

3. You can set CASDOOR\_HOSTNAME = `http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application and Jira

1. Create or use an existing Casdoor application.
2. You should install a [miniOrange](#) app to support OAuth. You can find this app in [Plans->Administration->Find new apps->search](#)

The screenshot shows the Atlassian Marketplace for JIRA interface. At the top, there's a navigation bar with tabs: Administration (highlighted with a red arrow), Applications, Projects, Issues, Manage apps (highlighted with a red arrow), User management, Latest upgrade report, and System. Below the navigation is a search bar: "Search Jira admin". Under the "Manage apps" tab, there's a sidebar titled "ATLASSIAN MARKETPLACE" with a "Find new apps" button (highlighted with a red arrow) and a "Manage apps" link. The main content area is titled "Atlassian Marketplace for JIRA" and displays a search result for "Oauth". A card for the "m0 Jira OAuth SSO, Jira OpenID Connect SSO, Jira OIDC SSO" app by miniOrange is shown. The card includes a thumbnail, the app name, developer information ("miniOrange • Supported by vendor • Data Center"), ratings ("★★★★ (56)", "607 installations"), categories ("ADMIN TOOLS", "INTEGRATIONS", "JIRA SERVICE DESK", "JIRA SOFTWARE", "SECURITY", "UTILITIES"), and a "Paid via Atlassian" note. A "Free trial" button and a "Buy now" button are also present. Below the card, a descriptive text states: "Login to Jira & Service Desk using OAuth2.0/OpenID Connect (OIDC) compliant applications like Google apps, AWS Cognito, Azure AD, Keycloak, GitHub, GitLab, Discord, Facebook, Microsoft, Meetup and custom apps. Best OAuth SSO App In Market!".

3. Set `Selected Application` to Custom OpenId
4. Find a redirect url:

The screenshot shows the "miniOrange OAuth Configuration" page. At the top, there's a header with the miniOrange logo, "miniOrange OAuth Configuration", and links for "@Manage apps", "Ask Us On Forum", and "Frequently Asked Questions". Below the header, there's a "Back to common setting" button. The main content area is titled "OAuth/OIDC Configurations". A red arrow points to the "Callback URL" field, which contains the value `http://localhost:8080/plugins/servlet/oauth/callback`.

## 5. Add a redirect url:

Client ID: 514e09591ee5554b16fe  
Client secret: e7f05b14a68fb23e526f08515aefb73bbab7814a  
Cert: cert-built-in  
Redirect URLs: http://localhost:8080/plugins/servlet/oauth/callback

## 6. You should config this app

Selected Application: Custom OpenId Import Details

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

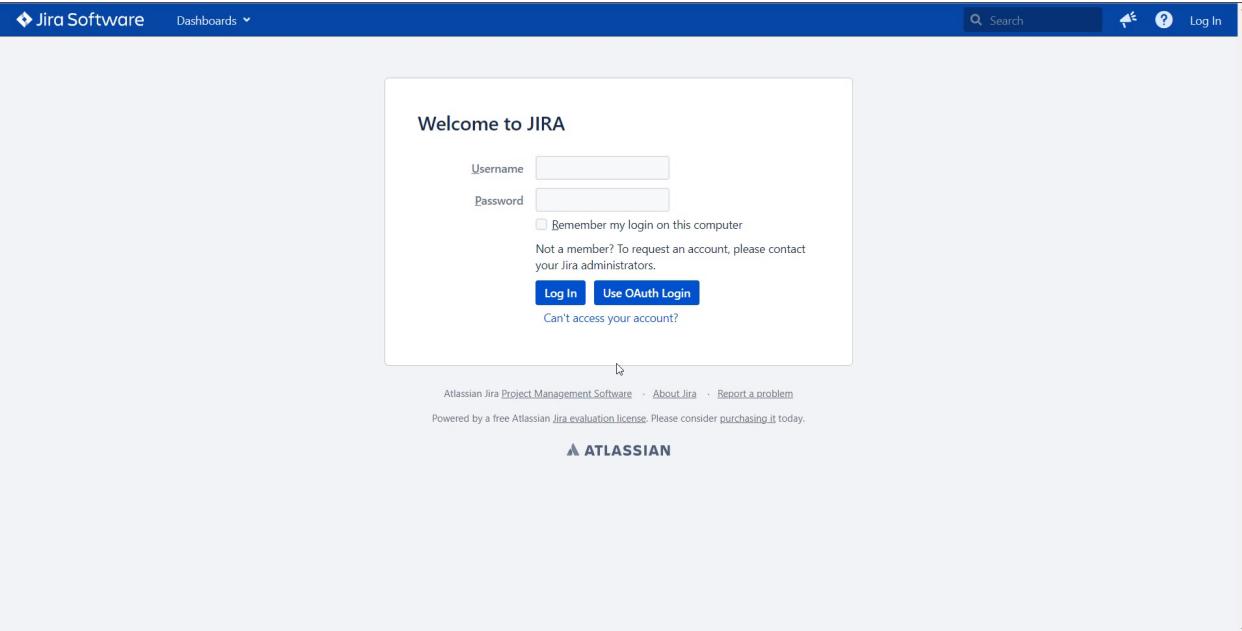
Enter the Logout endpoint of your OAuth/OpenID Provider. Leave blank if Logout endpoint not supported by provider.  
e.g. If Keycloak Logout endpoint is configured with {hostname}/auth/realm/{realm-name}/protocol/openid-connect/logout too.

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

Open your favorite browser and visit: http://**CASDOOR\_HOSTNAME**.well-known/openid-configuration, you will see the OIDC configure of Casdoor.

Log out of Jira, and test SSO.



# Confluence

Casdoor can use OIDC protocol as IDP to connect various applications. Here we will use Confluence as an example to show you how to use OIDC to connect to your applications.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Confluence_HOSTNAME`: Domain name or IP where Confluence is deployed.

## Step1. Deploy Casdoor and Confluence

Firstly, the Casdoor and Confluence should be deployed.

After a successful deployment, you need to ensure:

1. Set Confluence URL to `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 box and has a black arrow pointing to it from the left. On the right, 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 black arrow points to this field from the top right.

2. Casdoor can be logged in and used normally.
3. You can set CASDOOR\_HOSTNAME = `http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find a redirect url:

The screenshot shows the 'OAuth/OIDC Configurations' page. On the left, a sidebar has a 'OAuth/OIDC Configurations' option highlighted with a blue box. On the right, the main content area is titled 'OAuth/OIDC Configurations'. It shows a 'Callback URL' field containing 'http://localhost:8090/plugins/servlet/oauth/callback'. A black arrow points to this field from the top right.

3. Add a redirect url:

The screenshot shows the 'OAuth/OIDC Configurations' page. On the left, a sidebar has a 'OAuth/OIDC Configurations' option highlighted with a blue box. On the right, the main content area shows several configuration fields: 'Client ID' (value: 014ae4bd048734ca2dea), 'Client secret' (value: f26a4115725867b7bb7b668c81e1f8f7fae1544d), 'Cert' (value: cert-built-in), and 'Redirect URLs'. Under 'Redirect URLs', there is a 'Redirect URLs' field with an 'Add' button and a 'Redirect URL' field containing 'http://localhost:8090/plugins/servlet/oauth/callback'. Black arrows point to each of these four fields from the top right.

4. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: `Client ID` and `Client secret` like the picture above, we will use them in the next step.

Open your favorite browser and visit: [http://CASDOOR\\_HOSTNAME/.well-known/openid-configuration](http://CASDOOR_HOSTNAME/.well-known/openid-configuration), you will see the OIDC configure of Casdoor.

## Step3. Configure Confluence

1. You should install a [miniOrange](#) app to support OAuth. You can find this app in

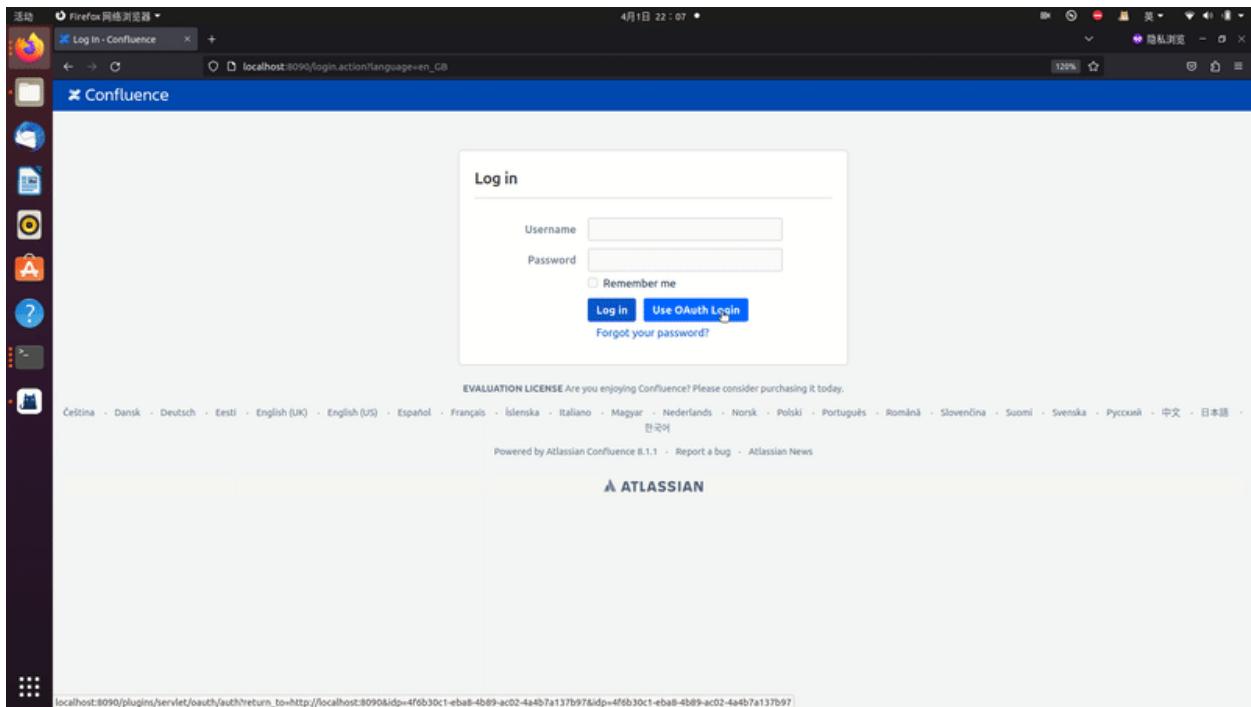
The screenshot shows the Atlassian Marketplace interface. On the left, there's a sidebar with various configuration options like Backup Administration, Clean up, and Recommended Updates. Below that is the 'ATLASSIAN MARKETPLACE' section with 'Find new apps' highlighted. The main area is titled 'Find new apps' and shows search results for 'oauth'. A search bar at the top has 'oauth' typed into it. Below the search bar are filters for '搜索结果', 'All categories', and 'All paid & free'. The first result is 'mO Confluence OAuth SSO, Confluence OpenID Connect/OIDC SSO' by miniOrange. This listing includes a star rating of 4.0 (40 reviews), 409 installations, and a '立即购买' (Buy Now) button. An arrow points from the 'Find new apps' button in the sidebar to this listing. The second result is 'Table Filter and Charts for Confluence' by Stiltsoft Europe OÜ, with a star rating of 3.47 (347 reviews), 15,179 installations, and a '立即购买' (Buy Now) button.

2. You should config this app

Selected Application:	<b>Custom OpenId</b>	<b>Import Details</b>	<b>Setup Guide</b>
Provider ID:	<b>4f6b30c1-eba8-4b89-ac02-4a4b7a137b97</b>		
Custom App Name:	* Casdoor SSO		
Client Id:	* 014ae4bd048734ca2dea		
Client Secret:	* f26a4115725867b7bb7b668c81e1f8f7fae1544d		
Scope:	* openid profile email		
Authorize Endpoint:	* <a href="https://door.casdoor.com/login/oauth/authorize">https://door.casdoor.com/login/oauth/authorize</a>		
Access Token Endpoint:	* <a href="https://door.casdoor.com/api/login/oauth/access_token">https://door.casdoor.com/api/login/oauth/access_token</a>		
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. Set **Selected Application** to Custom OpenId
  4. You can find Client Id and Client Secret in Casdoor application page.
- **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`
1. You can configure more complex authorization later, for now check if OpenID actually works.

Log out of Confluence, and test SSO.



# RuoYi

Casdoor can simply connect to RuoYi-cloud.

## Step 1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor-based login page in your own app with the following steps.

## Step 2. Configure Casdoor

Configure casdoor can refer to [casdoor](#)(Configure casdoor's browser better not use one browser as your develop browser).

You also should configure an organization, an application and the Synchronizer. You also can refer to [casdoor](#).

Some points needing attention:

## 1. The table columns in edit syncer:

Table columns <small>(<a href="#">?</a>)</small>		Column type	Casdoor column	Is hashed	Action
user_id	integer	Id	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
dept_id	integer	Affiliation	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
user_name	string	Name	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
nick_name	string	DisplayName	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
user_type	string	Type	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
email	string	Email	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
phonenumerber	string	Phone	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
sex	string	Gender	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
avatar	string	Avatar	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
password	string	Password	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
del_flag	string	IsDeleted	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
login_ip	string	Createdip	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
create_time	string	CreatedTime	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>
password	string	Password	<a href="#">▼</a>	<input checked="" type="checkbox"/>	<a href="#"></a> <a href="#"></a> <a href="#"></a>

## 2. The password type in edit organization:

Password type ([?](#)):

## 3. You also should open soft deletion.

# Step 3. Reform your front-end

## 3.1 jump to casdoor's login page

We can use front-end sdk, take vue-sdk as an example here. After you init vue-sdk, you can get casdoor login page url by `getSignInUrl()`.

You can link it with the way you like and you can delete some ruoyi-cloud original code which you have no further use, such as original account and password el-input.

## 3.2 Accept the code and state which return by casdoor

After we login in successfully by casdoor, casdoor sends the code and state to the page that we set up. We can get the code and state with function `create`.

```
created() {
  let url = window.document.location.href //get url
```

For RuoYi-Cloud, we just change its original method which sends account and password to send code and state. Therefore, it just changes what is sent to the back end, relative to the original login.

## Step 4. Reform your back-end

### 4.1 Accept the code and state which return by front-end

```
@PostMapping("login")
public R<?> callback(@RequestBody CodeBody code) {//we should define
a CodeBody entity which have code and state
    String token = casdoorAuthService.getOAuthToken(code.getCode(),
code.getState());
    CasdoorUser casdoorUser =
casdoorAuthService.parseJwtToken(token);
    if(casdoorUser.getName()!=null){
        String casdoorUserName = casdoorUser.getName();

        if(sysLoginService.getUserByCasdoorName(casdoorUserName)==null){//if
database haven't this user
            // add this user into database
            sysLoginService.casdoorRegister(casdoorUserName);
        }
    }
    LoginUser userInfo =
sysLoginService.casdoorLogin(casdoorUser.getName());//get this
user's information by database
    return R.ok(tokenService.createToken(userInfo));
}
```

In this method, we use casdoor-SpringBoot-sdk method and slightly modified RuoYi-Cloud Method.

For example, RuoYi-Cloud original register with account and password, I change the register with account like casdoorRegister.

I also add a method to execute whether this account exists like `getUserByCasdoorName` and change `execute userinfo` with account and password to with account.

It's easy, because we only need to delete the part of checking password.

## Step 5. Summary

### 5.1 front-end

- We need to delete original login and register.
- We also need to accept code and state and send them to back-end.

### 5.2 back-end

RuoYi back-end has perfect login and registration function. We just need to change a little, so it is very convenient.

## Step 6. Detailed steps

1. Deploy and configure casdoor. We must take care of the organization's password type which should choose bcrypt because RuoYi-Cloud's password type is bcrypt.
2. We should use casdoor syncers to copy database users to your casdoor organization. This step can make the original account import to casdoor.
3. After we deployed casdoor, we should change front-end. We should close RuoYi check code

```
// checkcode switch  
captchaEnabled: false,  
// register switch  
register: true,
```

Note that RuoYi-Cloud captcha needs to be close in nacos again. Note that RuoYi-Cloud open registration function requires changing sys.account.registerUser to true.

4. We should add button jump to casdoor and change data's loginForm

```
1 <el-button type="primary">  
2   <a href="http://localhost:7001/login/oauth/authorize?client_id=d509b6b3edc8a3d4cce9&response_type=code&redirect_uri=http%3A%2F%2Flocalhost%3D8080%2Fcasdoor">casdoor</a>  
3 </el-button>
```

```
loginForm: {  
  code: "",  
  state: ""  
},
```

Here I write url, you can get url by casdoor-vue-sdk or casdoor-SpringBoot-sdk.

5. Because we don't use the original login, we should delete the method about cookie and checkcode method.

So the new create function:

```
created() {  
  let url = window.document.location.href //get url  
  let u = new URL(url);  
  this.loginForm.code = u.searchParams.get('code') //get code and  
state  
  this.loginForm.state = u.searchParams.get('state')  
  if(this.loginForm.code!=null&&this.loginForm.state!=null){ //if  
code and state is null, execute handleLogin  
    this.handleLogin()  
  }  
}
```

6. In fact, we just need to change the parameter we send to back-end and delete the function we don't need, we don't need to change anything else.

```
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. Import dependency in back-end.

pom.xml

```
<dependency>
    <groupId>org.casbin</groupId>
    <artifactId>casdoor-spring-boot-starter</artifactId>
    <version>1.2.0</version>
</dependency>
```

You also need to configure casdoor in resource. 8. Callback function is defined as the redirect function. I change some methods in sysLoginService slightly. I delete the check password step because we don't need it.

```
@PostMapping("login")
public R<?> callback(@RequestBody CodeBody code) {//we should define a CodeBody entity which have code and state
    String token = casdoorAuthService.getOAuthToken(code.getCode(),
    code.getState());
    CasdoorUser casdoorUser =
    casdoorAuthService.parseJwtToken(token);
    if(casdoorUser.getName()!=null){
        String casdoorUserName = casdoorUser.getName();

        if(sysLoginService.getUserByCasdoorName(casdoorUserName)==null){//if database haven't this user
            // add this user into database
            sysLoginService.casdoorRegister(casdoorUserName);
        }
    }
    LoginUser userInfo =
    sysLoginService.casdoorLogin(casdoorUser.getName());//get this user's information by database
    return R.ok(tokenService.createToken(userInfo));
}
```

## 9. SysLoginService's new method

```
public LoginUser casdoorLogin(String username){
    // execute user
    R<LoginUser> userResult =
remoteUserService.getUserInfo(username, SecurityConstants.INNER);
    if (R.FAIL == userResult.getCode())
    {
        throw new ServiceException(userResult.getMsg());
    }

    if (StringUtils.isNull(userResult) ||
StringUtils.isNull(userResult.getData()))
    {
        recordLogService.recordLogininfor(username,
Constants.LOGIN_FAIL, "this user is not exist");
        throw new ServiceException("user" + username + " is not
exist");
    }
    LoginUser userInfo = userResult.getData();
    SysUser user = userResult.getData().getSysUser();
    if (UserStatus.DELETED.getCode().equals(user.getDelFlag()))
    {
        recordLogService.recordLogininfor(username,
Constants.LOGIN_FAIL, "sorry, your account was deleted");
        throw new ServiceException("sorry, your account" + username +
" was deleted");
    }
    if (UserStatus.DISABLE.getCode().equals(user.getStatus()))
    {
        recordLogService.recordLogininfor(username,
Constants.LOGIN_FAIL, "your account is disabled, you can contact
admin ");
        throw new ServiceException("sorry, your account" + username +
" is disabled");
    }
    recordLogService.recordLogininfor(username,
Constants.LOGIN_SUCCESS, "login successfully");
    return userInfo;
}
```

```
public String getUserByCasdoorName(String casdoorUsername){
    R<LoginUser> userResult =
remoteUserService.getUserInfo(casdoorUsername,
SecurityConstants.INNER);
    if (StringUtils.isNull(userResult) ||
StringUtils.isNull(userResult.getData()))
    {
        //if this user is not in Ruoyi-Cloud database and casdoor
have this user, we should create this user in database
        return null;
    }
    String username =
userResult.getData().getSysUser().getUserName();
    return username;
}
```

```
public void casdoorRegister(String username){
    if (StringUtils.isAnyBlank(username))
    {
        throw new ServiceException("User must fill in");
    }
    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.recordLoginInfo(username, Constants.REGISTER,
"register successfully");
}
```

# Pulsar-manager

Casdoor can simply connect to Pulsar-manager.

Because the code for connecting casdoor has been added in Pulsar-manager, we just need to configure application.yml in back-end and open front switch.

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a Casdoor-based login page in your own app with the following steps.

## Step2. Configure Casdoor

Configure casdoor can refer to [casdoor](#)(Configure casdoor's browser better not use one browser as your develop browser).

You also should configure an organization and an application. You also can refer to [casdoor](#).

## step2.1 you should create an organization

Edit Organization Save Save & Exit

Name ⓘ:	pulsar
Display name ⓘ:	pulsar
Favicon ⓘ:	URL ⓘ: <a href="https://cdn.casbin.org/img/favicon.png">https://cdn.casbin.org/img/favicon.png</a>
Preview:	
Website URL ⓘ:	<a href="http://localhost:9527/#/login?redirect=%2F">http://localhost:9527/#/login?redirect=%2F</a>
Password type ⓘ:	plain
Password salt ⓘ:	
Phone prefix ⓘ:	+ 86

## step2.2 you should create an application

Name ⓘ: app-pulsar  
Display name ⓘ: app-pulsar  
Logo ⓘ: URL ⓘ: [https://cdn.casbin.org/img/casdoor-logo\\_1185x256.png](https://cdn.casbin.org/img/casdoor-logo_1185x256.png)

Preview: 

Home ⓘ:	<a href="#">/</a>				
Description ⓘ:					
Organization ⓘ:	pulsar				
Client ID ⓘ:	6ba06c1e1a30929fdda7				
Client secret ⓘ:	df92bbf913225ebbae9af7ba8d41fe19507eb079				
Cert ⓘ:	cert-built-in				
Redirect URLs ⓘ:	<table border="1"><thead><tr><th>Redirect URLs</th><th>Add</th></tr></thead><tbody><tr><td>Redirect URL:</td><td><a href="http://localhost:9527/callback">http://localhost:9527/callback</a></td></tr></tbody></table>	Redirect URLs	Add	Redirect URL:	<a href="http://localhost:9527/callback">http://localhost:9527/callback</a>
Redirect URLs	Add				
Redirect URL:	<a href="http://localhost:9527/callback">http://localhost:9527/callback</a>				

## Step3. Open Pulsar-manager front-end

# switch

Open this switch to make code and state send to back-end.

This switch in the Line 80 of pulsar-manager/front-end/src/router/index.js

```
- // mode: 'history', // require service support
+ mode: 'history', // require service support
```

## Step4. Configure back-end code

You should configure casdoor's Configuration in the Line 154 of pulsar-manager/src/main/resources/application.properties

```
casdoor.endpoint = http://localhost:8000
casdoor.clientId = <client id in previous step>
casdoor.clientSecret = <client Secret in previous step>
casdoor.certificate=<client certificate in previous step>
casdoor.organizationName=pulsar
casdoor.applicationName=app-pulsar
```

# ShenYu

ShenYu has casdoor plugin to use casdoor

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application
2. Add Your redirect url

Name : app-test application name

Display name : app-test

Logo : 

Preview:

Home :

Description :

Organization :

Client ID :

Client secret :

Cert :

Redirect URLs :

Action	Redirect URL
<span style="color: red;">redirect url</span>	d <sup>o</sup> http://localhost:9195/http/hello
<span style="color: red;">redirect url</span>	d <sup>o</sup> http://localhost:9195/http/hello

### 3. On the certificate editing page, you can see your **Certificate**

Certificate :

Copy certificate
Download certificate

```
-----BEGIN CERTIFICATE-----
MIIE+TCCAUgGAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTABBgNVBAoTFENh
c2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENlcnQwHhcNMjEx
MDE1MDgxMTUyWhcNNDEXMDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIe9y
Z2FuaxphdGlvbjEVMBMGAEUEAxMMQ2FzZG9vcj8DZXj0MIIcjANBqkqhkiG9w0B
AQEFAAOCAg8AMiCCgKCAgEAstnpb5E1/ymf0tRfSDSSE8I7y+lw+RjIj74e5ej
rq4b8zMYk7HeHCyZr/hmNewEVXnhXu1P0mBeQ5ypp/QGo8vgEmjaETNmzkl1NjOQ
CjCYwUrasO/f/Mnl1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07
uvFMCje5W8+0rKErZCKTR8+9VB3janeBz/zQePFvh79bfZate/hLirPK0Go9P1g
OvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRS8b/wUjNCUBD
PTSLVjC04WIIIf6Nkfx0Z7KvmbPstSj+btvqsvRAGtvsB9h62Kptjs1Yn7GAuo
I3qt/4zoKbiURYxkQJXlvwCQsEftUuk5ew5zuPSIDRLoLByQTLbx0jLAFNfW3g/
pzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfakNkwep2REV+RMc0fx4Gu
hRsnlsmkmUDeylZ9aBL9oj11YEQfM2JZEq+RvtUx+wB4y8K/tD1bcY+lfnG5rBpw
IDpS262boq4SRsvb3Z7bB0w4ZxvOfj/1VLoRjtPbLifobhfr/AeZMHpiKOXvfz4
yE+hqzi6wdF0VR9xYc/RbSAf7323OsjYnjjEglnUtRohnRgCpjlk/Mt2Kt84Kb0
wn8CAaAMQMA4wDAYDVR0TAQH/BAlwADANBqkqhkiG9w0BAQsFAAOCAgEAn2lf
DKkLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgic4/Lsdzuf4Awe6ve
C06lVdWSlis8UPUPdjmt2uMPSNjwLxG3QsrimMURNlwFLTfRem/heJe0Zgur9J1M
8haawdSdjH2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCvl
2nR42Fybap3O/g2JXMhNNRowZmNjgpsF7XVENCSuFO1jTywLaqjuXCg54lL7XVLG
omKNNNcc8h1FCelj/nbbGMhodnFWKDTsJcbNmcOPNHo6ixzqMy/Hqc+mWv7maAG
Jtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisukftOPZgtH979XC4mdf0WPnOBLql
2DJ1zaBmjIGolvb7XNVKcUfdXYw85ZTQ5b9cli4e+6bmyWqQltlwt+Ati/uFEV
Xzcj70B4IALX6xau1kLepV9O1GERizYrz5P9NJNA7Ko05AVMp9w0DQTkt+LbXnZE
HHnWky8HQKF9sR7YBPGLs/Ac6tviv5ua15Ogj/8dLRZ/veyFfGo2yZsl+hKVU5
nCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VYalWSalADosHAgMWFxFuWP+h
8XKXmzlxuHbTMQytZPDgsps5aK+S4Q9wb8RRAYo=
-----END CERTIFICATE-----
```

## Step3. Use casdoor plugin in shenyu

1. Config casdoor plugin in shenyu

## 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

note: because the shenyu only have Single line input box so we need add \n in

every line of cert.

Certificate ? :

[Copy certificate](#)

[Download certificate](#)

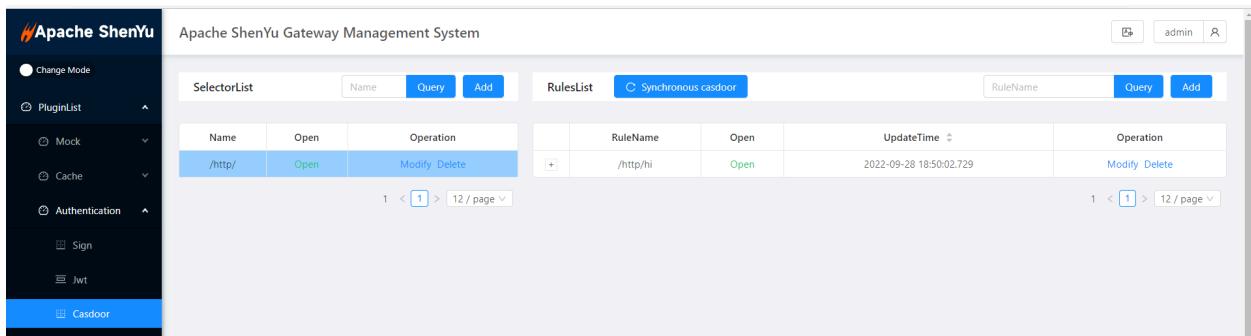
-----BEGIN CERTIFICATE-----\nMIIE+TCCAUgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENH\nn\nc2Rvb3lgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENlcnQwHhcNMjEx\nn\nMDE1MDgxMTUyWhcNNDExMDE1MDgxMTUyWja2MR0wGwYDVQQKErDYXNkb29yIEd9\nn\nZ2FuaXphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vcBDZXJ0MIIICjANBgkqhkiG9w0B\nn\nAQEFAAOCAg8AMIICgKCAgEAstnpb5E1/yM0f1RfSDSSE8IR7y+lw+RJi74e5ej\nn\nrq4b8zMjYk7HeHCyZr/hmNEwEVXnhXu1P0mBeQ5yp/QGo8vgEmjAETNmzkl1NjOQ\nn\nCjCYwUrasO/f/Mnl1C0j13vx6mV1kHZjsRsKmhYY1vaxTEP3+VB8Hjg3MHFWrb07\nn\nuvFMCJe5W8+0rKErZCKTR8+9VB3janeBz//zQePFVh79bfZate/hLirPK0Go9P1g\nn\nOvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRSBb/wUjNCUBD\nn\nPTSLVjc04WIISf6Nkf0Z7KvmbPstSj+btcqvRAgtvdsB9h62Kptjs1Yn7GAuo\nn\nl3qt/4zoKbiURYxkQJXlvwCQsEftUuk5ew5zuPSIDRLoLbyQLtbx0JqlAFNfW3g\nn\npzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4Gu\nn\nhRsnLsmkmUDeylZ9aBL9oj11YEQfm2JZEq+RvtUx+wB4y8K/tD1bcY+lfnG5rBpw\nn\nIDpS262boq4SRsvb3Z7bB0w4ZxvOfJ/1VLoRftjPbLif0bhfr/AeZMHpIKOXvfz4\nn\nyE+hqzi68wdF0VR9xYc/RbSAf7323OsjYnjjEgInUtRohnRgCpjlk/Mt2Kt84Kb0\nn\nwn8CAwEAAsMQMA4wDAYDVR0TAQH/BAlwADANBgkqhkiG9w0BAQsFAAOCAgEAn2If\nn\nDKkLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/LSdzuf4Awe6ve\nn\nC06IVdWSlis8UPUPdmT2uMPNSJwLxG3QsrimMURNwFILTfRem/heJe0ZgurJ1M\nn\n8haawdSdjH2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCv\nn\n2nR42Fybap3O/g2JXMHNNROwZmNjgpsF7XVENCSuFO1jTywLaajuXCg54IL7XVLG\nn\nomKNNNcc8h1FcEkj/nnbGMhodnFWKDTsJcbNmOPNHo6ixzqMy/Hqc+mWYv7maAG\nn\nJtevs3qgMZ8F9Qzr3HpUc6R3ZYYWDY/xxPisufktpZGtH979XC4mdf0WPnOBQl\nn\n2DJ1zaBmjGjolvb7XNVKcUfDXYw85ZTZQ5b9cl4e+6bmyWqQltlw+Ati/uFEV\nn\nXzCj70B4IALX6xau1kLepV9O1GERizYRz5P9NJNA7Ko05AVMp9w0DQTkt+LbXnZE\nn\nHHnWKy8xHQKZF9sR7YBPGls/Ac6tviv5ua15Ogj/8dLRZ/veyFfGo2yZsl+hKVU5\nn\nnCCJHBcAyFnmlhdvdwEdH33jDBjNB6ciotJzf/3VYalWSalADosHAgMWfXuWP+h\nn\n8XXKXmzlxuHbTMQYtZPDgspS5aK+S4Q9wb8RRAYo=\n

here not need add \n

You can copy it and paste it on the certificate of shenyu casdoor config.

You don't need save it in casdoor certificate editing page,because it just for copying.

## 2. Confin shenyu casdoor's plugin



The screenshot shows the Apache ShenYu Gateway Management System interface. On the left, there is a sidebar with a dark theme containing the following sections:

- Change Mode (radio button)
- PluginList
  - Mock
  - Cache
  - Authentication
    - Sign
    - Jwt
  - Casdoor (selected)

The main area has tabs: SelectorList and RulesList. The RulesList tab is active, showing a table with one row of data:

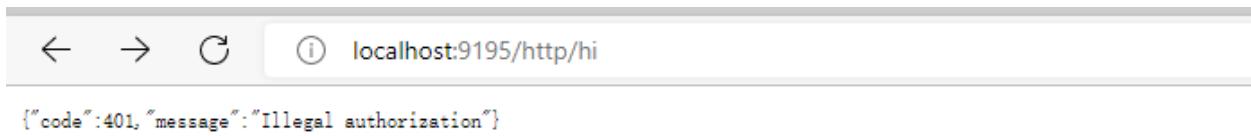
Name	Open	Operation	RuleName	Open	UpdateTime	Operation
/http/	Open	Modify Delete	/http/hi	Open	2022-09-28 10:50:02.729	Modify Delete

Pagination controls at the bottom indicate page 1 of 12.

You can config what you need to use casdoor config

## 3. Get the service and use

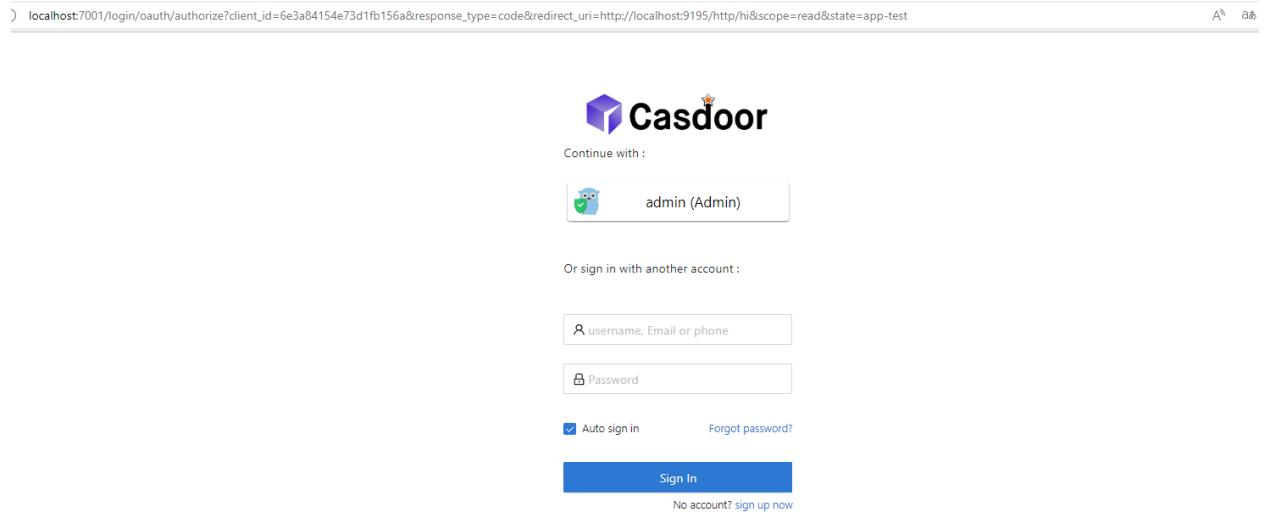
### 3.1 Visit the Web directly like



A screenshot of a web browser window. The address bar shows the URL `localhost:9195/http/hi`. The page content is a JSON object:

```
{"code":401,"message":"Illegal authorization"}
```

### 3.2 Use casdoor login like this



The screenshot shows the Casdoor login interface. At the top, there is a URL bar with the address `localhost:7001/login/oauth/authorize?client_id=6e3a84154e73d1fb156a&response_type=code&redirect_uri=http://localhost:9195/http/hi&scope=read&state=app-test`. Below the URL bar is the Casdoor logo and the text "Continue with:". A button labeled "admin (Admin)" is shown, which has a small owl icon and a green checkmark. Below this, there is a section for "Or sign in with another account:" containing two input fields: one for "username, Email or phone" and one for "Password". There are also links for "Auto sign in" (with a checked checkbox) and "Forgot password?". A large blue "Sign In" button is at the bottom, and a link for "No account? sign up now" is just below it. The browser's navigation bar at the bottom shows the URL `localhost:9195/http/hi?code=822607b015cca2515b2b&state=app-test`.

localhost:7001/login/oauth/authorize?client\_id=6e3a84154e73d1fb156a&response\_type=code&redirect\_uri=http://localhost:9195/http/hi&scope=read&state=app-test

localhost:9195/http/hi?code=822607b015cca2515b2b&state=app-test

hi! null! I'm Shenyu-Gateway System. Welcome!

### 3.3 Carry token in Headers, you also can visit it

The screenshot shows the Postman interface with a GET request to `http://localhost:9195/http/hi`. The **Headers (8)** tab is selected, displaying the following header information:

Key	Description
Postman-Token	<calculated when request is sent>
Host	<calculated when request is sent>
User-Agent	PostmanRuntime/7.29.2
Accept	*
Accept-Encoding	gzip, deflate, br
Connection	keep-alive
Authorization	eyJhbGciOiJSUzI1NjI6ImtpZCI6ImNlcnQtYn... <span style="color:red">Your token</span>

The **Body** tab is selected, showing the response body:

```
1 hi! null! I'm Shenyu-Gateway System. Welcome!
```

### 3.4 It also can save name,id and organization in Headers so that you can use them in next time

# ShardingSphere

[shardingsphere-elasticjob-ui](#) have integrated Casdoor. We can use it after config it.

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a casdoor based login page in your own app with the following steps.

## Step2. Configure Casdoor application and configure application in ShardingSphere

1.Create or use an existing Casdoor application

Name ⓘ: ShardingSphere

Display name ⓘ: ShardingSphere

Logo ⓘ: URL ⓘ: https://cdn.casbin.org/img/casdoor-logo\_1185x256.png

Preview: 

Home ⓘ:

Description ⓘ:

Organization ⓘ: ShardingSphere

Client ID ⓘ: 3ed79fa530645fb3653

Client secret ⓘ: 54633c82b7796a4332c6976864c6c16bc3b05556

Cert ⓘ: cert-built-in

Redirect URLs ⓘ:

Redirect URLs	Add	Action
http://localhost:8080		[Edit] [Delete]

RedirectURLs is depend on what url you need redirect.The selected data will use in next.

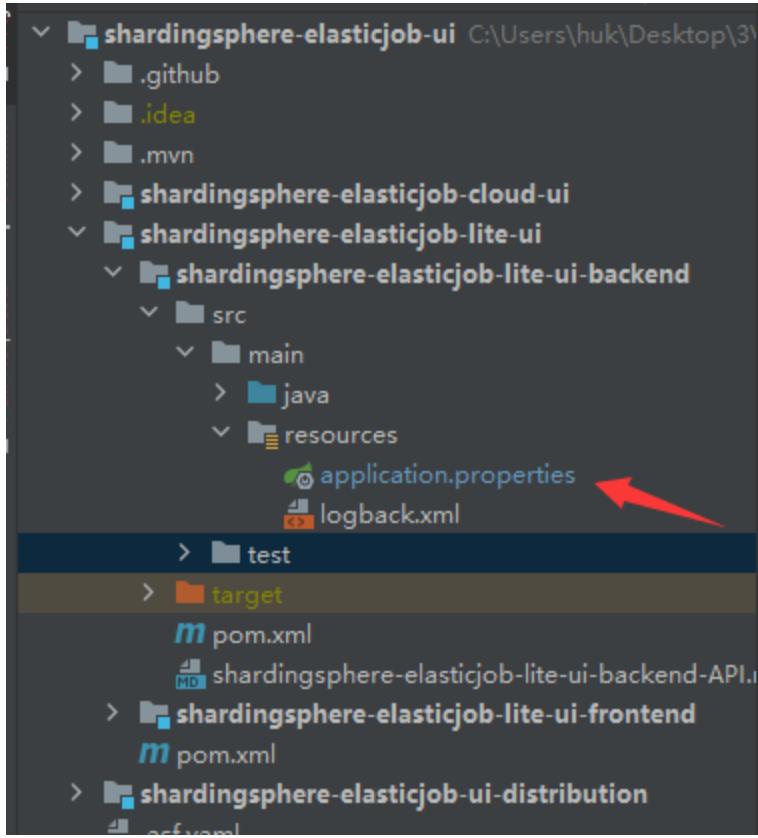
2.On the certificate editing page, you can see your **Certificate**

Certificate [?](#)  [Copy certificate](#) [Download certificate](#) Private

-----BEGIN CERTIFICATE-----  
MIIE+TCCAuGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENh  
c2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENlcnQwHhcNMjEx  
MDE1MDgxMTUyWhcNNExMDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIE9y  
Z2FuaXphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vciBDZXJ0MIICljANBqkqhkiG9w0B  
AQEFAOCAg8AMIICCgKCAgEAsInpb5E1ym0f1RfSDSSE8IR7y+lw+RJi74e5ej  
rq4b8zMk7HeHCyZr/hmNewEVXnhXu1P0mBeQ5ypp/QGo8vgEmjAETNmzkI1NjOQ  
CjCYwUrasO/f/MnI1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07  
uvFMCJe5W8+0rKErZCKTR8+9VB3janeBz//zQePFVh79bFZate/hLirPK0Go9P1g  
OvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRSBb/wJNCUBD  
PTSLVjC04WIISf6Nkfx0Z7KvmbPstSj+btcqvRA GTvdsB9h62Kptjs1Yn7GAuo  
l3qt/4zoKbiURYxkJXlvwCQsEftUuk5ewzuPSIDRLoLByQTLbx0JqLAFNfW3g/  
pzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4Gu  
hRsnLsmkmUDeylZ9aBL9oj11YEQfm2JZEq+RVtUx+wB4y8K/tD1bcY+lfnG5rBpw  
IDPs262boq4SRsvb3Z7b80w4ZxvOfj/1VLorftjPbLIIf0bhfr/AeZMHplKOXvfz4  
yE+hqzi68wdF0VR9xYc/RbSAf7323OsjYnjjEgInUtRohnRgCpjlk/Mt2Kt84Kb0  
wn8CAwEAaMQMA4wDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAgEAn2If  
DKKLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/LSdzuf4Awe6ve  
C06IVdWSlis8UPUPdmT2uMPSNjwLxG3QsrimMURNwFILTfRem/heJe0Zgur9J1M  
8haawdSdJjh2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCvl  
2nR42Fybap3O/g2JXMhNNR0wZmNjgpsF7XVENCSuFO1jTywLaqjuXCg54IL7XVLG  
omKNNNcc8h1FCeKj/nnbGMhodnFWKDTsJcbNmcoPNHo6ixzqMy/Hqc+mWYv7maAG  
Jtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisuKftOPZgtH979XC4mdf0WPnOBLql  
2DJ1zaBmjIGjolvb7XNVKcUDXYw85TZQ5b9cl4e+6bmyWqQltlw+Ati/uFEV  
XzCj70B4IALX6xau1kLEpV9O1GERizYRz5P9NJNA7KoO5AVMp9w0DQTkt+LbXnZE  
HHnWKy8xHQKZF9sR7YBPGls/Ac6tviv5Ua15OgJ/8dLRZ/veyFfGo2yZsl+hKVU5  
nCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VYalWSalADosHAgMWfXuWP+h  
8XXXmzlxuHbTMQYtZPDgspS5aK+S4Q9wb8RRAYo=  
-----END CERTIFICATE-----

### 3. Configure application in ShardingSphere

First we need find the application.properties we need configure



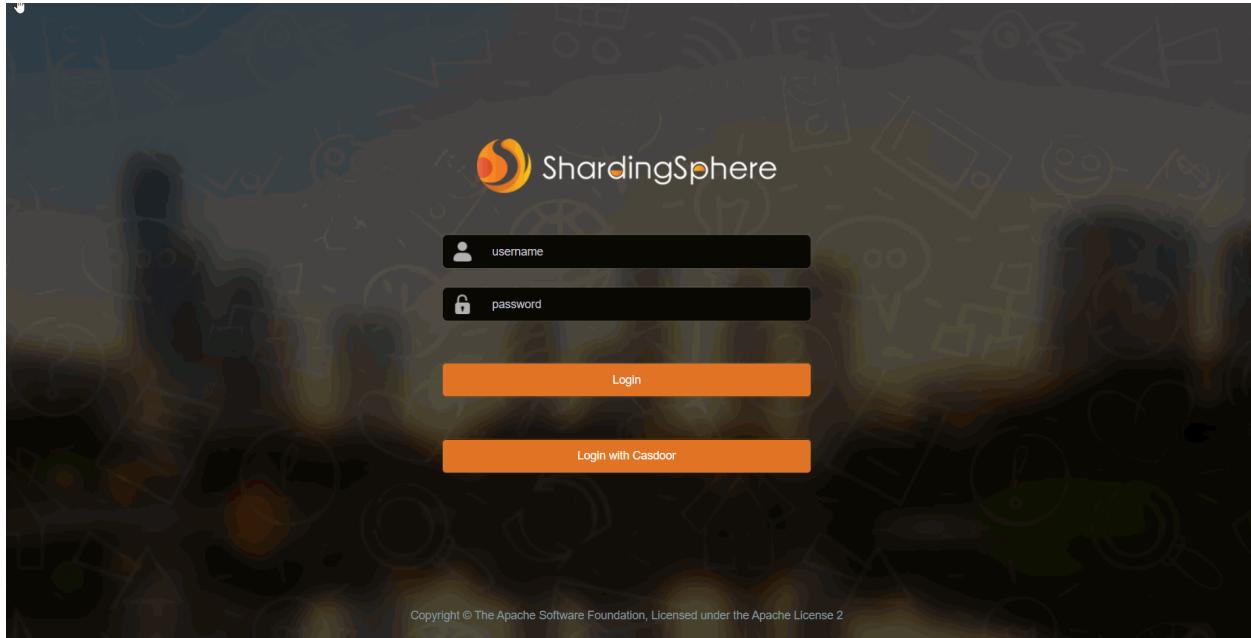
Second we need copy the data in Casdoor application and paste them into application.

```

casdoor.endpoint=http://localhost:7001
casdoor.client-id=3ed79fa530645fb3653
casdoor.client-secret=54633c82b7796a4332c6976864c6c16bc3b05556
casdoor.certificate=\n\
-----BEGIN CERTIFICATE-----\n\
MIIE+TCCAuGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENh\n\
c2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxYDXNkb29yIEEnlcnQwHhcNMjEx\n\
MDE1MDgxMTUyWhcNNDExMDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIE9y\n\
Z2FuaXphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vcibDZXJ0MIICijANBqkghkiG9w0B\n\
AQEFAAOCAg8AMIICCgKCACgEAAsInpb5E1/ym0f1RfSDSSE8IR7y+lw+RjI74e5ej\n\
rq4b8zMYk7HeHCyZr/hmNewEVXnhXu1P0mBeQ5yp/QGo8vgEmjAETNmzkI1Nj0Q\n\
CjCYwUras0/f/MnI1C0j13vx6mV1kJHzSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07\n\
uvFMCJe5W8+0rKErZCKTR8+9VB3janeBz//zQePFvh79bFZate/hLirPK0Go9P1g\n\
0vwIoC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDfE7mtTstRSBb/wUjNCUBD\n\
PTSLVjC04Wllsf6Nkfx0Z7KvmbPstsj+btvcsrvAGtvdsB9h62Kptjs1Yn7GAuo\n\
I3qt/4zoKbiURYxkQJXIvwCQsEftUuk5ew5zuPSlDRLoLByQTLbx0JqLAFNfW3g/\n\
pzSDjqd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4Gu\n\
hRsnLsmkmUDeyIZ9aBL9oj11YEQfM2JZEeq+RvtUx+wB4y8K/tD1bcY+IfnG5rBpw\n\
IDpS262boq4SRSvb3Z7b0w4Zxv0fJ/1VLoRftjPbLIf0bhfr/AeZMHpIK0Xvfz4\n\
yE+hqzi68wdF0VR9xYc/RbSAf73230sjYnjjEgInUtRohnRgCpjIk/Mt2Kt84Kb0\n\
wn8CAwEEAaMQMA4wDAYDVR0TAQH/BAIwADANBqkghkiG9w0BAQsFAAOCAgEAn2lf\n\
DKkLX+F1vKR0/5gJ+PLr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/LSdzuf4Awe6ve\n\
C06LVdWSIis8UPUPdjmT2uMPSNjwLxG3QsrilmMURNwFLLTfRem/heJe0Zgur9J1M\n\
8●awdSdJjH2RgmFoDeE2r8NVRfhbR8KnC01ddTJKuS1N0/irHz21W4jt4rxzCvl\n\
2nR42Fybap30/g2JXMhNNR0wZmNjqpsF7XVENCSuF01jTywLaqjuXCg54IL7XVLG\n\
omKNNNcc8h1FCeKj/nnbGMhodnFWKDTsJcbNmcOPNHo6ixzqMy/Hqc+mWYv7maAG\n\
Jtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisuKft0PZgtH979XC4mdf0WPn0BLql\n\
2DJ1zaBmjigJolvb7XNVKcUfDXYw85TZQ5b9cLI4e+6bmyWqQItlw+Ati/uFEV\n\
XzCj70B4lALXxau1kLEpV901GERizYRz5P9NJNA7Ko05AVMp9w0DQTkt+LbXnZE\n\
HHnWKy8xHQKF9sR7YBPGls/Ac6tviv5Ua150gJ/8dLRZ/veyFfGo2yZsI+hKVU5\n\
nCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VYaIWSalADosHAgMWfXuWP+h\n\
8XKXmzlxuHbTMQYtZPDqspS5aK+S4Q9wb8RRAYo=\n\
-----END CERTIFICATE-----\n
casdoor.organization-name=ShardingSphere
casdoor.application-name=ShardingSphere

```

#### 4. Test it



# Apache IoTDB

Casdoor can simply connect to [Apache IoTDB](#).

Because the code for connecting casdoor has been added in [Apache IoTDB Web Workbench](#), we just need to configure application.yml in back-end and open front switch.

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on <http://localhost:8000>.
- Open your favorite browser and visit <http://localhost:7001>, you will see the login page of Casdoor.
- Input `admin` and `123` to test login functionality is working fine.

Then you can quickly implement a Casdoor-based login page in your own app with the following steps.

## Step2. Configure Casdoor

Configure casdoor can refer to [casdoor](#)(Configure casdoor's browser better not use one browser as your develop browser).

You also should configure an organization and an application. You also can refer to [casdoor](#).

## 2.1 you should create an organization

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 you should create an application

Name ⓘ: app\_IoTDB

Display name ⓘ: app\_IoTDB

Logo ⓘ: URL ⓘ: [https://cdn.casbin.org/img/casdoor-logo\\_1185x256.png](https://cdn.casbin.org/img/casdoor-logo_1185x256.png)

Preview: 

Home ⓘ: [🔗](#)

Description ⓘ:

Organization ⓘ: built-in

Client ID ⓘ: 6f561b83d119be3e1e3c

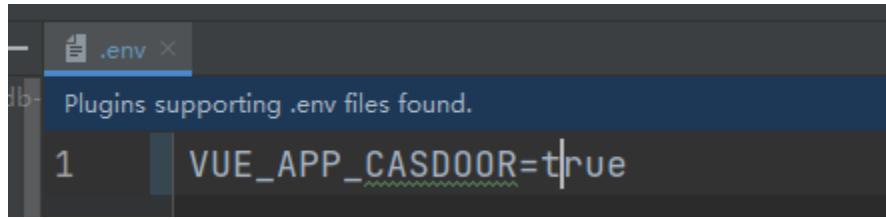
Client secret ⓘ: 242082e823b31a9b0d3a0a4a5a80cd5e415c75f

Cert ⓘ: cert-built-in

## Step3. Open Apache IoTDB Web Workbench front-end switch

Open this switch to make code and state send to back-end.

This switch in the iotdb-web-workbench/fronted/.env



A screenshot of a code editor showing a file named '.env'. The file contains the line 'VUE\_APP\_CASDOOR=true'. A status bar at the top says 'Plugins supporting .env files found.'

## Step4. Configure back-end code

You should configure casdoor's Configuration in the iotdb-web-workbench/backend/src/main/resources/application.properties

```
casdoor.endpoint = http://localhost:8000
casdoor.clientId = <client id in previous step>
casdoor.clientSecret = <client Secret in previous step>
casdoor.certificate=<client certificate in previous step>
casdoor.organizationName=IoTDB
casdoor.applicationName=app-IoTDB
```

# Result

The image is a composite of two screenshots. On the left, there is a photograph of a factory conveyor belt system, showing several large, dark cylindrical components and a bright yellow rectangular object being processed. 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: one for "Account" with the placeholder "Please Input Account" and one for "Password" with placeholder "\*\*\*\*\*". To the right of the password field is a "Forgot Password?" link. At the bottom of the page are two buttons: a teal "Sign In" button and a green "Sign In With Casdoor" button with a small circular icon.

# Apache DolphinScheduler

Casdoor is one of the supported login method for [Apache DolphinScheduler](#).

## Step1. Deploy Casdoor

Firstly, the Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#).

After a successful deployment, you need to ensure:

- The Casdoor server is successfully running on `http://localhost:8000`.
- Open your favorite browser and visit `http://localhost:7001`, you will see the login page of Casdoor.
- Input admin and 123 to test login functionality is working fine.

Then you can quickly implement a Casdoor based login page in your own app with the following steps.

## Step2. Configure Casdoor Application

1. Create or use an existing Casdoor application.
2. Add Your redirect url (You can see more details about how to get redirect url in the next section)

Name [?](#) : application\_a6ftas → your application name

Display name [?](#) : New Application - a6ftas

Logo [?](#) : URL [?](#) : [https://cdn.casbin.org/img/casdoor-logo\\_1185x256.png](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

### 3. Add provider you want and supplement other settings.

Not surprisingly, you can get two values on the application settings page: Client ID and Client secret like the picture above. We will use them in next step.

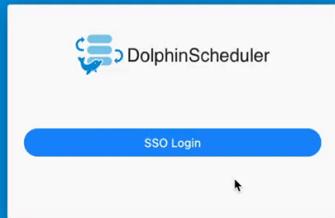
Open your favorite browser and visit: [http://CASDOOR\\_HOSTNAME/.well-known/openid-configuration](http://CASDOOR_HOSTNAME/.well-known/openid-configuration), you will see the OIDC configure of Casdoor.

# Step3. Configure Dolphinscheduler

| dolphinscheduler-api/src/main/resources/application.yaml

```
security:
  authentication:
    # Authentication types (supported types:
    # PASSWORD, LDAP, CASDOOR_SSO)
    type: CASDOOR_SSO
  casdoor:
    # Your Casdoor server url
    endpoint:
    client-id:
    client-secret:
      # The certificate may be multi-line, you can use `|-` for ease
      certificate:
        # Your organization name added in Casdoor
        organization-name:
        # Your application name added in Casdoor
        application-name:
        # Dolphinscheduler login url
        redirect-url: http://localhost:5173/login
```

Now, Dolphinschduler will automatically redirect you to Casdoor for authentication.



# FireZone

Casdoor can use OIDC protocol as IDP to connect various applications. Here we will use [FireZone](#) as an example to show you how to use OIDC to connect to your applications.

## Step 1. Deploy Casdoor and FireZone

Firstly, the Casdoor and FireZone should be deployed.

After a successful deployment, you need to ensure:

1. Set FireZone URL(Sigin → Security → Add OpenID Connect Provider) to FIREZONE\_HOSTNAME.

The screenshot shows the Firezone Site Settings page. On the left is a dark sidebar with navigation links: Configuration (Users, Devices, Rules), Settings (Defaults, Account, Customization, Security), and Diagnostics (WAN Connectivity). The main content area is titled "Site Settings" and contains "Site Defaults". It includes fields for "Allowed IPs" (172.21.0.0/16, 172.16.0.0/16), "DNS Servers" (172.16.250.155), and "Endpoint" (localhost:8080). A red arrow points to the "Endpoint" field. Below these are sections for "Persistent Keepalive" (0) and "MTU" (1280).

2. Casdoor can be logged in and used normally.
3. `CASDOOR_HOSTNAME`: `http://localhost:8000`. If you deploy Casdoor using default `app.conf`.

## Step 2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url:

For example, the Configid in the FireZone Provider is TEST, so the redirect URL should be `http://[FIREZONE_HOST]/auth/oidc/[PROVIDER_CONFIG_ID]/callback/`

Home ? :

Description ? :

Organization ? :

Client ID ? :

Client secret ? :

Cert ? :

Redirect URLs ? :   
Redirect URLs   
Redirect URI

Open your favorite browser and visit: [http://\[CASDOOR\\_HOSTNAME\]/.well-known/openid-configuration](http://[CASDOOR_HOSTNAME]/.well-known/openid-configuration), you will see the OIDC configure of Casdoor.

### 3. Configure 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>

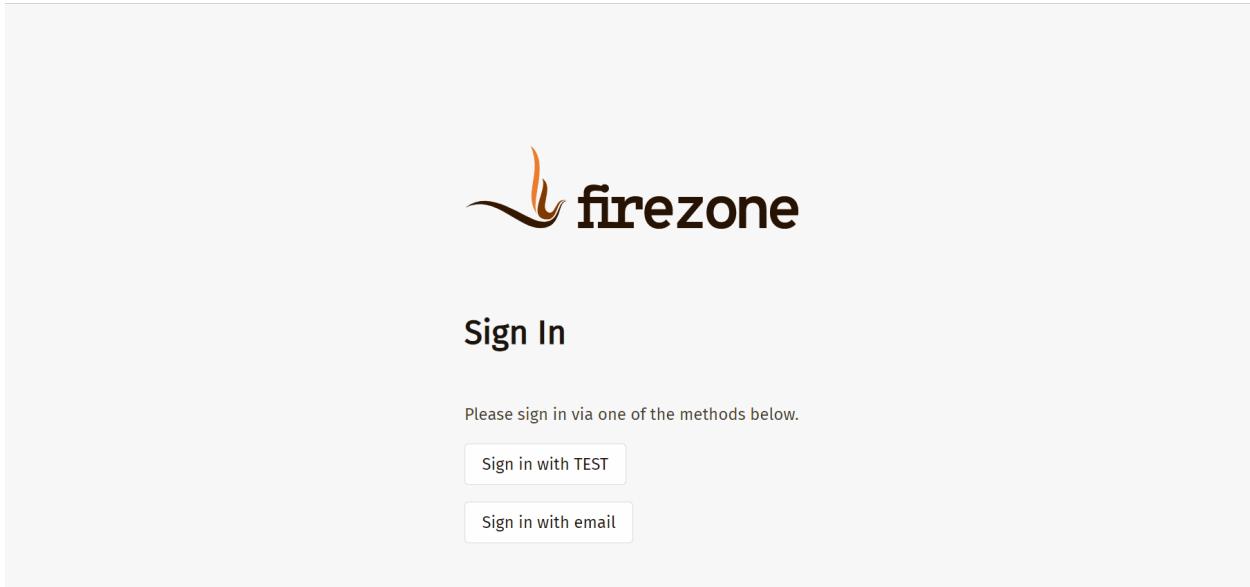
**Auto create users**

**Save**

- **Discovery Document URI**: FireZone Provider Discovery Document URI should be [https://\[CASDOOR\\_HOST\]/.well-known/openid-configuration](https://[CASDOOR_HOST]/.well-known/openid-configuration)
- **Scopes**: openid email profile

- `ConfigID`: ConfigID should be the PROVIDER\_CONFIG\_ID of the redirect URL and should correspond to casdoor redirect URL
- `Auto create users`: Successful login will automatically create a user

## Log out of FireZone, and test SSO.



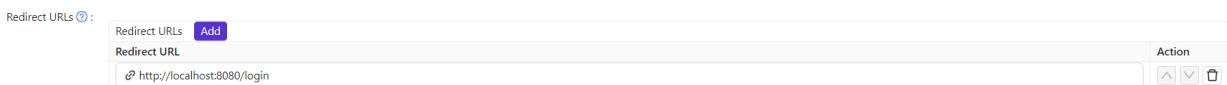
# CloudFoundry

Before the integration, we need to deploy Casdoor locally.

Then we can quickly implement a Casdoor-based login page in our own app with the following steps.

## Step1. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://CASDOOR_HOSTNAME/login`



3. Copy the client ID, we will need it in the following steps.

## Step2. Add user in Casdoor

Now you have the application, but not a user. That means you need to create a user and assign the role.

Go to the "Users" page and click on "Add user" in the top right corner. That opens a new page where you can add the new user.

Save the user after adding a username and adding the organisation CloudFoundry(other details are optional).

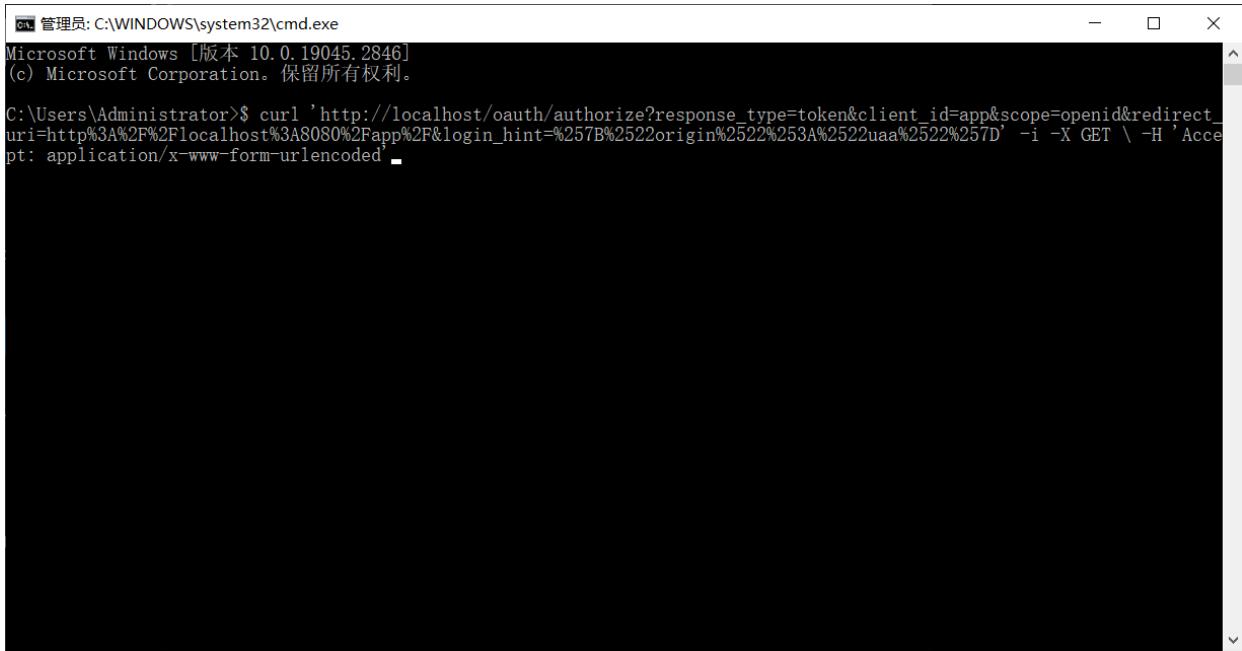
Now you need to set up a password for your user, which you can do by clicking manage your password.

Choose a password for your user and confirm it.

## Step3. Build CloudFoundry App

Start the CloudFoundry by follow.

- `$git clone git://github.com/cloudfoundry/uaa.git`
- `$ 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 being run:

```
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'
```

## Step4. Integrate Casdoor

Now open another command line and input :

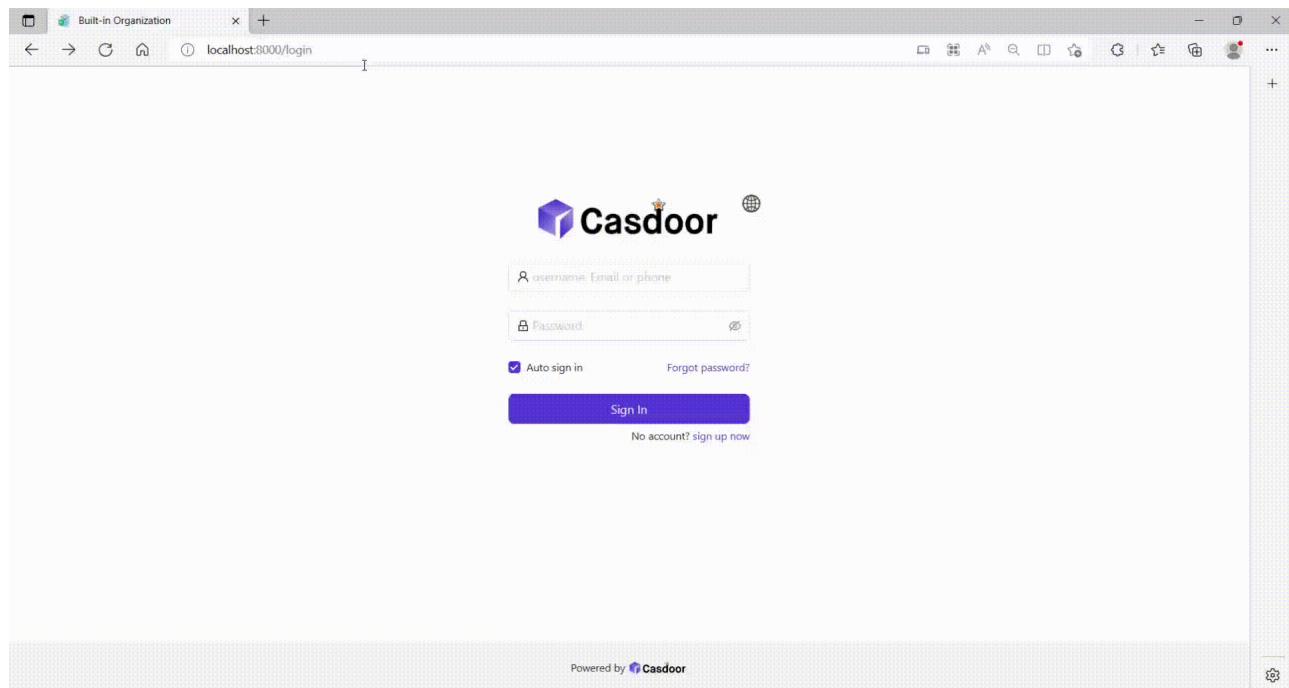
- \$ curl 'http://localhost/oauth/authorize?response\_type=token&client\_id=app&scope=openid&redirect\_uri=http%3A%2F%2Flocalhost%3A8080%2Fapp%2F -i -X GET \ -H 'Accept: application/x-www-form-urlencoded'

we have already got the client\_id and redirect\_uri before, we input these parameters.

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

execute the command, we can get the result below, which means that we have integrated Casdoor with CloudFoundry successfully.

```
HTTP/1.1 302 Found
Content-Security-Policy: script-src 'self'
Strict-Transport-Security: max-age=31536000
Set-Cookie: X-Uaa-Csrf=09mMqMDhcwHGLMufnB4YA1; 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
```



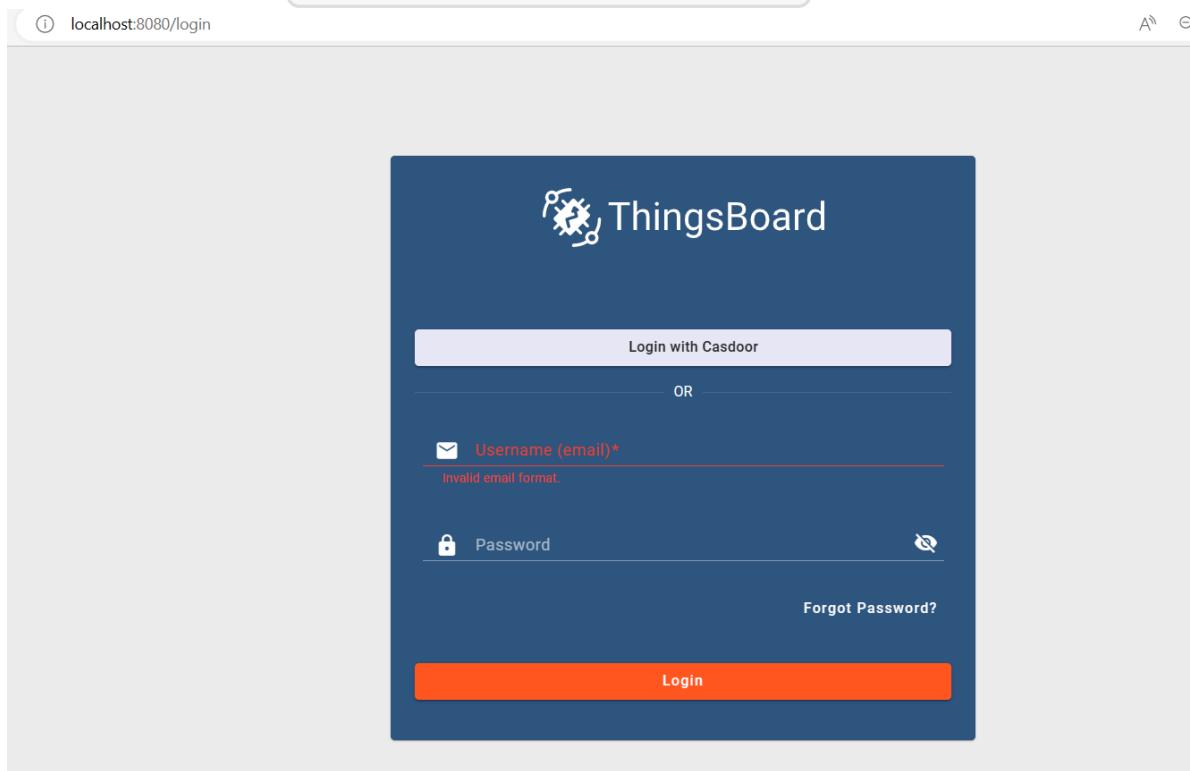
# Thingsboard

Before the integration, we need to deploy Casdoor locally.

Then we can quickly implement a Casdoor-based login page in our own app with the following steps.

## Step1. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://CASDOOR_HOSTNAME/login`



3. Copy the client ID and client secret, we will need it in the following steps.

## Step2. Add user in Casdoor

Now you have the application, but not a user. That means you need to create a user and assign the role.

Go to the "Users" page and click on "Add user" in the top right corner. That opens a new page where you can add the new user.

Save the user after adding a username and adding the organisation Thingsboard(other details are optional).

Now you need to set up a password for your user, which you can do by clicking manage your password.

Choose a password for your user and confirm it.

## Step3. Prerequisites and Build Thingsboard App

First of all, Thingsboard only support Java 11 (OpenJDK)

You can download in the following link:

[JDK Download Page](#)

Start the Thingsboard by follow.(Take Windows system as example)

- \$Download and extract the package. [Download the package](#)
- \$We can configure Thingsboard in \thingsboard\conf\thingsboard.yml as you like, configure the Kafka♦PostgreSQL and others.

- \$Run “install.bat –loadDemo” in command line in Thingsboard folder to install and add demo data

```
C:\Program Files (x86)\thingsboard>install.bat --loadDemo  
Detecting Java version installed.  
CurrentVersion 110  
Java 11 found!  
Installing thingsboard ...  
...  
ThingsBoard installed successfully!
```

- \$Input "net start thingsboard" in command line, we will get  
The ThingsBoard Server Application service is starting.  
The ThingsBoard Server Application service was started successfully.
- 

## Step4. Integrate Casdoor

Now open <http://localhost:8080/> and login in admin account:

account: [sysadmin@thingsboard.org](mailto:sysadmin@thingsboard.org) / password: sysadmin

After login in successfully, we click the oath2 button on the left bottom in the page.

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 features several cards:

- Tenants**: Shows 2 tenants with a "+" button.
- Tenant profiles**: Shows 2 tenant profiles with a "+" button.
- CPU**: Shows 15% usage on 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**: History from May 02 to May 05, showing 0k messages.
- Configured features**: Includes Email, SMS, Slack, OAuth 2, and 2FA.

Fill in the blank like this:

## Providers

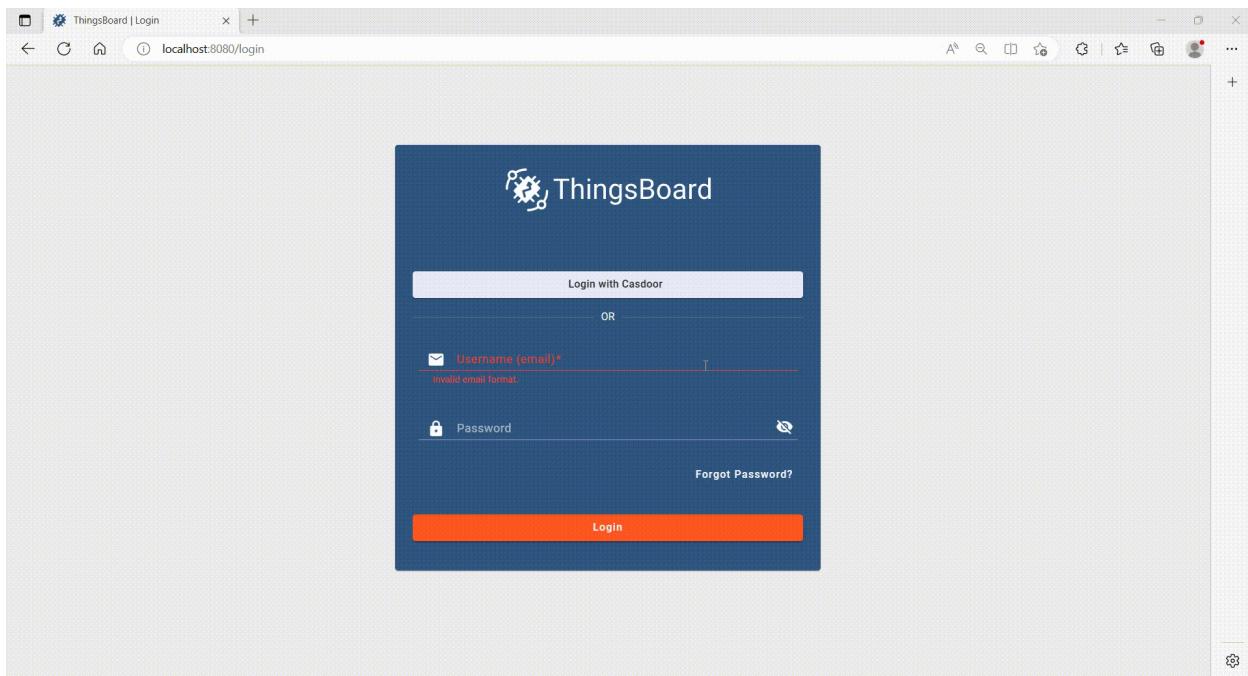
Custom

Login provider*	Custom	Allowed platforms	Web, Android, iOS
Client ID*	e324f9a3f55e1adac4ef	Client secret*	28b3f98c1f55c1cc57f74b9b1a68b5d2e79
General		Mapper	
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
Client authentication method*	POST		
Provider label*	Casdoor	Login button icon	
<input checked="" type="checkbox"/> Allow user creation			

We can get these values in this link: [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"]}
```

After filling these blanks, we successfully integrate Casdoor with Thingsboard, when we login <http://localhost:8080/>, we can get this:



# JavaScript

## WeChat MiniProgram

Using Casdoor in WeChat MiniProgram

# WeChat MiniProgram

## ⓘ INFO

Casdoor supports WeChat Mini Program after version 1.41.0

## Introduction

Since WeChat Mini Program does not support standardized OAuth, it cannot jump to the self-host Casdoor webpage for login. Therefore, the process of using Casdoor for WeChat Mini Program is different from that of ordinary programs.

This document will talk about how to access Casdoor to WeChat Mini Program. You can find the example on GitHub here: [casdoor-wechat-miniprogram-example](#). More detailed information can be found in the WeChat Mini Program [login document](#).

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

e.g., `https://door.casbin.com`.

## Step1. Deploy Casdoor

Firstly, the [Casdoor](#) should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. Set Casdoor's `origin` value (conf/app.conf) to `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
```

## Step2. Configure Casdoor application

1. Create a wechat idp in casdoor and fill your `APPID` and `APPSECRET` given to you by WeChat Mini Program develop platform:

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. Create or use an existing Casdoor application.
3. Add the idp added above to the application you want to use.

#### TIPS

For convenience, casdoor will read the first WeChat type idp in the application as the WeChat Mini Program idp by default.

So if you want to use the WeChat Mini Program in this app, don't add multiple WeChat type idp in one app.

# Step3. Write WeChat MiniProgram code

WeChat Mini Program provides an API to login internally and gets the Code. All you need to do is to send this Code to Casdoor. Casdoor will use this Code to get some information from WeChat server (such as OpenID, SessionKey, etc.).

The following code shows how to accomplish the above process:

```
// login in mini program
wx.login({
  success: res => {
    // this is your login code you need to send to casdoor
    console.log(res.code)

    wx.request({
      url: `${CASDOOR_HOSTNAME}/api/login/oauth/access_token`,
      method: "POST",
      data: {
        "tag": "wechat_miniprogram", // required
        "client_id": "6825f4f0af45554c8952",
        "code": res.code,
        "username": this.data.userInfo.nickName, // update user
        profile, when you login.
        "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 // get
        casdoor's accessToken
      }
    })
  }
})
```

It is worth mentioning that the `tag` parameter is mandatory and you need to make casdoor understand that this is a request from the WeChat Mini Program.

The above code passes in the username and avatar uri of the WeChat Mini Program user while logging in. You can also pass these two parameters without passing them first, and then pass them to casdoor after the login is successful and accessToken is obtained:

```
wx.getUserProfile({
  desc: 'share your info to casdoor',
  success: (res) => {
    this.setData({
      userInfo: res.userInfo,
      hasUserInfo: true
    })
    console.log(app.globalData.accessToken)
    wx.request({
      url: `${CASDOOR_HOSTNAME}/api/update-user`, // casdoor uri
      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)
      }
    })
  }
})
```

Also, you can use accessToken as a bearer token for any Casdoor operation you want.

 TIPS

Currently Casdoor is unable to bind existing accounts to the WeChat Mini Program users. After Casdoor gets the openID from WeChat if this id does not exist, a new user will be created, and if it exists, the old one will be used.

# Lua



Using Casdoor in APISIX

# APISIX

Currently there are 2 methods to use Casdoor to connect to APISIX via APISIX plugins and protect the apis behind the APISIX: using APISIX's Casdoor plugin or using APISIX's OIDC plugin.

## Connect Casdoor via APISIX's Casdoor plugin

This plugin, authz-casdoor, can protect apis behind APISIX, forcing every single request to get authenticated, without modifying codes of api.

### How to enable it

You need to specify this plugin when creating the route, and give out all required fields. Here is an example.

```
curl "http://127.0.0.1:9080/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"  
        }  
    }  
}
```

In this example, using apisix's admin API we created a route "/anything/\*" pointed to "httpbin.org:80", and with "authz-casdoor" enabled. This route is now under authentication protection of Casdoor.

## Attributes

Name	Type	Requirement	Default	Valid	Description
endpoint_addr	string	required			The url of casdoor.
client_id	string	required			The client id in casdoor.
client_secret	string	required			The client secret in casdoor.
callback_url	string	required			The callback url which is used to receive state and code.

*endpoint\_addr and callback\_url should not end with '/'*

In the configuration of "authz-casdoor" plugin we can see four parameters.

The first one is "callback\_url". This is exactly the callback url in OAuth2. It should be emphasized that this callback url **must belong to the "uri" you specified for the route**, for example, in this example, http://localhost:9080/anything/callback obviously belongs to "/anything/\*". Only by this way can the visit toward callback\_url can be intercepted and utilized by the plugin(so that the plugin can

get the code and state in Oauth2). The logic of `callback_url` is implemented completely by the plugin so that there is no need to modify the server to implement this callback.

The second parameter "endpoint\_addr" is obviously the url of Casdoor. The third and fourth parameters are "client\_id" and "client\_secret", which you can acquire from Casdoor when you register an app.

## How it works?

Suppose a new user who has never visited this route before is going to visit it (`http://localhost:9080/anything/d?param1=foo&param2=bar`), considering that "authz-casdoor" is enabled, this visit would be processed by "authz-casdoor" plugin first. After checking the session and confirming that this user hasn't been authenticated, the visit will be intercepted. With the original url user wants to visit kept, he will be redirected to the login page of Casdoor.

After successfully logging in with username and password(or whatever method he uses), Casdoor will redirect this user to the "callback\_url" with GET parameters "code" and "state" specified. Because the "callback\_url" is known by the plugin, when the visit toward the "callback\_url" is intercepted this time, the logic of "Authorization code Grant Flow" in Oauth2 will be triggered, which means this plugin will request the access token to confirm whether this user is really logged in. After this confirmation, this plugin will redirect this user to the original url user wants to visit, which was kept by us previously. The logged-in status will also be kept in the session.

Next time this user want to visit url behind this route (for example, `http://localhost:9080/anything/d`), after discovering that this user has been authenticated previously, this plugin won't redirect this user anymore so that this user can visit whatever he wants under this route without being interfered.

# Connect Casdoor via APISIX's OIDC plugin

Casdoor can use the OIDC protocol to link to APISIX, and this document will show you how to do it.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`APISIX_HOSTNAME`: Domain name or IP where APISIX is deployed.

## Step1. Deploy Casdoor and APISIX

Firstly, the [Casdoor](#) and [APISIX](#) should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. Set Casdoor's `origin` value (conf/app.conf) to `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
```

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://APISIX_HOSTNAME/REDIRECTWHATYOUWANT`, and change `REDIRECTWHATYOUWANT` to the redirect url you need.
3. Select "JWT-Empty" for the Token format option
4. Add provider you want and supplement other settings.

The screenshot shows the Casdoor application settings page. It includes fields for Client ID (07860a229bd0b162cd1a), Client secret (ea021...9373fe3e), Redirect URLs (with an 'Add' button and a URL entry field containing http://localhost:9000/callback), and Token format (JWT-Empty).

Not surprisingly, you can get two values on the application settings page: `Client ID` and `Client secret` like the picture above, and we will use them in the next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure APISIX

APISIX has official [OIDC](#) support, which is implemented using [lua-resty-openidc](#).

You can customize the settings according to the APISIX OIDC documentation, in which the following routing settings will be used:

```
#Use your own X-Api-Key
$ curl -XPOST APISIX_HOSTNAME/apisix/admin/routes -H "X-Api-Key:"
```

Now, visit `http://APISIX_HOSTNAME/get`, the browser will redirect you to the casdoor login page, and after successfully logging in, you will, not surprisingly, see that we have sent a request to `httpbin.org`.



# PHP

## Zentao

Using Casdoor for authentication in Zentao

## ShowDoc

Using Casdoor as oAuth2 server in ShowDoc

## Flarum

Using OAuth2 to connect various applications, like Flarum

## Moodle

Using Oauth to connect Moodle

# Zentao

Zentao is an agile(scrum) project management system/tool, but it does not support OIDC itself. For integrating Zentao with Casdoor SSO, we should via 3rd-party OIDC module [zentao-oidc](#), and this document will show you how to do it.

## Step1. Deploy Casdoor and Zentao

Firstly, the [Casdoor](#) and [Zentao](#) should be deployed. After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used successfully.
2. You can successfully log in and use Zentao

## Step2. Integrated Zentao OIDC third party module

install [zentao-oidc](#)

```
git clone https://github.com/casdoor/zentao-oidc.git
```

or you can download the ZIP and unzip it.

This module is used for Zentao integrating with SSO for OpenId. The usage is as follows:

1. Copy the entire oidc directory to the Module of The Zentao and use it as a

module of the Zentao. Rename the downloaded package to "oidc"

## 2. Configure the filter

Because the framework of Zentao filters the parameters in URL and does not allow Spaces. So you need to put the following code at the end of `/config/my.php`.

```
$filter->oidc=new stdclass();
$filter->oidc->index=new stdclass();
$filter->oidc->index->paramValue['scope']='reg::any';
```

## 3. Modify `/module/common/model.php`

Put 'oidc' on the anonymous access list and add a line to the `isOpenMethod` method of `model.php`.

```
public function isOpenMethod($module, $method){
    if($module == 'oidc' and $method == 'index') return true;
}
```

## 4. If you do not want the Zentao login screen to appear, go directly to the Casdoor login screen. Modify the last line of code at `public function checkPriv()` in `/module/common/model.php`.

```
//return print(js::locate(helper::createLink('user', 'login',
"referer=$referer")));
return print(js::locate(helper::createLink('oidc', 'index',
"referer=$referer")));
```

## 5. Modify `setSuperVars()` method inside of `framework/base/`

`router.class.php`, comment out the following statements.

```
public function setSuperVars()  
// unset($_REQUEST);
```

## Step3. Configure Casdoor Application

1. Create or use an existing Casdoor application.
2. Add Your redirect 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 ? :	d8d7715e24f077066a20						
Client secret ? :	[REDACTED]						
Cert ? :	cert-built-in						
Redirect URLs ? :	<table border="1"><tr><td>Redirect URLs</td><td>Add</td></tr><tr><td colspan="2">Redirect URL</td></tr><tr><td colspan="2">🔗 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. Add provider you want and supplement other settings.

## Step4. Configure Zentao

Configure `config.php` in the oidc

```
$config->oidc->clientId=<Your ClientId>;  
$config->oidc->clientSecret=<Your ClientSecret>;  
$config->oidc->issuer="http://localhost:8000";
```

set your redirect Url in module/oidc `public function index()`

```
$oidc->setRedirectURL($path."/zentao/oidc-index.html");
```

 NOTE

The URL here refers to calling the 'index' method in the 'oidc' module. You also need to set a variable separator, which the framework defaults to with a dash : -

please refer to zentao's official framework for details. "[zentaoPHP](#)"

# ShowDoc

## Using Casdoor for authentication in ShowDoc

ShowDoc is an online API documentation, technical documentation tool perfect for IT teams. Showdoc makes it easy to use Markdown syntax to write beautiful API documents, data dictionary documents, technical documents, online Excel documents, and more.

Showdoc supports 3rd-party authentication including Oauth. Here is the tutorial for achieving this.

### step1. Create an Casdoor application

Go to your Casdoor and add your new application Showdoc. Here is an example of creating the Showdoc application in Casdoor.

[Edit Application](#)[Save](#)[Save & Exit](#)Name [?](#) :

myApplication

Display name [?](#) :

myApplication

Logo [?](#) :URL [?](#) :[https://cdn.casdoor.com/logo/casdoor-logo\\_1185x256.png](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

Please remember the `client ID` and `client Secret` for next step.

**!** INFO

Please don't fill in the `callback url` in this step. The url depends on the configurations on `showdoc` in next step. Later we will come back to set a correct callback url.

## step2. Configure Showdoc

First, start the oAuth2 login button. Then fill in the `callback url` as shown in the example. Fill in the `client ID` and `client secret` remembered in previous step.

The screenshot shows the ShowDoc configuration interface. On the left, there is a sidebar with the following menu items:

- 用户管理
- 项目管理
- 附件管理
- 集成登录** (highlighted with a red box)
- 站点设置
- 关于本站

The main configuration area has the following tabs at the top: LDAP, **OAuth2**, and 通用接入. The OAuth2 tab is selected. A red box highlights the "启动OAuth2登录" toggle switch, which is turned on. Below it, the "callback url" field contains the value `http://127.0.0.1/server/?s=/api/extLogin/oauth2`. A note below the field says "callback url填写示例 http://【你的showdoc地址】/server/?s=/api/extLogin/oauth2". The configuration fields are as follows:

入口文字提示	casdoor sso
Client id	208d745196c23df9fd5b
Client secret	4c89f447af77bc276431ab885463ebcb8d6efc3c
Oauth host	http:// 127.0.0.1:8000
Authorize path	/login/oauth/authorize
AccessToken path	/api/login/oauth/access_token

`Authorize path`, `AccessToken path`, `User info path` are required. You can fill as shown below.

```
Authorize path: /login/oauth/authorize
AccessToken path: /api/login/oauth/access_token
User info path: /api/get-account
```

## step3. Configure the callback url in casdoor

Go back to the application edit page in step 1, and add the `callback url` you filled in showdoc.

The screenshot shows a user interface for managing redirect URLs. At the top, there is a header with the text "Redirect URLs (2)". Below the header, there are two buttons: "Redirect URLs" and "Add". The "Add" button is highlighted with a blue background. Underneath these buttons, there is a section titled "Redirect URL" containing a single entry: "<http://127.0.0.1/server/?s=/api/extLogin/oauth2>".

## step4. Have a try on showdoc

You are supposed to see this in login page:

# 登录

用户名/邮箱

密码

验证码



登录

[注册新账号](#)

[casdoor sso](#)

Congratulations! You have completed all the steps. Press the 'casdoor sso' button and you will be redirected to casdoor login page.

# Flarum

Casdoor can use OAuth2 to connect various applications. Here we will use Flarum as an example to show you how to use OAuth2 to connect to your applications.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Flarum_HOSTNAME`: Domain name or IP where Flarum is deployed.

## Step1. Deploy Casdoor and Flarum

Firstly, the Casdoor and Flarum should be deployed.

After a successful deployment, you need to ensure:

1. Download the Flarum plugin [FoF Passport](#)
2. Casdoor can be logged in and used normally.
3. You can set `CASDOOR_HOSTNAME = http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find a redirect url: `<CASDOOR_HOSTNAME>/auth/passport`
3. Add your redirect url to casdoor application:

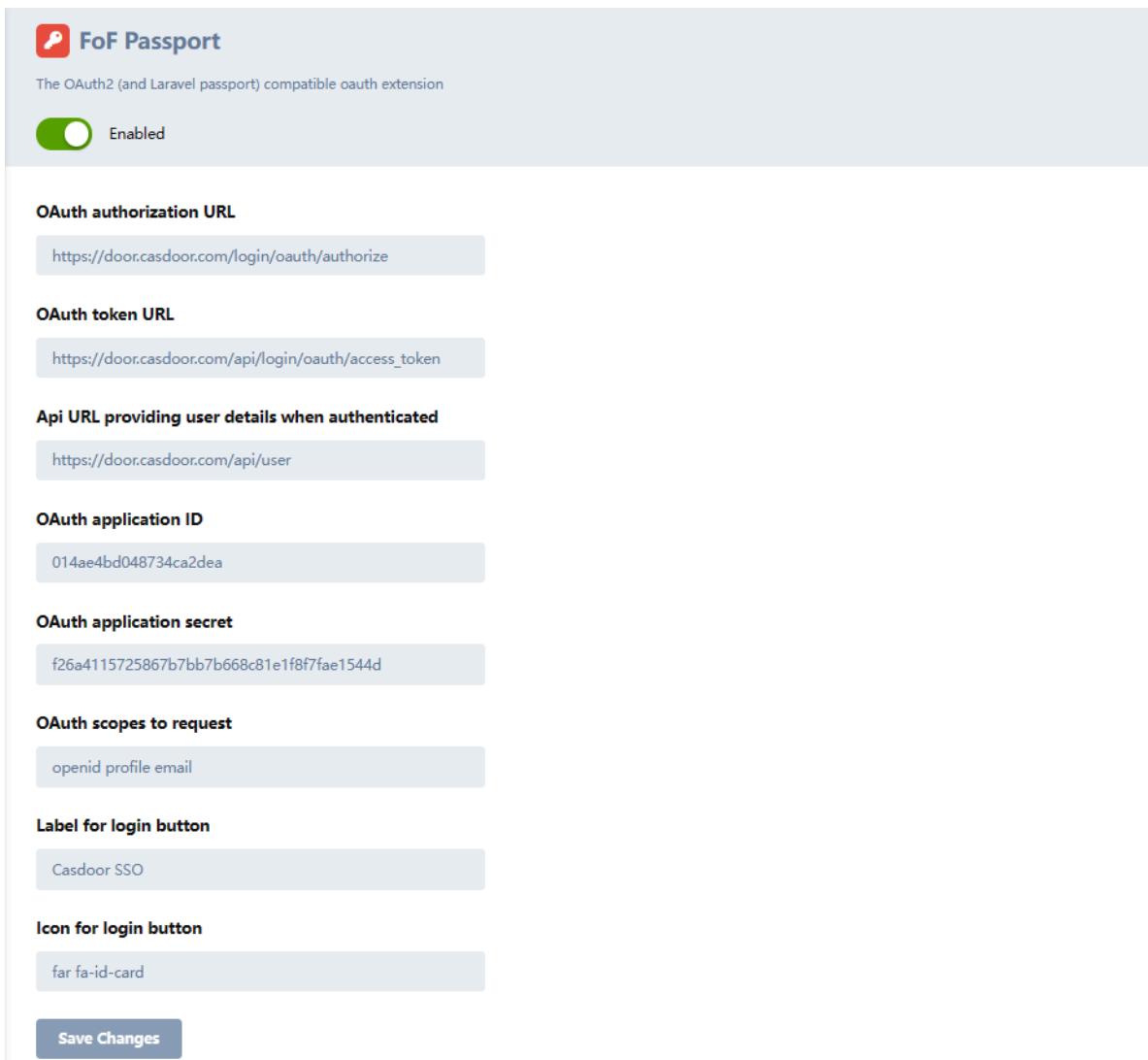
The screenshot shows the 'Application Settings' section of the Casdoor web interface. It includes fields for 'Client ID' (014ae4bd048734ca2dea), 'Client secret' (f26a4115725867b7bb7b668c81e1f8ffae1544d), 'Cert' (cert-built-in), and a 'Redirect URLs' section containing a single entry: <your flarum install>/auth/passport.

Not surprisingly, you can get two values on the application settings page: `Client ID` and `Client secret` like the picture above, we will use them in the next step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure Flarum

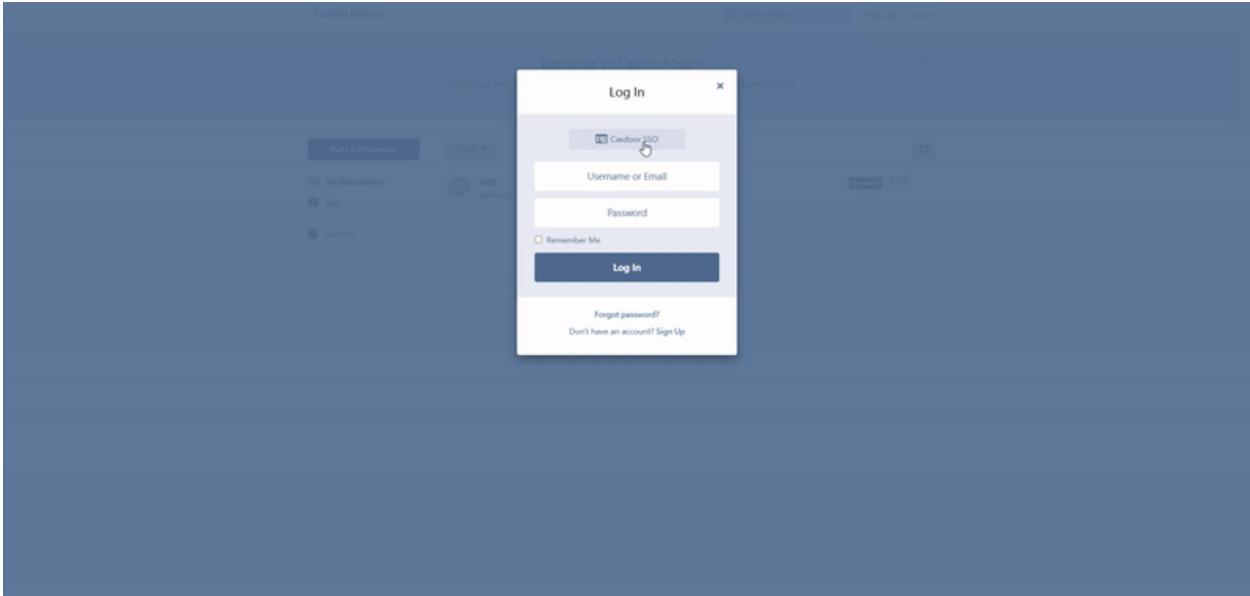
1. You should install a plugin [FoF Passport](#)
2. You should config this app



3. You can find Client Id and Client Secret in Casdoor application page.

- 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

Log out of Flarum, and test SSO.



# Moodle

Casdoor can use Oauth to connect Moodle.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`Moodle_HOSTNAME`: Domain name or IP where Moodle is deployed.

## Step1. Deploy Casdoor and Moodle

Firstly, the Casdoor and Moodle should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. You can set `CASDOOR_HOSTNAME = http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find a redirect url: `Moddle_HOSTNAME /admin/oauth2callback.php`
3. Add your redirect url to casdoor application

More infomation for [OAuth](#)

# Step3. Configure Moodle

## 1. You should find OAuth

MyMoodle Home Dashboard My courses Site administration AU Edit mode

Site administration

General Users Courses Grades Plugins Appearance Server Reports Development

Your site is not yet registered. [Register your site](#)

**Server**

- System paths
- Support contact
- Session handling
- HTTP
- Maintenance mode
- Cleanup
- Environment
- PHP info
- Performance
- Update notifications
- File types
- OAuth 2 services**

## 2. You should config this app

MyMoodle Home Dashboard My courses Site administration AU Edit mode

Detailed instructions on configuring the common OAuth 2 services

Name: Casdoor

Client ID: 154fb67917b18c0a1850 → **your Client ID**

Client secret: 380a93b571ab0f8545fbc → **your Client secret**

Authenticate token requests via HTTP headers

Service base URL: https://demo.casdoor.com → **your Casdoor\_Home**

Logo URL: https://cdn.casdoor.com/s

This service will be used: Login page and internal services

Name displayed on the login page:

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:

Require email verification

I understand that disabling email verification can be a security issue.

Save changes Cancel

## 3. You should config this Mappling

## 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"

## 4. Find OAuth2 plugin

The screenshot shows the Moodle Plugins page. At the top, there is a navigation bar with tabs: General, Users, Courses, Grades, Plugins, Appearance, Server, Reports, and Development. The Plugins tab is highlighted with a blue underline. Below the navigation bar, a red arrow points to the 'Plugins' tab. A pink banner at the top says 'Your site is not yet registered.' with a 'Register your site' button. The main content area is divided into sections:

- Plugins**: Includes links to 'Install plugins' and 'Plugins overview'.
- Activity modules**: A large list of activity types including Book, Chat, Database, External tool, Feedback, File, Folder, Forum, Glossary, H5P, IMS content package, Lesson, Page, Quiz, and Workshop.
- Admin tools**: Includes links to 'Manage admin tools', Accessibility, Brickfield registration, Accessibility toolkit settings, Reports, and Recycle bin.
- Antivirus plugins**: Includes a link to 'Manage antivirus plugins'.
- Authentication**: Includes a link to 'Manage authentication'. A red arrow points to this section.

## 5. Enable OAuth2 plugin

## Manage authentication

### Available authentication plugins

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	2			<a href="#">Settings</a>		
No login	0					
Email-based self-registration	0			<a href="#">Settings</a>		<a href="#">Uninstall</a>
OAuth 2	8			<a href="#">Settings</a>	<a href="#">Test settings</a>	

## 6. if you want Casdoor's email can't be edited

### 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	Unlocked Default: Unlocked
Lock value (Last name) auth_oauth2   field_lock_lastname	Unlocked Default: Unlocked
Lock value (Email address) auth_oauth2   field_lock_email	Locked Default: Unlocked
Lock value (City/town) auth_oauth2   field_lock_city	Unlocked Default: Unlocked
Lock value (Country) auth_oauth2   field_lock_country	Unlocked Default: Unlocked
Lock value (Language) auth_oauth2   field_lock_lang	Unlocked Default: Unlocked

here is switch to lock email

More infomation for [Moodle](#) and Fields mapping

Log out of Moodle, and test SSO.

The screenshot shows the Moodle login page with the title "MyMoodle Website". At the top, there are links for "MyMoodle" and "Home". On the right side, there is a "Log in" button. A red circle highlights this "Log in" button, indicating where the user should click to log out and test SSO.

# Ruby



Using Casdoor for authentication in self-developed GitLab server

# GitLab

Casdoor can use the OIDC protocol to link to self-deployed GitLab server, and this document will show you how to do it.

## ⚠ CAUTION

As [GitLab docs](#) said, GitLab only works with OpenID providers that use HTTPS, so you need to deploy Casdoor with HTTPS, like putting Casdoor behind a NGINX reverse proxy with SSL certificate setup. Casdoor itself only listens to 8000 port by default via HTTP and has no HTTPS related functionality.

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed. e.g.,  
`https://door.casbin.com`.

`GITLAB_HOSTNAME`: Domain name or IP where GitLab is deployed. e.g.,  
`https://gitlab.com`.

## Step1. Deploy Casdoor and GitLab

Firstly, the [Casdoor](#) and [GitLab](#) should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. Set Casdoor's `origin` value (`conf/app.conf`) to `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
```

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: [http://GITLAB\\_HOSTNAME/users/auth/openid\\_connect/callback](http://GITLAB_HOSTNAME/users/auth/openid_connect/callback).
3. Add provider you want and supplement other settings.

Description <a href="#">?</a> :	GitLab
Organization <a href="#">?</a> :	built-in
Client ID <a href="#">?</a> :	eab9...35b6 <span style="color: red;">Client ID</span>
Client secret <a href="#">?</a> :	95e7...b3a0188a5 <span style="color: red;">Client secret</span>
Redirect URLs <a href="#">?</a> :	<a href="#">Redirect URLs</a> <a href="#">Add</a>
	<a href="#">Redirect URL</a>
	<a href="http://GITLAB_HOSTNAME/users/auth/openid_connect/callback">http://GITLAB_HOSTNAME/users/auth/openid_connect/callback</a> <span style="color: red;">GitLab redirect url</span>

Not surprisingly, you can get two values on the application settings page: [Client ID](#) and [Client secret](#) like the picture above, and we will use them in the next

step.

Open your favorite browser and visit: `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`, you will see the OIDC configure of Casdoor.

## Step3. Configure GitLab

You can follow the steps below to set this up, or make custom changes according to [this document](#)(e.g., you are installing GitLab using source code rather than Omnibus).

1. On your GitLab server, open the configuration file.

```
sudo editor /etc/gitlab/gitlab.rb
```

2. Add the provider configuration. (HOSTNAME url should include http or https)

```
gitlab_rails['omniauth_providers'] = [
  {
    name: "openid_connect",
    label: "Casdoor", # optional label for login button,
    defaults to "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>",
      }
    }
  }
]
```

3. Reboot your GitLab server.
4. Each registered user can open `GITLAB_HOSTNAME/-/profile/account`, connect the casdoor account.

User Settings > Account

Two-Factor Authentication  
Status: Disabled

Enable two-factor authentication

Social sign-in  
Activate sign in with one of the following services

Connected Accounts  
Click on icon to activate sign in with one of the following services

**Connect Casdoor**

5. Finish. Now, you can login your own GitLab by casdoor.

## GitLab

### A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

This is a self-managed instance of GitLab.

Username or email

Password

Remember me      [Forgot your password?](#)

**Sign in**

Don't have an account yet? [Register now](#)

Sign in with

**Casdoor**

Remember me

# Haskell

## Hasura

Before the integration, we need to deploy Casdoor locally.

# Hasura

Before the integration, we need to deploy Casdoor locally.

Then we can quickly implement a Casdoor-based login page in our own app with the following steps.

## Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Add a redirect url: `http://CASDOOR_HOSTNAME/login`



The screenshot shows the Casdoor Redirect URLs configuration page. It has a header with "Redirect URLs" and a "Add" button. Below is a table with one row:

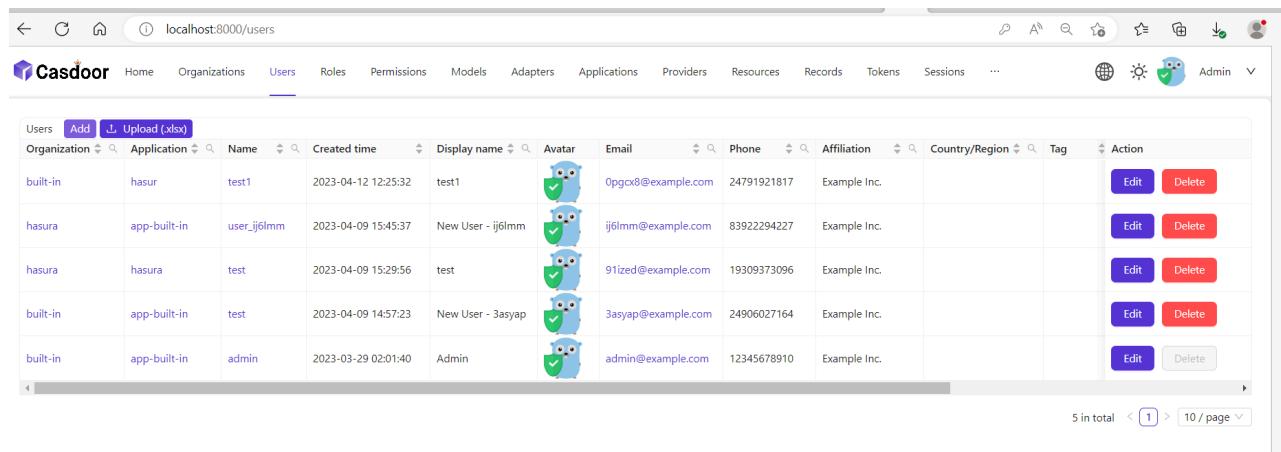
Redirect URL	Action
<code>http://localhost:8080/login</code>	

3. Copy the client ID, we will need it in the following steps.

## Add user in Casdoor

Now you have the application, but not a user. That means you need to create a user and assign the role.

Go to the “Users” page and click on “Add user” in the top right corner. That opens a new page where you can add the new user.



The screenshot shows the Casdoor Users management page. The table lists the following users:

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		0pgox8@example.com	24791921817	Example Inc.			
hasura	app-built-in	user_ij6lmm	2023-04-09 15:45:37	New User - ij6lmm		ij6lmm@example.com	83922294227	Example Inc.			
hasura	hasura	test	2023-04-09 15:29:56	test		91ized@example.com	19309373096	Example Inc.			
built-in	app-built-in	test	2023-04-09 14:57:23	New User - 3asyap		3asyap@example.com	24906027164	Example Inc.			
built-in	app-built-in	admin	2023-03-29 02:01:40	Admin		admin@example.com	12345678910	Example Inc.			

At the bottom, it says "5 in total" and has navigation buttons for page 1 of 10.

Save the user after adding a username and adding the organisation Hasura(other details are optional).

Now you need to set up a password for your user, which you can do by clicking manage your password.

Choose a password for your user and confirm it.

# Build Hasura App

Start the Hasura by docker or Hasura Cloud.

Now create a `users` table with the following columns:

- `id` of type Text (Primary Key)
- `username` of type Text

See the image below for reference.

The screenshot shows the Hasura Data Manager interface. On the left, there's a sidebar with 'Data Manager' and 'Databases (1)'. It lists two databases: 'default' and 'public'. Under 'default', it says 'No tables or views in this schema'. Below that is a 'SQL' section. The main area is titled 'Add a New Table' and has a form for creating a 'users' table. The 'Table Name' field contains 'users'. The 'Table Comment' field contains 'comment'. In the 'CONFIGURE FIELDS' section, there are three columns defined: 'id' (Text, nullable, unique), 'username' (Text, nullable, unique), and 'column\_name' (column\_type, nullable, unique). A button '+ Frequently used columns' is visible. In the 'TABLE PROPERTIES' section, the 'Primary Key' is set to 'id'. A 'Foreign Keys' section is also present. A yellow hand icon is in the bottom right corner of the main form area.

The next step is to create a `user` role for the app. Users should be able to see only their records, but not the other people's records.

Configure the `user` role as shown in the image below. For more information, read about [configuring permission rules in Hasura](#).

The screenshot shows the Hasura Cloud interface with the 'DATA' tab selected. On the left, the 'Data Manager' sidebar lists databases: 'default' and 'public'. Under 'public', there is a 'users' table. The main area displays a permissions matrix:

Role	insert	select	update	delete
admin	✓	✓	✓	✓
user	✗	✗	✗	✗

Below the matrix, a modal window titled 'Role: user Action: select' is open, showing a custom check for row-level permissions:

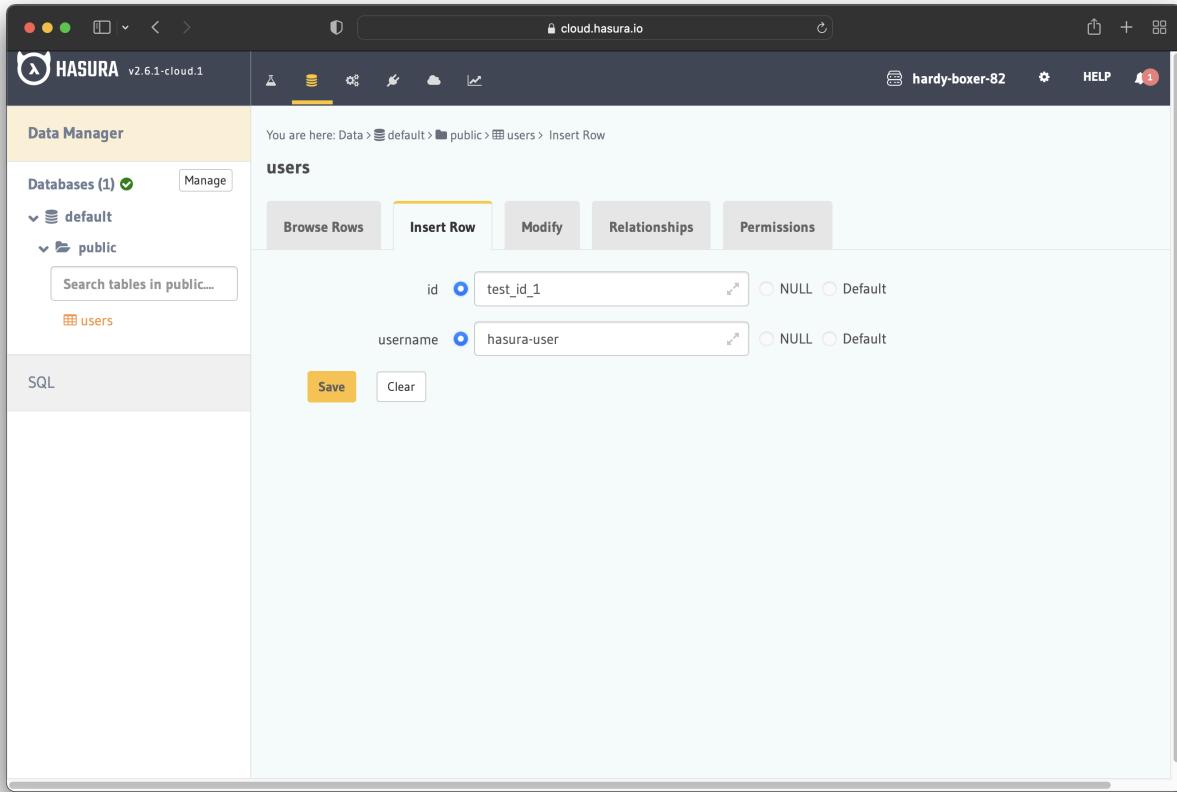
```
1  {"id": {"_eq": "X-Hasura-User-Id"}}

{
  "id": {
    "eq": "X-Hasura-User-Id"
  }
}
```

Under 'Column select permissions', it shows that the 'user' role has access to the 'id' and 'username' columns.

This way, users cannot read other people's records. They can only access theirs.

For testing purposes, add a dummy user. This is to ensure that when you use the JWT token, you only see your user's details and not other users' details.



Now you need to set the `JWT_SECRET` in Hasura.

## Configure Hasura with Casdoor

In this step, you need to add the `HASURA_GRAPHQL_JWT_SECRET` to Hasura.

To do so, go to the Hasura docker-compose.yaml and then add the new `HASURA_GRAPHQL_JWT_SECRET` as below.

The `HASURA_GRAPHQL_JWT_SECRET` should be in the following format:

```
HASURA_GRAPHQL_JWT_SECRET: '{"claims_map": {  
    "x-hasura-allowed-roles": ["user", "editor"],  
    "x-hasura-default-role": "user",  
    "x-hasura-user-id": "userID"  
}, "jwk_url": "https://door.casdoor.com/.well-known/jwks"}'
```

Save the change, and reload the 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"}
```

## Retrieve JWT Token

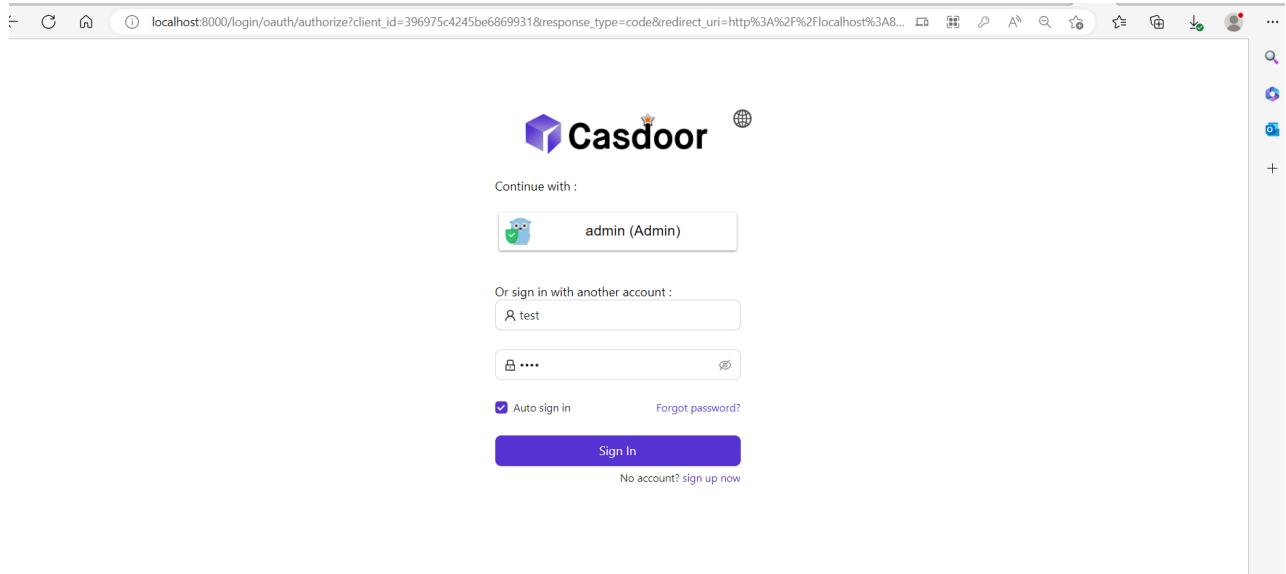
Since there is no client implementation, you can get your access token by making a request by below URL:

```
http://localhost:8000/login/oauth/authorize?client\_id=<clientID>&response\_type=code&redirect\_uri=http%3A%2Flocalhost%3A8080%2Flogin&scope=read&state=app-built-in<public certificate>
```

Change the client ID to the ID you copied before, and input the public certificate of Casdoor which you can find in Casdoor/Certs.

Then input the username and password you create for Hasura before.

Click Sign in.



Go back to Casdoor/Token page

localhost:8000/tokens

Name	Created time	Application	Organization	User	Authorization code	Access token	Action
b6ea3e35-abcf-41d8-a1a2-01f0fd8264b	2023-04-12 13:06:53	hasura	hasura	test	433b504b4f6a593e4a11	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
16024557-df21-4779-bfb9-959e5dae078c	2023-04-12 12:51:47	hasur	built-in	test1	2879fbcc282019cf7f23c	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
f3cb1070-c2d4-40f0-8bc0-59919d26d162	2023-04-11 15:04:00	hasura	hasura	test	2a370971798d403fc6ef	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
64993582-2322-4df7-ab20-cb23201bc77b	2023-04-11 00:37:22	springboot	built-in	admin	a2396037c3ba4fd9221e	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
f65a3813-a655-47f0-9c9a-f08ce4607815	2023-04-11 00:31:37	springboot	built-in	admin	d048c7f9cd1469fd829d	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
5828069e-15eb-4c92-933c-feada8ed621c	2023-04-11 00:06:54	springboot	built-in	admin	7cc27dc752cc4188ac8d	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
2277e0f2-7e78-462f-a654-3c53759784af	2023-04-11 00:05:17	springboot	built-in	admin	56141e709a06931b7faa	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
55bd324a-6039-40f6-b707-2a55d78ae911	2023-04-11 00:05:07	springboot	built-in	admin	9a1413bc172591a64353	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
4b30acbe-fa22-4387-8098-9a46e70f6972	2023-04-10 23:59:19	springboot	built-in	admin	88b0997b675917f20fdc	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>

Find the Username you input before then click edit

Copy the Access Token.

Edit Token		<button>Save</button>	<button>Save &amp; Exit</button>
Name:	b6ea3e35-abcf-41d8-a1a2-01f0fd8264b		
Application:	hasura		
Organization:	hasura		
User:	test		
Authorization code:	433b504b4f6a593e4a11		
Access token:	eyJhbGciOiJSUz1NilsImtpZC16lmNcnQtYnVpbHQtaW4iLCj0eXAIoIKV1QifQ.eyJvd25ciI6lmhhc3VyYSlsm5hbWUiOj0ZXN0IwiY3JlYXRIZFRpbWUiOilyMDIzLTA0LTAsVDE1Oj50JU2KzA4OjAwliwidXBkYXRIZFRpbWUiOiiLCjPZC16ijRly		
Expires in:	604800		
Scope:	read		
Token type:	Bearer		
<button>Save</button>		<button>Save &amp; Exit</button>	

Now you can use the access token to make the authenticated request. Hasura returned the appropriate user rather than returning all the users from the database.

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 eyJhbGciOiJSUzI1NiIsImtpZCI6ImNlcnQtYnVpbHQtaW4iLCJ0eXAiOiJKV1QiLCJyIvd25ciI6Imhhc3VyYSlsImShbWL
Enter Key		Enter Value

Explorer X GraphiQL ▶ Prettify History Explorer Code Exporter REST Derive action Analyze ◀ Docs

query MyQuery {  
 users {  
 id  
 username  
 }  
}

1 {  
 "data": {  
 "users": [  
 {  
 "id": "4ec7cce-ec7b-4191-a78d-e11f50686f8b",  
 "username": "test"  
 }  
 ]  
 }  
}

QUERY VARIABLES

# Python



JumpServer

Using CAS to connect JumpServer

# JumpServer

[Casdoor](#) can use CAS to connect [JumpServer](#).

The following are some of the names in the configuration:

`CASDOOR_HOSTNAME`: Domain name or IP where Casdoor server is deployed.

`JumpServer_HOSTNAME`: Domain name or IP where JumpServer is deployed.

## Step1. Deploy Casdoor and JumpServer

Firstly, the [Casdoor](#) and [JumpServer](#) should be deployed.

After a successful deployment, you need to ensure:

1. Casdoor can be logged in and used normally.
2. You can set `CASDOOR_HOSTNAME = http://localhost:8000`. When deploy Casdoor in `prod` mode. See [production mode](#).

## Step2. Configure Casdoor application

1. Create or use an existing Casdoor application.
2. Find a redirect url: `CASDOOR_HOSTNAME/cas/your organization/your application/login`
3. Add your redirect url to casdoor application: `JumpServer_HOSTNAME`

More information for [CAS](#)

# Step3. Configure JumpServer

## 1. You should find Auth

The screenshot shows the 'Auth' configuration page in the JumpServer web interface. The left sidebar has a 'Auth' option highlighted with a red arrow. The main content area has a 'Basic' tab selected, and a 'CAS' tab is also present, indicated by another red arrow. The 'Basic' section contains fields for 'Enable CAS Auth' (switched on), '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 includes 'Logout completely' (switched on) and a 'User attr map' code editor containing:

```
1 = [
2   "uid": "username"
3 ]
```

Buttons for 'Reset' and 'Submit' are at the bottom.

## 2. You should config this app

This screenshot is identical to the one above, showing the 'Auth' configuration page. It highlights the 'Auth' tab in the sidebar and the 'CAS' tab in the main content area. Red arrows point to the 'Enable CAS Auth' switch, the 'Server url' field (containing http://101.43.192.216:8000/cas/jump/jumpServer/login), and the 'User attr map' code editor. The code in the editor is the same as in the previous screenshot.

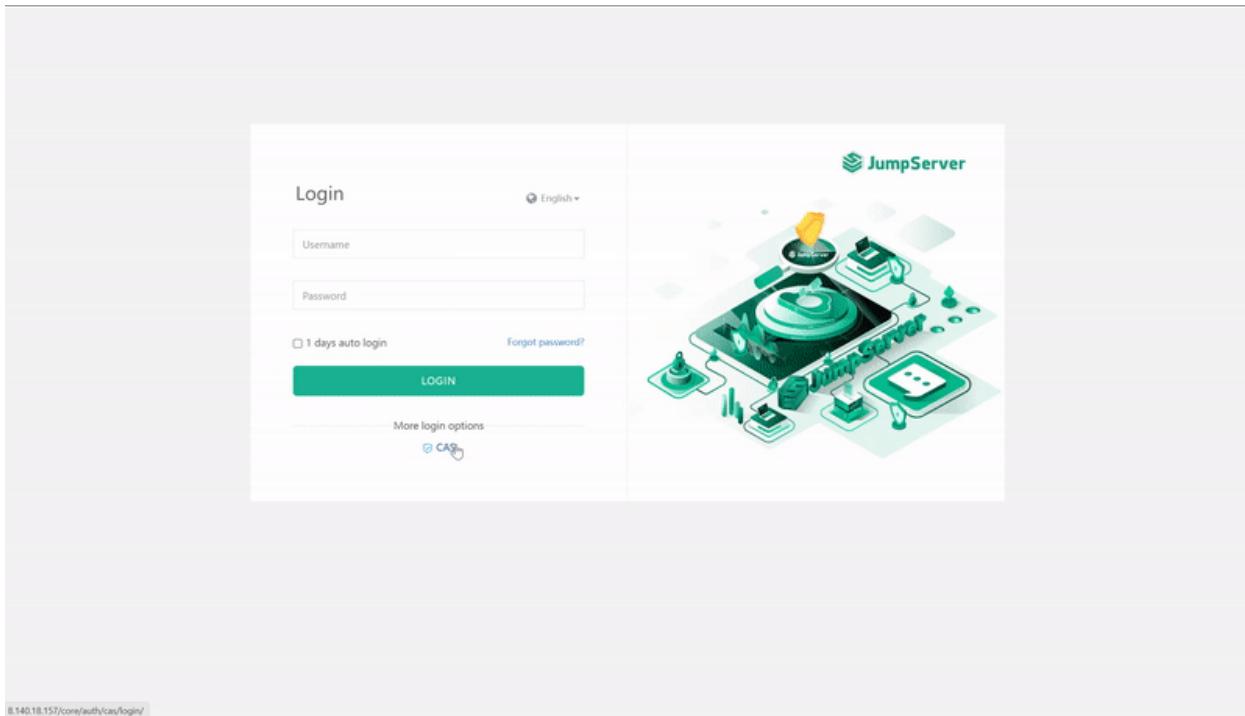
- /login endpoint: <https://door.casdoor.com/cas/casbin/cas-java-app/>

## 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>

More infomation for [CAS](#) and [JumpServer](#)

Log out of JumpServer, and test SSO.





&gt;

Monitoring

# Monitoring

## Web UI

Monitor runtime information on the casdoor Web page

## Prometheus

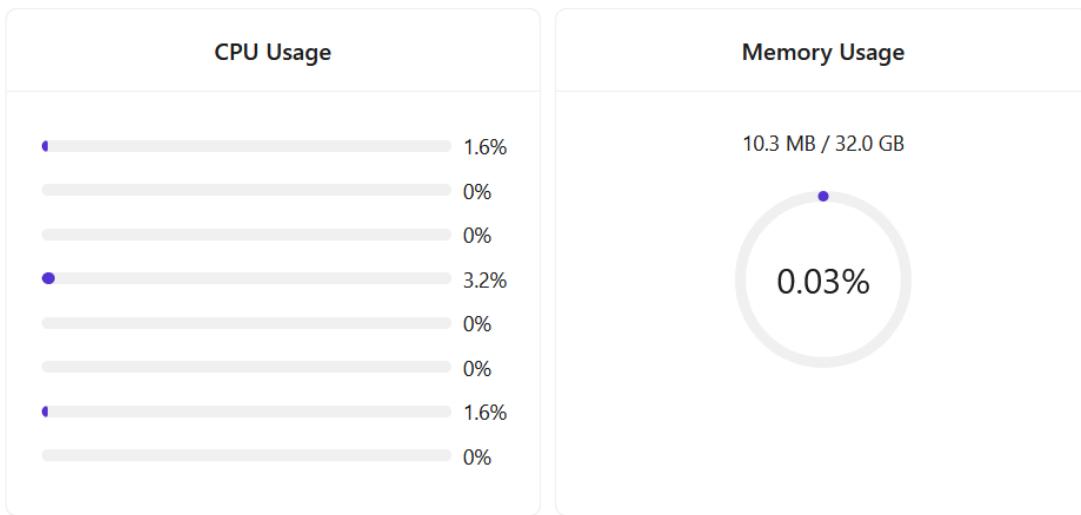
Use prometheus to collect information about running casdoor

# Web UI

You can monitor the runtime information of casdoor on the [casdoor Web page](#), including CPU Usage, Memory Usage, API Latency, and API Throughput

You can view the following information on the UI

- CPU Usage and Memory Usage



- API Latency, Including count times and average latency

API Latency				
Method	Endpoint	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	1.000	

- API Throughput, Including total throughput and throughput per API

API Throughput			
Total Throughput: 2			
Name	Method	Throughput	
/api/get-prometheus-info	GET	1	
/api/get-system-info	GET	1	

# Prometheus

Use Prometheus to collect casdoor's runtime metrics, including API Throughput, API Latency, CPU Usage, Memory Usage, and so on, as you should configure your Prometheus profile

```
global:  
  scrape_interval: 10s #The time interval for fetching metrics  
  
scrape_configs:  
  - job_name: 'prometheus'  
    static_configs:  
      - targets: ['localhost:9090']  
  - job_name: 'casdoor' #Name of the application to be monitored  
    static_configs:  
      - targets: ['localhost:8000'] #Back-end address of casdoor deployment  
    metrics_path: '/api/metrics' #Path for collecting indicators
```

After the configuration is successful, you will find the following information in Prometheus







> Internationalization

# Internationalization

Casdoor supports multi-languages. By deploying the translations to [Crowdin](#), we support Chinese, French, German, Russian, Japanese and Korean.

Casdoor uses the official Crowdin cli to sync translations from Crowdin. If you want to add more languages supports, please propose in [our community](#), and if you want to help us speed up the translating work, please help us translate on [Crowdin](#).



&gt;

Contributor guide

# Contributing to Casdoor

Welcome to Casdoor! This document is a guideline about how to contribute to Casdoor.

If you find something incorrect or missing, please leave comments / suggestions.

## Get involved

There are many ways to contribute to Casdoor. Here are some ideas to get started:

Use Casdoor and report issues! When using Casdoor, report issues to promote development of Casdoor, no matter bugs or proposal. Before filing an issue on GitHub, it would be better to discuss first on [Discord](#) or [GitHub Discussions](#)



When reporting an issue, please use English to describe the details of your problem.

Help with docs! Contributing start from docs is a good choice to start your contribution.

Help solve issues! We prepare a table containing easy tasks suitable for beginners, with different levels of challenges labeled with different tags, check the table here [Casdoor Easy Tasks](#).

# Contributing

Now, if you are ready to create PR, here is the workflow for contributors:

1. Fork to your own
2. Clone fork to a local repository
3. Create a new branch and work on it
4. Keep your branch in sync
5. Commit your changes (make sure your commit message is concise)
6. Push your commits to your forked repository
7. Create a pull request from your branch to our **master** branch.

# Pull Requests

## Before you get started

Casdoor uses GitHub as its developing platform. So the pull requests are the main source of contributions.

There are something you need to know before you open a pull request:

- When you first pull request, you need to sign the CLA.
- Explain why you send this PR and what this PR would do to the repo.

- One commit is allowed. Make sure the PR does only one thing, otherwise please split it.
- If there are newly added files, please include Casdoor license to the top of new file(s).

```
// 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.  
// You may obtain a copy of the License at  
//  
//     http://www.apache.org/licenses/LICENSE-2.0  
//  
// Unless required by applicable law or agreed to in writing,  
// software  
// distributed under the License is distributed on an "AS IS"  
// BASIS,  
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or  
// implied.  
// See the License for the specific language governing permissions  
// and  
// limitations under the License.
```

## Semantic PRs

Your pull requests should follow the Conventional Commits spec. The basic requirement is that only the PR title or at least one commit message. For example, three commonly used PR titles are given below:



The PR title must be in lower case.

1. fix: a commit of the type `fix` patches a bug in your codebase.

```
fix: prevent racing of requests
```

2. feat: a commit of the type `feat` introduces a new feature to the codebase.

```
feat: allow provided config object to extend other configs
```

3. docs: a commit of the type `docs` add or improve a document.

```
docs: correct spelling of CHANGELOG
```

For more details, please refer to [Conventional Commits](#).

## Link PR with issue (if existed)

You can link a pull request to an issue to show that a fix is in progress and to automatically close the issue when the pull request is merged.

### Linking a pull request to an issue using a keyword

You can link a pull request to an issue by using a supported keyword in the pull request's description or in a commit message. The pull request **must be** on the default branch.

- close
- fix
- resolve

Issue in the same repository, for example:

Fix: #902

For more details, please see [Link PR to issue](#).

## Modify PRs

Inevitably, your PR may need to be revised. Please re-use the same PR when the code needs changes. Don't close the PR and open a new one.

Here is a possible example:

- Modify the code in your local.
- Modify this commit.

```
git commit --amend
```

- Push to your remote repository.

```
git push --force
```

Then the PR has been modified successfully! You can check it in Casdoor repository.

## Code Related

Some principles:

Readability - Important code should be well-documented. Code style should be complied with the existing one.

## Naming convention

e.g., `signupUrl` for var names, `Signup URL` for UI

## How to update i18n data?

Please note that we use [Crowdin](#) as translating platform and i18next as translating tool. When you add some words using i18next in the `web/` directory, you can run the `i18n/generate_test.go` to auto-generate the `web/src/locales/**/data.json`.

Run `i18n/generate_test.go`:

```
cd i18n && go test
```

All languages are filled in English by default. You are encouraged to help translate the newly added strings in the `web/src/locales/zh/data.json` by [Crowdin](#) after your PR has been merged.

 CAUTION

If you are not familiar with other language, please don't translate it. Keep the file as it is.

## License

By contributing to Casdoor, you agree that your contributions will be licensed under its Apache License.