



# keycloak - Social Login ( Google, Kakao )

## ● 개요 ●

● 미리 구성해야 하는 요소

● 진행 과정

### ■ 1. keycloak realm&client 생성

■ realm 생성

■ client 생성

### ■ 2. identity provider 설정 - Client ID 및 secret 발급

■ identity provider?

■ Google 이용

■ 발급된 Client ID 와 Secret (예시)

■ Kakao 이용

■ 발급된 Client ID 와 Secret (예시)

### ■ 3. keycloak - social 연동

■ keycloak 설정

■ keycloak이 지원하는 IdP 이용 시 - Google

■ 사용자 지정 OpenID Connect v1.0 이용 시 - Kakao

■ TEST

## ● 개요 ●

social 로그인을 keycloak 에 적용시키기 위한 설정요소를 설명한다.

## ● 미리 구성해야 하는 요소

- keycloak: 22.0.1 설치
  - keycloak 도메인 : (예시) <https://sdevtest.genians.kr:30001>

## ● 진행 과정

1. keycloak realm 및 client 생성
2. identity provider Client ID 및 secret 발급
  - a. keycloak 이 지원하는 idP 확인
  - b. google, kakao Client ID 및 secret 발급
3. Keycloak - social login 연동 설정 및 테스트

## ■ 1. keycloak realm&client 생성

### ■ realm 생성

- create Realm

Master

Master ✓

Test

Create Realm

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Enabled

Action

l the options for users, applications, roles, and groups in the current

ThemesKeysEventsLocalizationSecurity defens

logo-text"><span>Keycloak</span></div>

ests

ent Configuration

ity Provider Metadata

revert

## Create realm

A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Resource file

Drag a file here or browse to upload

Browse...

Clear

1

Upload a JSON file

Realm name \*

minions

Enabled

☒ On

Create

Cancel



realm

- 각 realm은 독립적이며, 고유의 설정과 애플리케이션 및 사용자를 가짐
  - 예를 들어, 내부 애플리케이션 및 직원들을 위한 realm과 외부 애플리케이션 및 고객을 위한 realm을 설정할 수 있다.

## client 생성

- create client

# Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients listInitial access tokenClient registration

Create client

Import client

1 - 6

Client ID	Name	Type	Descripti...	Home URL
account	\$_client_...	OpenID Connect	–	<a href="https://sdevtest.genians.kr:30001/realms/minions/account/">https://sdevtest.genians.kr:30001/realms/minions/account/</a>
account-console	\$_client_...	OpenID Connect	–	<a href="https://sdevtest.genians.kr:30001/realms/minions/account/">https://sdevtest.genians.kr:30001/realms/minions/account/</a>
admin-cli	\$_client_...	OpenID Connect	–	–
broker	\$_client_...	OpenID Connect	–	–
realm-management	\$_client_...	OpenID Connect	–	–
security-admin-console	\$_client_...	OpenID Connect	–	<a href="https://sdevtest.genians.kr:30001/admin/minions/console/">https://sdevtest.genians.kr:30001/admin/minions/console/</a>

1 - 6

[Clients](#) > Create client

## Create client

Clients are applications and services that can request authentication of a user.

### 1 General Settings

Client type ?	OpenID Connect
Client ID * ?	kevin
Name ?	
Description ?	
Always display in UI ?	<input type="checkbox"/> Off

Next

Back









Cancel

Clients > Create client

## Create client

Clients are applications and services that can request authentication of a user.

### 2 Capability config

Client authentication 	<input checked="" type="checkbox"/> On
Authorization 	<input type="checkbox"/> Off
Authentication flow	<div><input checked="" type="checkbox"/> Standard flow <input type="checkbox"/> Implicit flow <input type="checkbox"/> OAuth 2.0 Device Authorization Grant </div> <div><input checked="" type="checkbox"/> Direct access grants <input type="checkbox"/> Service accounts roles <input type="checkbox"/> OIDC CIBA Grant </div>

[Next](#) [Back](#) [Cancel](#)

- client authentication을 활성화 한다.
- Authentication flow는 디폴트 값으로 진행한다.
  - Standard flow를 이용하여, OIDC Authorization Code Flow를 사용할 예정임.

Clients > Create client

## Create client

Clients are applications and services that can request authentication of a user.

3
Login settings

Root URL ⓘ

Home URL ⓘ

Valid redirect URIs ⓘ

+ Add valid redirect URIs

Valid post logout redirect URIs ⓘ

+ Add valid post logout redirect URIs

Web origins ⓘ

+ Add web origins

Save Back Cancel

- Root URL
  - 루트 URL이 상대 URL에 추가
  - (예시) <https://sdevtest.genians.kr:30003>
- Home URL
  - 인증 서버가 클라이언트로 리디렉션 또는 다시 연결해야 할 때 사용할 기본 URL.
  - (예시) <http://sdevtest.genians.kr:30003/loginButton.html>
- Valid redirect URIs
  - 성공적으로 로그인한 후 브라우저가 리디렉션할 수 있는 유효한 URI 패턴.
  - 클라이언트 사이드 애플리케이션이 OpenID Connect를 사용하는 경우 OpenID Connect 인가 코드 흐름에서 매우 중요한 값이다. 클라이언트 사이드 애플리케이션은 애플리케이션의 사용자에게 자격증명을 노출할 수 있기 때문에 어떠한 자격증명도 가질 수 없다. 악의적인 애플리케이션이 실제 애플리케이션으로 속이는 행위를 방지하기 위해 valid redirect URIs에 설정된 URL로 사용자를 리다이렉트하도록 keycloak에게 알려준다.
  - SAML의 경우 로그인 요청에 포함된 소비자 서비스 URL에 의존하는 경우 유효한 URI 패턴을 설정해야 합니다.
  - (예시) <http://sdevtest.genians.kr:30003/loginOk.html>
    - 'http://example.com/\*' 과 같은 간단한 와일드카드 사용이 가능

- 상대 경로도 /my/relative/path/\*와 같이 지정 가능
- Valid post logout redirect URIs
  - 로그아웃이 성공한 후 브라우저가 리디렉션할 수 있는 유효한 URI 패턴.
  - (예시) <http://sdevtest.genians.kr:30003/logoutOk.html>
- Web origins
  - (예시) 미설정
    - 모든 원점을 허용하려면 '\*'를 명시적으로 추가합니다.
  - 애플리케이션의 CORS(Cross-Origin Resource Sharing)요청에 대한 유효한 웹 출처를 등록한다. keycloak으로부터 토큰을 발급받으려면 프론트엔드 애플리케이션은 Keycloak에게 AJAX요청을 전송해야하며, CORS가 설정돼 있지 않은 경우 브라우저는 서로 다른 웹 출처의 AJAX 요청을 허용하지 않는다.



주의!

상대 경로도 사용가능

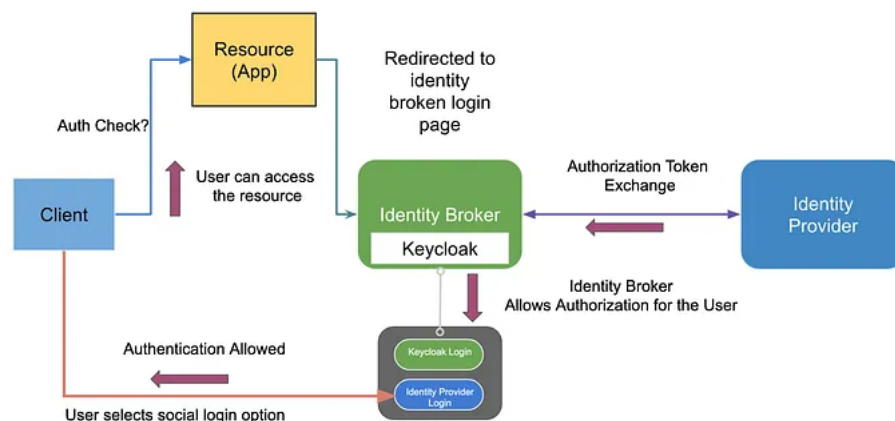
상대경로는 클라이언트 루트 URL에 상대적인 경로이거나, 지정된 경로가 없는 경우 인증 서버 루트 URL이 사용됩니다.

## 2. identity provider 설정 - Client ID 및 secret 발급

### identity provider?

- 사용자가 keycloak에 인증 할 수 있도록 하는 소셜 네트워크나 ID 브로커
  - IDentity Provide 지원 리스트
    - BitBucket, Facebook, GitHub, GitLab, Google, Instagram, LinkedIn, Microsoft, Open Shift v3, Open Shift v4, PayPal, Stack Overflow, Twitter
  - 그 외, 사용자 지정 지원도 가능하다.
    - keycloak OpenID Connect, OpenID Connect v1.0, SAML 이용

### Identity Flow



- 사용자가 리소스(응용프로그램)에 액세스하려고 합니다



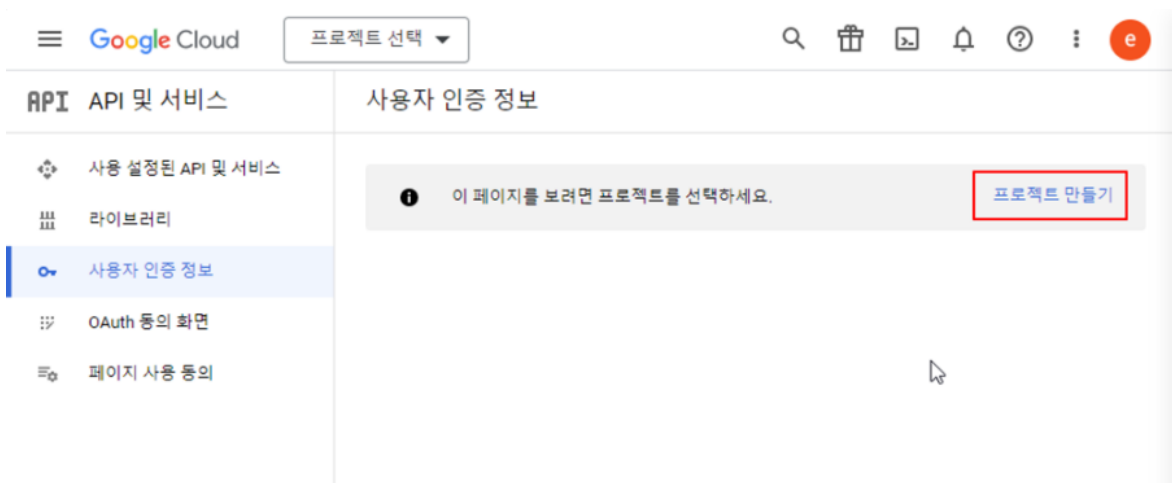
- 인증되지 않으면 ID 브로커, 즉 Keycloak 로그인 페이지로 리디렉션됩니다.
- 사용자는 키cloak 로그인을 이용하여 인증을 받거나 소셜로그인 버튼, 페이스북 로그인을 이용할 수 있습니다.
- ID 브로커는 사용자에게 권한 승인을 요청하는 ID 제공자의 권한 토큰을 교환합니다.
- 사용자가 승인을 제공하면 ID 브로커가 사용자에게 대한 인증 세션을 만듭니다.
- 이제 사용자는 요청한 리소스에 액세스할 수 있습니다.

## Google 이용

- 개발자 홈페이지 접속

<https://console.cloud.google.com/apis/credentials>

- 로그인 후 프로젝트 만들기 선택



- 프로젝트 이름 및 조직 설정

Google Cloud

새 프로젝트

projects 할당량이 7개 남았습니다. 할당량 증가를 요청하거나 프로젝트를 삭제하세요. [자세히 알아보기](#)

[MANAGE QUOTAS](#)

프로젝트 이름 \*

minions-keycloak

프로젝트 ID: minions-keycloak입니다. 나중에 변경할 수 없습니다. [수정](#)

위치 \*

조직 없음

찾아보기

상위 조직 또는 폴더

만들기

취소

- 프로젝트 이름 : 자유롭게 작성
    - (예시) minions-keycloak
  - 프로젝트 이름 작성 후 프로젝트 ID 생성됨.
    - 프로젝트 이름과 동일하지 않을 수 있음.
    - (예시) 생성된 프로젝트 ID : minions-keycloak
  - 위치 : 내 계정 google cloud 구성에 따라 자율 선택
- 클라이언트 ID를 만들기 전에 OAuth 동의 화면 구성 우선 처리 필요

Google Cloud

minions-keycloak

e

API

API 및 서비스

← OAuth 클라이언트 ID 만들기

사용 설정된 API 및 서비스

라이브러리

사용자 인증 정보

OAuth 동의 화면

페이지 사용 동의

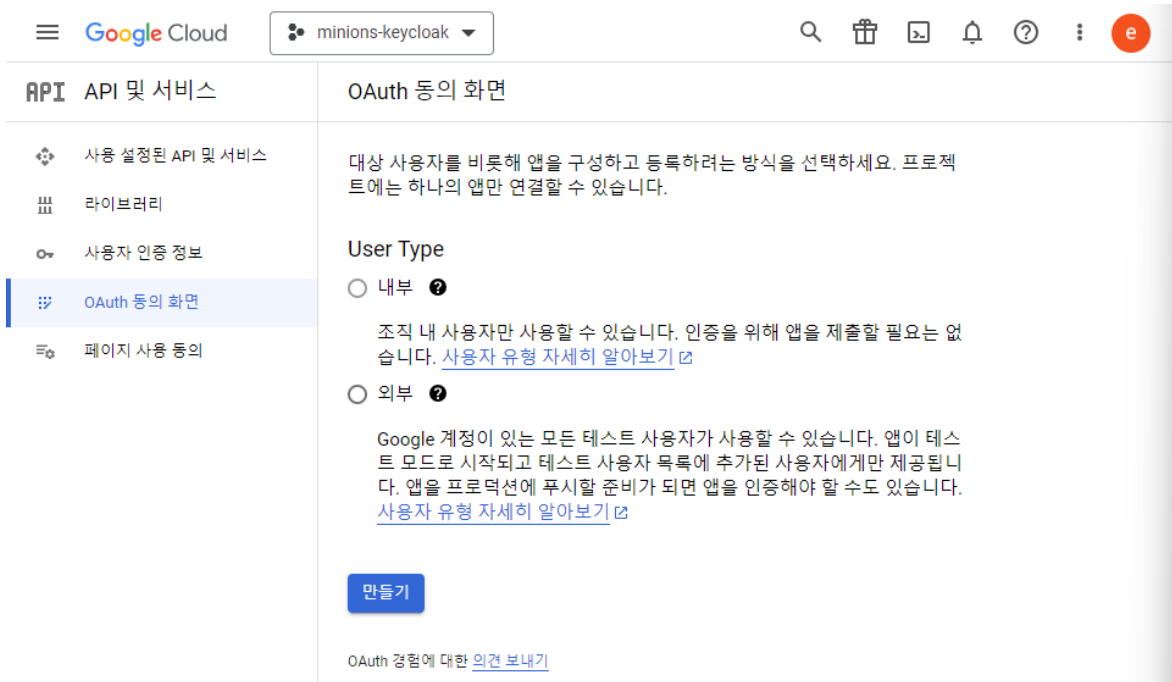
클라이언트 ID는 Google OAuth 서버에서 단일 앱을 식별하는 데 사용됩니다. 앱이 여러 플랫폼에서 실행되는 경우 각각 자체 클라이언트 ID가 있어야 합니다. 자세한 내용은 [OAuth 2.0 설정](#)을 참조하세요. OAuth 클라이언트 유형을 [자세히 알아보세요](#).

OAuth 클라이언트 ID를 만들려면 먼저 동의 화면을 구성해야 합니다.

동의 화면 구성

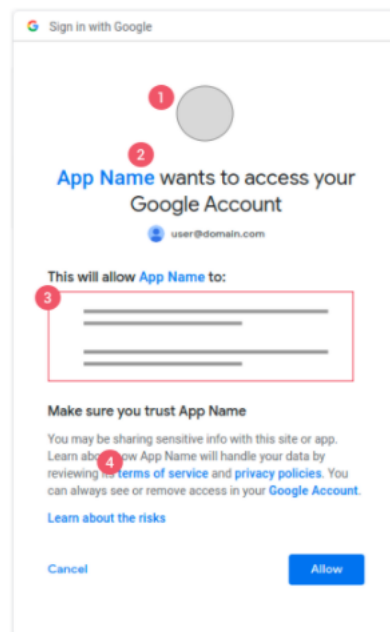
keycloak - Social Login ( Google, Kakao )

10



- User Type: 외부 선택
  - 내부: 앱 사용이 조직 내 Google Workspace 사용자로 제한
  - 외부: Google 계정이 있는 모든 테스트 사용자가 사용

## • 동의 화면 구성





- 도메인 앞에 http 또는 https 는 입력하지 않음.
  - 개발자 연락처 정보
    - Google에서 프로젝트 변경사항에 대해 알림을 보내기 위한 용도
  - 선택 작성 요소
    - 로고
    - 홈페이지 및 개인정보처리방침 및 서비스 약관 링크
      - 동의 화면에서 홈페이지, 약관 및 개인정보처리방침으로 이동 가능
  - 관련 사이트
    - <https://developers.google.com/identity/protocols/oauth2/production-readiness/brand-verification?hl=ko#authorized-domains>
- 사용자 데이터 액세스 권한 승인 요청 범위 설정 (필수 아님)

The screenshot shows the Google Cloud console interface for the 'minions-keycloak' project. The left sidebar contains the 'API 및 서비스' (APIs and Services) section, with 'OAuth 동의 화면' (OAuth consent screen) selected. The main content area displays the '앱 등록 수정' (Edit app registration) page, specifically the '범위' (Scopes) tab. The '범위' tab is highlighted with a blue circle and a checkmark. Below the tab, a description states: '범위는 사용자에게 앱 승인을 요청하는 권한을 나타내며 프로젝트에서 사용자의 Google 계정에 있는 특정 유형의 비공개 사용자 데이터에 액세스하도록 허용합니다. [자세히 알아보기](#)'. A red box highlights the '범위 추가 또는 삭제' (Add or remove scopes) button. Below this, there are three sections: '민감하지 않은 범위' (Unselected scopes), '민감한 범위' (Sensitive scopes), and '제한된 범위' (Restricted scopes). Each section has a table with columns 'API', '범위', and '사용자에게 표시되는 설명'. All three sections show '표시할 행이 없습니다.' (No rows to display). At the bottom, there are two buttons: '저장 후 계속' (Save and continue) and '취소' (Cancel).

## ✕ 선택한 범위 업데이트



아래에는 사용 설정된 API의 범위만 나와 있습니다. 이 화면에 누락된 범위를 추가하려면 [Google API 라이브러리](#)에서 API를 찾아 사용 설정하거나 아래의 '붙여넣은 범위' 텍스트 상자를 사용하세요. 라이브러리에서 사용 설정한 새 API를 확인하려면 페이지를 새로고침하세요.

≡ 필터 속성 이름 또는 값 입력



<input type="checkbox"/>	API ↓	범위	사용자에게 표시되는 설명
<input checked="" type="checkbox"/>	Service Management API	.../auth/service.management	Google API 서비스 구성을 관리합니다.
<input checked="" type="checkbox"/>	Service Management API	.../auth/service.management.readonly	Google API 서비스 구성 확인
<input checked="" type="checkbox"/>	Service Management API	.../auth/iam.test	ID 및 액세스 관리(IAM) 권한 테스트
<input type="checkbox"/>	Cloud Trace API	.../auth/trace.readonly	프로젝트 또는 애플리케이션용 Trace 데이터 읽기
<input type="checkbox"/>	Cloud Trace API	.../auth/trace.append	프로젝트 또는 애플리케이션용 Trace 데이터 쓰기
<input type="checkbox"/>	Cloud Storage API	.../auth/devstorage.write_only	Google 클라우드 저장소에서 데이터 관리
<input type="checkbox"/>	Cloud Monitoring API	.../auth/monitoring	Google과 타사의 모든 클라우드 및 API 프로젝트 관련 모니터링 데이터 보기 및 작성하기
<input type="checkbox"/>	Cloud Monitoring API	.../auth/monitoring.read	모든 Google 클라우드 및 타사 프로젝트의 모니터링 데이터 보기
<input type="checkbox"/>	Cloud Monitoring API	.../auth/monitoring.write	통계 데이터를 Google 클라우드 프로젝트에 게시
<input type="checkbox"/>	Cloud Logging API	.../auth/logging.read	프로젝트의 로그 데이터 보기

페이지당 행 수: 10 ▼ 1 - 10 (전체 24행) < >

### 직접 범위 추가

추가할 범위가 위 표에 표시되지 않으면 여기에 입력할 수 있습니다. 각 범위를 새 줄에 입력하거나 쉼표로 구분해야 합니다. 'https://'로 시작하는 전체 범위 문자열을 입력하세요. 완료되면 '표에 추가'를 클릭하세요.

### 필요한 권한 선택



관련 사이트

- <https://developers.google.com/identity/protocols/oauth2/scopes?hl=ko>



#### 직접범위추가(선택)

- 사용자 권한 범위는 OIDC 요청 중의 "scope" 매개변수를 통해 지정됩니다. 일반적으로 다음과 같은 범위 값 중 하나 또는 여러 개를 지정할 수 있습니다:
1. **openid** : 필수 요소로서, 사용자의 ID Token을 가져올 수 있게 해줍니다.
  2. **profile** : 사용자의 프로필 정보를 가져오는 권한을 나타냅니다. 이름, 프로필 사진 등의 정보를 요청할 수 있습니다.
  3. **email** : 사용자의 이메일 주소에 대한 접근 권한을 나타냅니다.
  4. **offline\_access** : 사용자의 리프레시 토큰을 받을 수 있는 권한을 부여하여, 장기적인 세션 유지를 지원할 수 있습니다.
  5. 사용자 지정 범위: 애플리케이션에서 필요한 특정 범위를 정의할 수도 있습니다. 이를 통해 애플리케이션에 필요한 사용자 데이터에만 액세스할 수 있습니다.
- 예를 들어, 다음은 OIDC 요청에서 여러 사용자 권한 범위를 지정하는 방법입니다

(예시) `https://accounts.google.com/o/oauth2/auth  
?response_type=code  
&client_id=your-client-id  
&redirect_uri=your-redirect-uri  
&scope=openid profile email  
&state=your-state  
&nonce=your-nonce`





- OAuth 동의 화면 — 범위 — 3 테스트 사용자 — 4 요약

게시 상태가 '테스트 중'으로 설정된 동안에는 테스트 사용자만 앱에 액세스할 수 있습니다. 앱 인증 전에 허용되는 사용자 한도는 100명이며 앱의 전체 수명 주기에서 계산됩니다. [자세히 알아보기](#)

[+ ADD USERS](#)

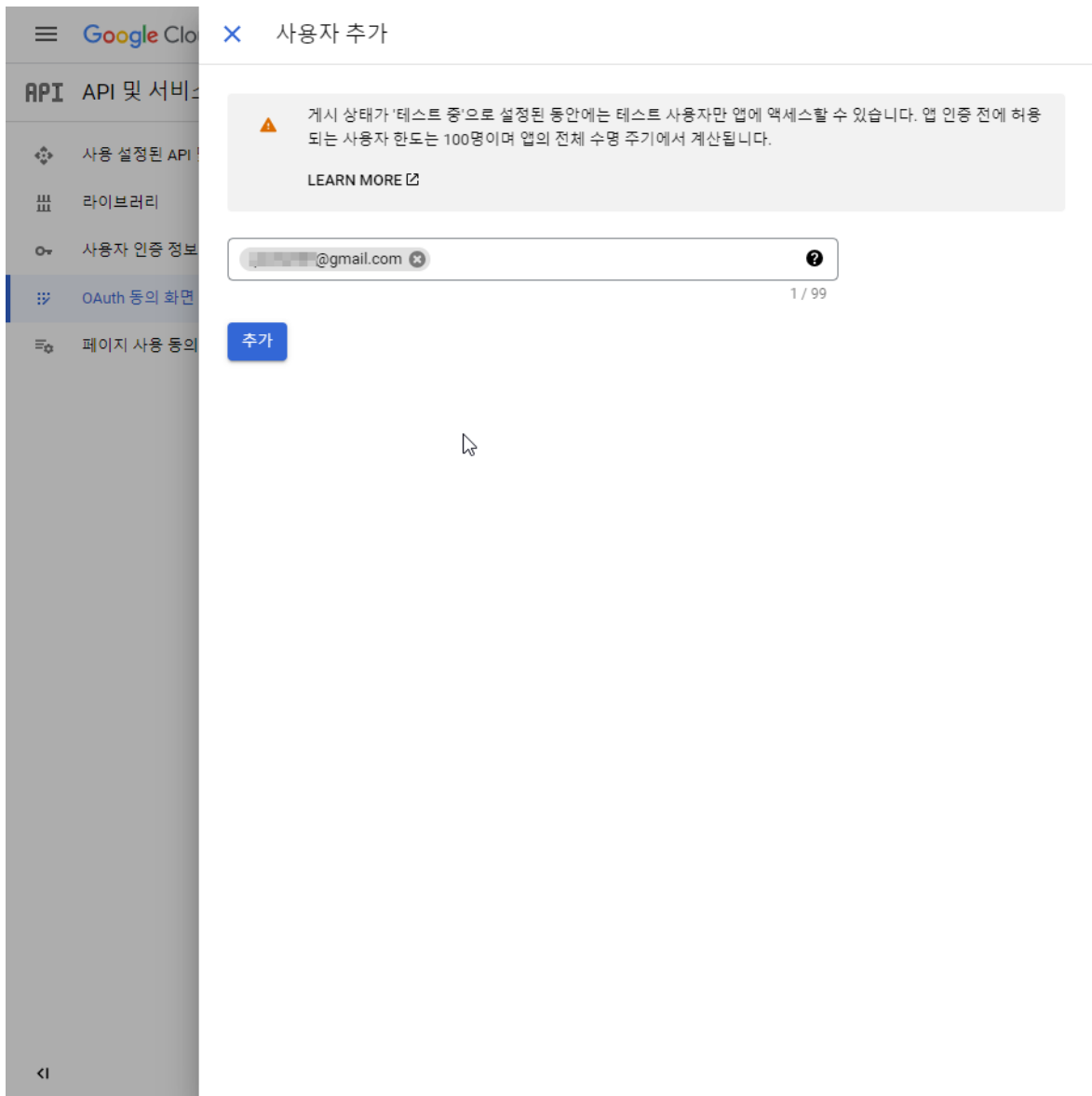
≡ 필터 속성 이름 또는 값 입력

사용자 정보

표시할 행이 없습니다.

[저장 후 계속](#)

취소



- 계시 상태가 '테스트 중'으로 설정된 동안에는 테스트 사용자만 앱에 액세스할 수 있다
- 이메일 주소는 활성 상태인 Google 계정, Google Workspace 계정 또는 Cloud ID 계정과 연결되어 있어야 한다.



Google Cloud minions-keycloak

API API 및 서비스 사용자 인증 ... **+ 사용자 인증 정보 만들기** 삭제

사용 설정된 API 라이브러리 사용자 인증 정보 OAuth 동의 화면 페이지 사용 등

API 키  
활당량과 액세스 권한을 확인하기 위해 간단한 API 키로 프로젝트를 확인합니다.

OAuth 클라이언트 ID  
앱에서 사용자 데이터에 액세스할 수 있도록 사용자 동의를 요청합니다.

서비스 계정  
로봇 계정을 사용하여 서버 간의 앱 수준 인증을 사용 설정합니다.

사용자 인증 정보 선택 도움말  
사용할 사용자 인증 정보의 유형을 결정할 수 있도록 몇 가지 질문을 합니다.

자세히 알아보기

동의를 구성해야 합니다. **동의 화면 구성**

제한사항 작업

OAuth 2.0 클라이언트 ID

<input type="checkbox"/>	이름	생성일 ↓	유형	클라이언트 ID	작업
표시할 OAuth 클라이언트가 없습니다.					

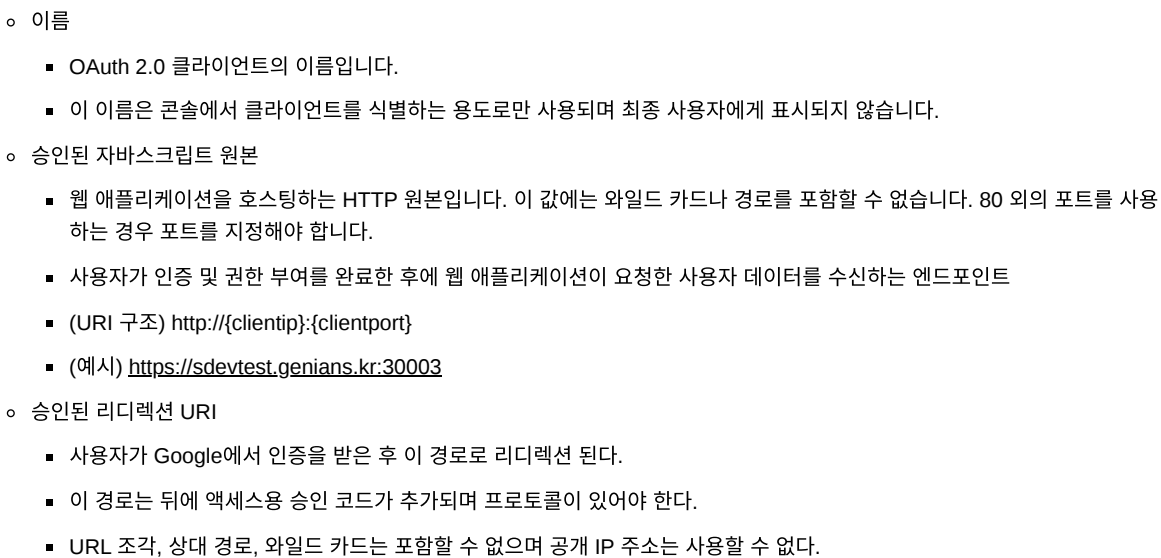
서비스 계정 [서비스 계정 관리](#)

<input type="checkbox"/>	이메일	이름 ↑	작업
표시할 서비스 계정이 없습니다.			

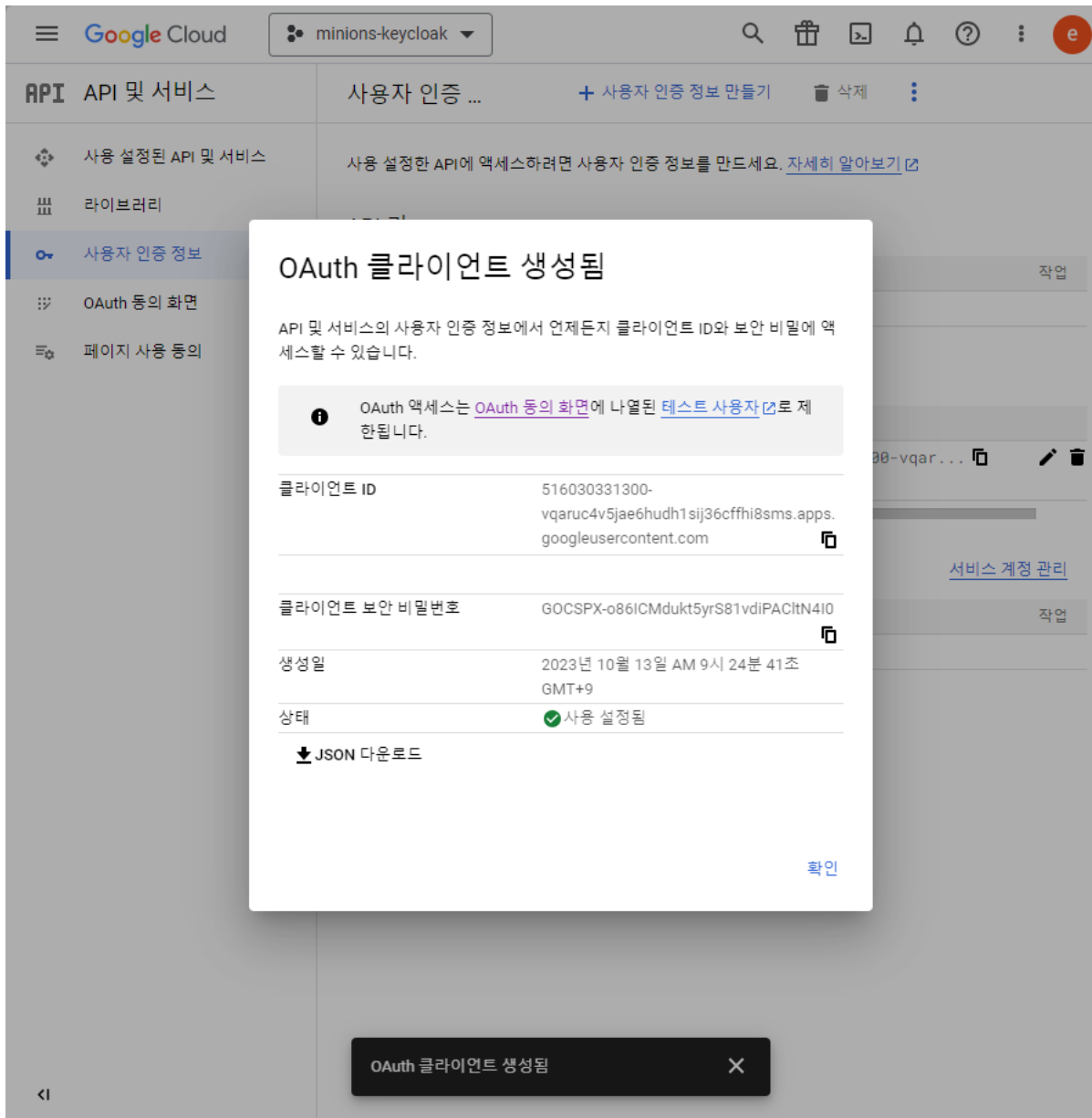
◦ OAuth클라이언트 ID 선택

- 애플리케이션 유형 선택





- (URI 구조) `https://{keycloakip}:{keycloakport}/realms/{realm_name}/broker/google/endpoint`
- (예시) `https://sdevtest.genians.kr:30001/realms/minions/broker/google/endpoint`



### ■ 발급된 Client ID 와 Secret (예시)

- Client ID: `516030331300-vqaruc4v5jae6hudh1sij36cffi8sms.apps.googleusercontent.com`
- Secret: `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`
- json
  - `client_secret_516030331300-vqaruc4v5jae6hudh1sij36cffi8sms.apps.googleusercontent.com.json`
  - `{"web":{"client_id":"516030331300-vqaruc4v5jae6hudh1sij36cffi8sms.apps.googleusercontent.com","project_id":"minions-keycloak","auth_uri":"https://accounts.google.com/o/oauth2/auth","token_uri":"https://oauth2.googleapis.com/token","aut`


```
o86lCMdukt5yrS81vdiPACltN4lQ","redirect_uris":  
["https://sdevtest.genians.kr:30001/realms/minions/broker/google/endpoint"],"javascript_origins":  
["https://sdevtest.genians.kr:30003"]}]]}
```

## Kakao 이용

- 개발자 홈페이지 접속

Kakao Developers

카카오 API를 활용하여 다양한 어플리케이션을 개발해보세요. 카카오 로그인, 메시지 보내기, 친구 API, 인공지능 API 등을 제공합니다.

 <https://developers.kakao.com/>

kakao developers

- 로그인 후 카카오 로그인 제품소개로 이동

kakao developers

내 애플리케이션   제품   문서   도구   포럼   kho

추천 제품

### 카카오싱크

시작하기

카카오싱크는 가입에서 약관 동의, (마케팅 메시지 발송을 위한) 카카오톡 채널 추가까지 이 모든 과정을 한번에 할 수 있는 간편가입 기능입니다. 카카오싱크를 통해 복잡한 가입 절차 없이 손쉽게 회원을 만들어보세요.

제품소개   문서보기

### 카카오 로그인

Login

카카오계정 하나로 간편하게 여러분의 서비스에 로그인 할 수 있도록 하는 서비스입니다. 누구나 가지고 있는 카카오 계정으로 빠르고 안전하게 고객을 만들어 보세요.

제품소개   문서보기

### 카카오톡 소셜

카카오톡 친구들의 닉네임, 사진 정보를 활용할 수 있습니다. 고객에게 개인화된 서비스를 제공하세요.

제품소개   문서보기

### 지도/로컬

언제나 최신 정보를 제공하는 카카오맵의 API를 통해 지도, 위치, 장소와 관련된 정보를 다양한 위치 기반 서비스에 활용해 보세요.

제품소개   문서보기

### 카카오톡 채널

Ch

카카오톡 채널을 운영한다면 서비스에 채널 추가 버튼과 1:1 채팅 버튼을 추가해보세요. 고객파일 관리 API를 통해 고객 정보를 쉽고 빠르게 업로드하여 타겟메시지를 발송할 수 있습니다.


제품소개   문서보기

### 검색

A

다음과 카카오의 방대한 검색 결과를 여러분의 서비스에서 바로 보여줄 수 있습니다. 웹, 동영상, 카페, 이미지, 블로그, 팁, 책 등 다양한 검색 정보로 여러분의 콘텐츠를 강화해보세요.

제품소개   문서보기



<https://developers.kakao.com/product/kakaoLogin>



kakao developers
내 애플리케이션
제품
문서
더 보기
khoko@kakao.com
KOR ENG

제품 > 카카오 로그인

## 제공 기능

- 로그인: 카카오계정을 통한 빠르고 간편한 사용자 로그인 기능입니다.
- 로그아웃: 사용자 토큰을 만료시켜 로그인 상태를 해제합니다.
- 연결 끊기: 카카오 플랫폼에서 사용자와 앱의 연결을 해제합니다.
- 토큰 정보 보기: 액세스 토큰(Access token)의 정보와 토큰의 유효기간을 제공합니다.
- 사용자 정보 가져오기: 사용자 카카오계정에 등록된 정보를 제공합니다.
- 사용자 정보 저장하기: 사용자 카카오계정에 사용자 정의(Custom)한 서비스 데이터를 저장합니다.
- 동의 내역 확인하기: 서비스에서 현재 사용 중이거나 사용자가 동의한 동의 항목을 확인합니다.
- 동의 철회하기: 불필요한 동의 항목에 대해 사용자 동의를 철회합니다.

## API 사용하기

카카오 오픈 API로 서비스의 가치를 높여보세요.

시작하기

문서보기

↑

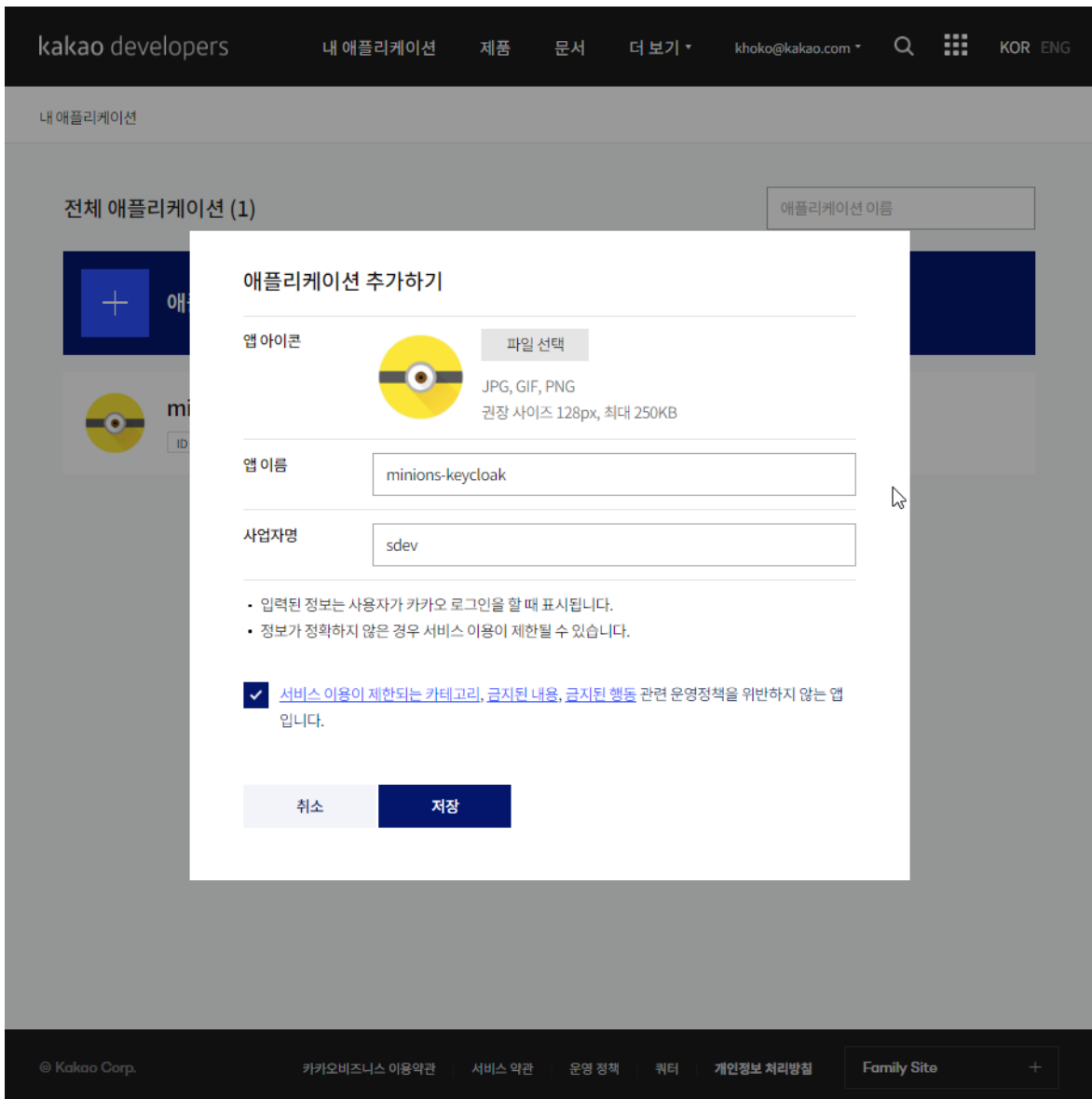
<https://developers.kakao.com/console>

◦ API 사용하기 > 시작하기 클릭

#### • 애플리케이션 추가하기

keycloak - Social Login ( Google, Kakao )

25



- 앱 이름과 사업자명 설정
  - 카카오 로그인 시 표기되므로 신중히 설정

- 앱 설정 확인



kakao developers

내 애플리케이션

제품

문서

더 보기 ▾


khoko@kakao.com ▾

Q

KOR ENG

☰

내 애플리케이션 > 제품 설정 > 카카오 로그인 > 보안



minions-keycloak

ID 980378 OWNER

카카오 로그인 OFF

Client Secret

토큰 발급 시, 보안을 강화하기 위해 Client Secret을 사용할 수 있습니다. (REST API인 경우에 해당)

코드 생성

© Kakao Corp.

카카오비즈니스 이용약관

서비스 약관

운영 정책


취터

개인정보 처리방침

Family Site +

kakao developers
내 애플리케이션
제품
문서
더 보기
khoko@kakao.com
KOR ENG

내 애플리케이션 > 제품 설정 > 카카오 로그인 > 보안


minions-keycloak
ID 980378 OWNER

카카오 로그인 OFF

Client Secret 삭제

토큰 발급 시, 보안을 강화하기 위해 Client Secret을 사용할 수 있습니다. (REST API인 경우에 해당)

코드	mvBcJX1WQYYmPxEUlJlqEYVNMgZ8f1kK	재발급
활성화 상태	사용함	설정

© Kakao Corp.
카카오비즈니스 이용약관
서비스 약관
운영 정책
취터
개인정보 처리방침
Family Site

- 코드 생성으로 Client Secret 을 발급받고 활성화 상태를 사용함으로 설정함.

#### • 카카오 로그인 활성화 및 Redirect URI 지정

kakao developers
내 애플리케이션
제품
문서
더 보기
khoko@kakao.com
KOR ENG

내 애플리케이션 > 제품 설정 > 카카오 로그인

minions-keycloak
ID 980378
OWNER

카카오 로그인 ON

동의 화면 미리보기

활성화 설정

상태 ON

카카오 로그인 API를 활용하면 사용자들이 번거로운 회원 가입 절차 대신, 카카오톡으로 서비스를 시작할 수 있습니다.

상태가 OFF일 때도 카카오 로그인 설정 항목을 변경하고 서버에 저장할 수 있습니다.

상태가 ON일 때만 실제 서비스에서 카카오 로그인 화면이 연결됩니다.

OpenID Connect 활성화 설정

상태 ON

카카오 로그인의 확장 기능인 OpenID Connect를 활성화합니다.

이 설정을 활성화하면 카카오 로그인 시 사용자 인증 정보가 담긴 ID 토큰을 액세스 토큰과 함께 발급받을 수 있습니다.

Redirect URI

삭제 수정

Redirect URI

https://sdevtest.genians.kr:30001/realms/minions/broker/kakao/endpoint

- 카카오 로그인에서 사용할 OAuth Redirect URI를 설정합니다. (최대 10개)
- REST API로 개발하는 경우 필수로 설정해야 합니다.

© Kakao Corp.
카카오비즈니스 이용약관
서비스 약관
운영 정책
쿼터
개인정보 처리방침
Family Site
+

- 카카오 로그인 활성화 설정
  - On
- OpenID Connect 활성화 설정
  - On
- Redirect URI
  - <https://sdevtest.genians.kr:30001/realms/minions/broker/kakao/endpoint>

자세한 설명은 아래의 내용을 참조

- <https://developers.kakao.com/docs/latest/ko/kakaologin/prerequisite#redirect-uri>

## 발급된 Client ID 와 Secret (예시)

- Client ID(REST API 키): 78cada2256b055fc73b787e7ebc5c6d5

keycloak - Social Login ( Google, Kakao )

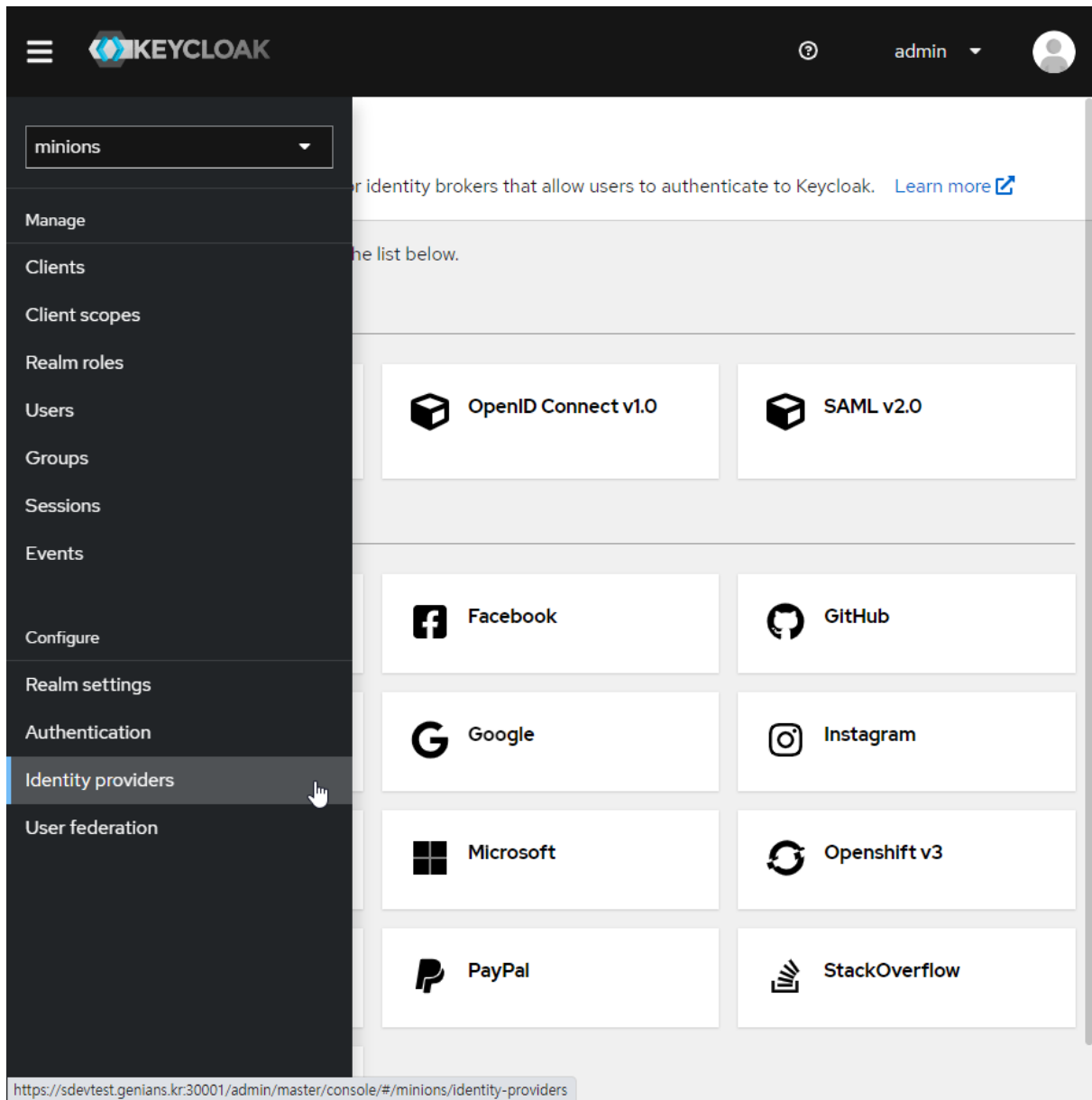
30

- Secret: mvBcJX1WQYYmPxEUJIqEVYNMgZ8f1kK

### 3. keycloak - social 연동

적용하고자 하는 realm에 다음과 같이 발급받은 Client ID 와 secret을 설정한다.

#### keycloak 설정



#### keycloak이 지원하는 IdP 이용 시 - Google

## Identity providers

Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. [Learn more](#)

To get started, select a provider from the list below.

### User-defined:



Keycloak OpenID Connect



OpenID Connect v1.0



SAML v2.0

### Social:



BitBucket



Facebook



GitHub



GitLab



Google



Instagram



LinkedIn



Microsoft



OpenShift v3



OpenShift v4



PayPal



StackOverflow





Twitter



Identity providers > Add provider

## Add Google provider

Redirect URI ?	<input type="text" value="https://sdevtest.genians.kr:30001/realms/minions/broker/google/endpoint"/>	
Client ID * ?	<input type="text" value="516030331300-vqaruc4v5jae6hudh1sij36cffhi8sms.apps.googleusercontent.com"/>	
Client Secret * ?	<input type="password" value="....."/>	
Display order ?	<input type="text"/>	
Hosted Domain ?	<input type="text"/>	
Use userIp param ?	<input type="checkbox"/> Off	
Request refresh token ?	<input type="checkbox"/> Off	

- Client ID: 516030331300-vqaruc4v5jae6hudh1sij36cffhi8sms.apps.googleusercontent.com
- Secret: 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


### 사용자 지정 OpenID Connect v1.0 이용 시 - Kakao


## Identity providers


Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. [Learn more](#)

To get started, select a provider from the list below.


### User-defined:


 Keycloak OpenID Connect


 OpenID Connect v1.0


 SAML v2.0


### Social:


 BitBucket


 Facebook


 GitHub


 GitLab


 Google


 Instagram


 LinkedIn


 Microsoft

 OpenShift v3

 OpenShift v4

 PayPal

 StackOverflow

 Twitter

KEYCLOAK
admin

Identity providers > Add OpenID Connect provider

## Add OpenID Connect provider

Redirect URI ⓘ

https://sdevtest.genians.kr:30001/realms/minions/broker/oidc/endpoint

Alias \* ⓘ

kakao

Display name ⓘ

Display order ⓘ

### OpenID Connect settings

Use discovery endpoint ⓘ

☒ On

Discovery endpoint \* ⓘ

https://kauth.kakao.com/.well-known/openid-configuration

Show metadata

Client authentication ⓘ

Client secret sent as post

Client ID \* ⓘ

78cada2256b055fc73b787e7ebc5c6d5

Client Secret \* ⓘ

.....

Client assertion signature algorithm ⓘ

Algorithm not specified

Add

Cancel



### 주의!

keycloak 설정에서 alias를 kakao 적용하면 Redirect URI 가 <https://sdevtest.genians.kr:30001/realms/minions/broker/kakao/endpoint>로 변경됨.  
그렇기에 kakao client id 발급받을 때 Redirect uri를 위처럼 설정해줌

- Discovery endpoint
  - <https://kauth.kakao.com/.well-known/openid-configuration>
  - Discovery endpoint는 OIDC 프로바이더가 제공하는 메타데이터를 조회할 수 있는 URL입니다. 메타데이터란 OIDC 프로바이더가 어떤 기능을 지원하고, 어떤 엔드포인트를 사용하고, 어떤 스코프와 클레임을 제공하고, 어떤 공개키를 사용하는지 등의 정보를 말합니다. Discovery endpoint를 통해 이러한 정보를 JSON 형식으로 받아볼 수 있습니다.
- Client ID 와 Client Secret 작성
  - Client ID(REST API 키): 78cada2256b055fc73b787e7ebc5c6d5
  - Secret: mvBcJX1WQYYmPxEUlJlqEVYNMgZ8f1kK

## ■ TEST

- authorization\_endpoint(인증을 받는 URL)를 이용
- url
  - URL 구조
    - `http://{keycloakip}:{keycloakport}/realms/{realm_name}/protocol/openid-connect/auth?response_type={response_type}&client_id={clientid}&state={randomvalue}`
    - (예시) [https://sdevtest.genians.kr:30001/realms/minions/protocol/openid-connect/auth?response\\_type=code&client\\_id=kevin&state=12345](https://sdevtest.genians.kr:30001/realms/minions/protocol/openid-connect/auth?response_type=code&client_id=kevin&state=12345)
  - response\_type: 인증에 성공했을 때, 어떤 값을 응답값으로 받을 것인가
    - (설정) code로 고정 사용
    - 값이 code이면 기본 승인 코드 흐름을 실행하여 토큰을 가져오려면 POST를 토큰 엔드포인트로 요구. 값이 token id\_token 또는 id\_token token이면 암시적 흐름을 실행하여 리디렉션 URI에서 자바스크립트를 사용하여 URI #fragment 식별자로 반환.
  - client\_id: 인증절차를 거칠 Realm에 생성된 클라이언트의 id
  - redirect\_uri: 인증에 성공 한 후, redirect될 url
    - 관리자 콘솔에서 미리 정의된 redirect\_uri만 사용 가능
  - scope: 인증을 통해서 조회할 데이터의 범위를 설정
  - state(선택): 동일한 값을 유지하는 임의의 문자열(정해진 형식 없음) Cross-Site Request Forgery(CSRF) 공격으로부터 카카오 로그인 요청을 보호하기 위해 사용

# MINIONS

Sign in to your account

Username or email

Password

Sign In

Or sign in with



Google

kakao

 Google 계정으로 로그인

## 로그인

[genians.kr](#)(으)로 이동

[이메일을 잊으셨나요?](#)

계속 진행하기 위해 Google에서 내 이름, 이메일 주소, 언어 환경설정, 프로필 사진을 [genians.kr](#)과(와) 공유합니다. 앱을 사용하기 전에 [genians.kr](#)의 [개인정보처리방침](#) 및 [서비스 약관](#)을 검토하세요.

[계정 만들기](#)

[다음](#)

한국어



[도움말](#)

[개인정보처리방침](#)

[약관](#)

Google 계정으로 로그인

@gmail.com

비밀번호 입력

.....

☐ 비밀번호 표시

계속 진행하기 위해 Google에서 내 이름, 이메일 주소, 언어 환경설정, 프로필 사진을 geniains.kr과(와) 공유합니다. 앱을 사용하기 전에 geniains.kr의 [개인정보처리방침](#) 및 [서비스 약관](#)을 검토하세요.

비밀번호 찾기

다음

한국어

▼

도움말

개인정보처리방침

약관

kakao



**minions-keycloak**

sdev

@kakao.com

[계정 변경](#)

해당 카카오텔정을 minions-keycloak 서비스에 연결합니다. 서비스 연결 시 회원 식별을 위한 회원번호가 제공됩니다.

확인하고 계속하기

Copyright © Kakao Corp. All rights reserved.



MINIONS

### Update Account Information

Username  
3095534185

Email  
[masked]@kakao.com

First name  
fn

Last name  
ln

Submit

그 외

- kakao 약관 설정
- 사용자 정보 이용 권한 설정
  - mapper 이용
- OIDC 활성화 유무
- 카카오 설명 더 자세히
- 내계정 블러처리