



**SANGFOR**



# **IAM**

## **Otentikasi Akun Media Sosial**

**Versi 12.0.25**



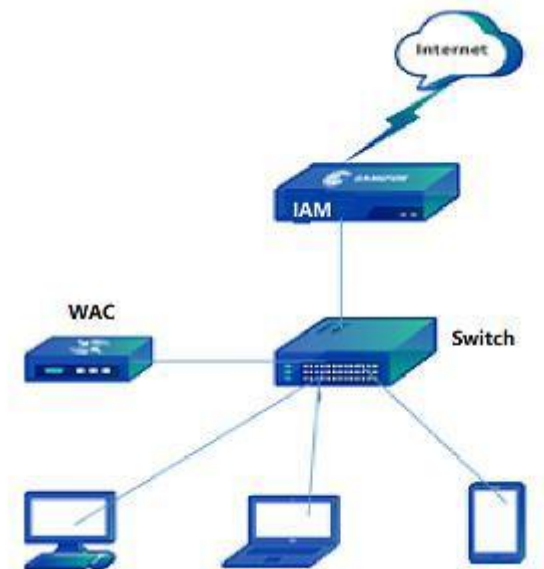
## Perubahan Catatan

Tanggal	Deskripsi Perubahan
22 Juli 2019	Rilis dokumen versi 12.0.25.

# Daftar Isi

1 Contoh Topologi.....	1
2 Panduan Konfigurasi.....	1
2.1 Konfigurasi Dasar.....	1
2.2 Otentikasi Facebook.....	1
2.2.1 Platform Pengembang.....	1
2.2.2 Konfigurasi Otentikasi IAM.....	3
2.2.3 Proses Otentikasi.....	4
2.3 Otentikasi Gmail.....	5
2.3.1 Platform Pengembang.....	5
2.3.2 Konfigurasi Otentikasi IAM.....	7
2.3.3 Proses Otentikasi.....	8
2.4 Otentikasi Line.....	9
2.4.1 Platform Pengembang.....	9
2.4.2 Konfigurasi Otentikasi IAM.....	11
2.4.3 Proses Otentikasi.....	11
2.5 Otentikasi Twitter.....	13
2.5.1 Platform Pengembang.....	13
2.5.2 Konfigurasi Otentikasi IAM.....	13
2.5.3 Proses Otentikasi.....	14

# 1 Contoh Topologi



## 2 Panduan Konfigurasi

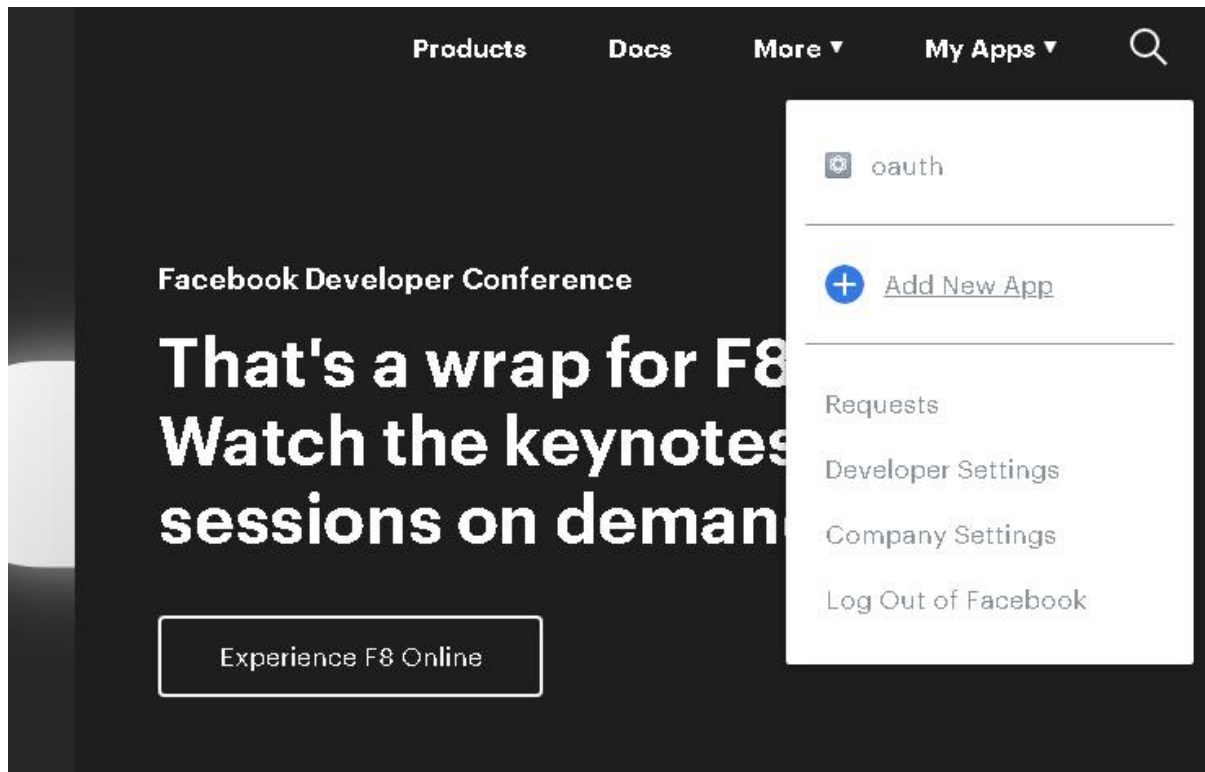
### 2.1 Konfigurasi Dasar

1. Masuk ke konsol web IAM.
2. [User]-->[Authentication]-->[External Auth Server]
3. Klik **tambah** dan periksa [Social Media Account]
4. [User]-->[Authentication]-->[Authentication Policy]-->[Add new Authentication Policy, isi segmen IP range, pilih Social Media Server].

### 2.2 Otentikasi Facebook

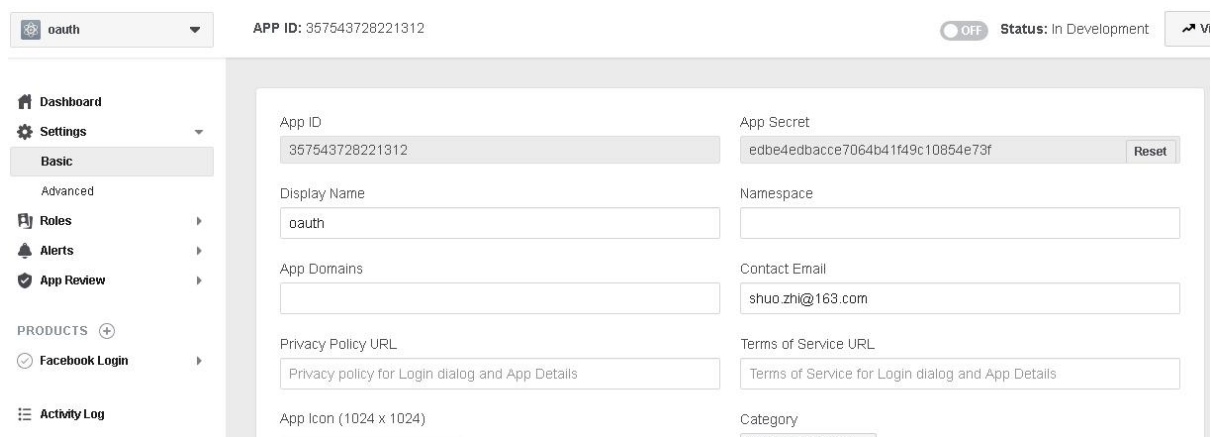
#### 2.2.1 Platform Pengembang

1. Situs web Platform pengembang Facebook:  
<https://developers.facebook.com>  
Periksa Add **New App**, isi **Name** dan **Mail Address**.

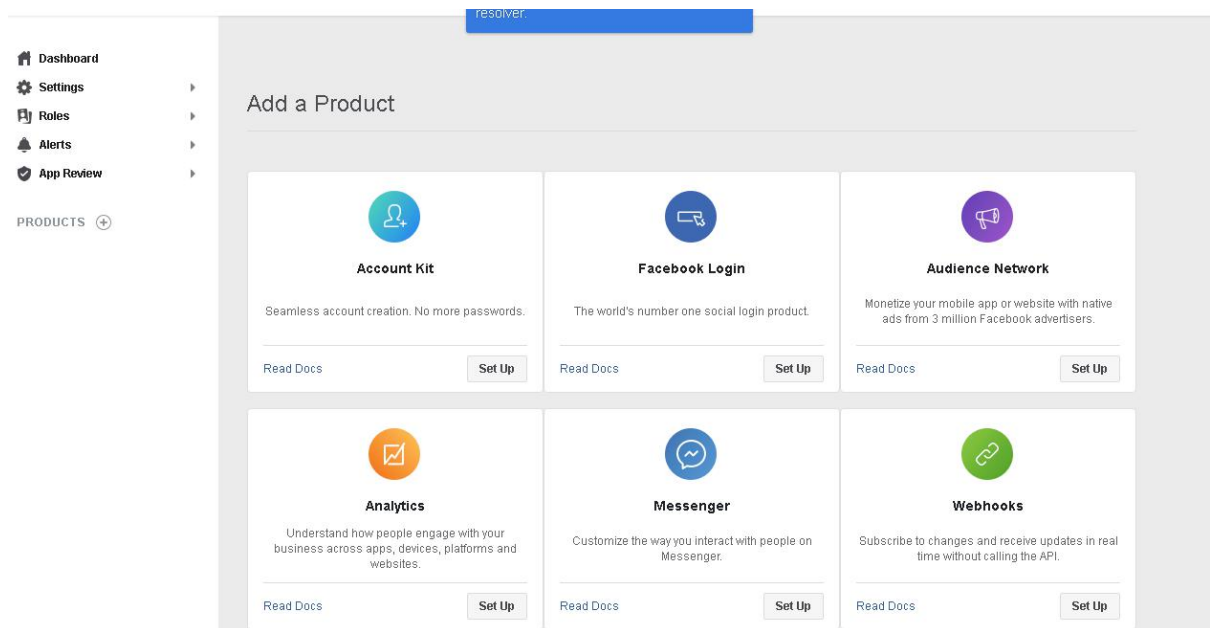


2. Periksa **Setting** dan periksa **Basic**,
3. Dapatkan **App ID** dan **App Secret**;

Isi **Privacy Policy URL**: itu **Privacy Policy URL** yang diperlukan untuk mengisi beranda perusahaan anda. Faktanya, parameter ini tidak digunakan untuk otentikasi oauth. Anda bahkan dapat menulis URL yang tidak ada.



4. tambah "**Facebook Login**" produk ,periksa "**Web**":

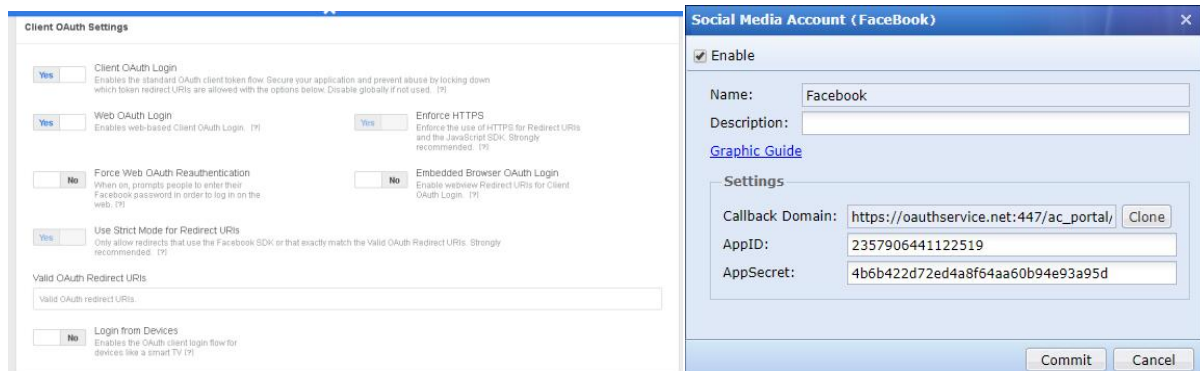


Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.



5. Arahkan ke pengaturan, Isi URIs pengalihan OAuth yang valid:

[https://oauthservice.net:444/ac\\_portal/oauth\\_callback.html](https://oauthservice.net:444/ac_portal/oauth_callback.html) (Salin dari konsol IAM)



Terakhir, Isi URL kebijakan privasi, lalu lakukan semua pengaturan.

## 2.2.2 Konfigurasi Otentikasi IAM

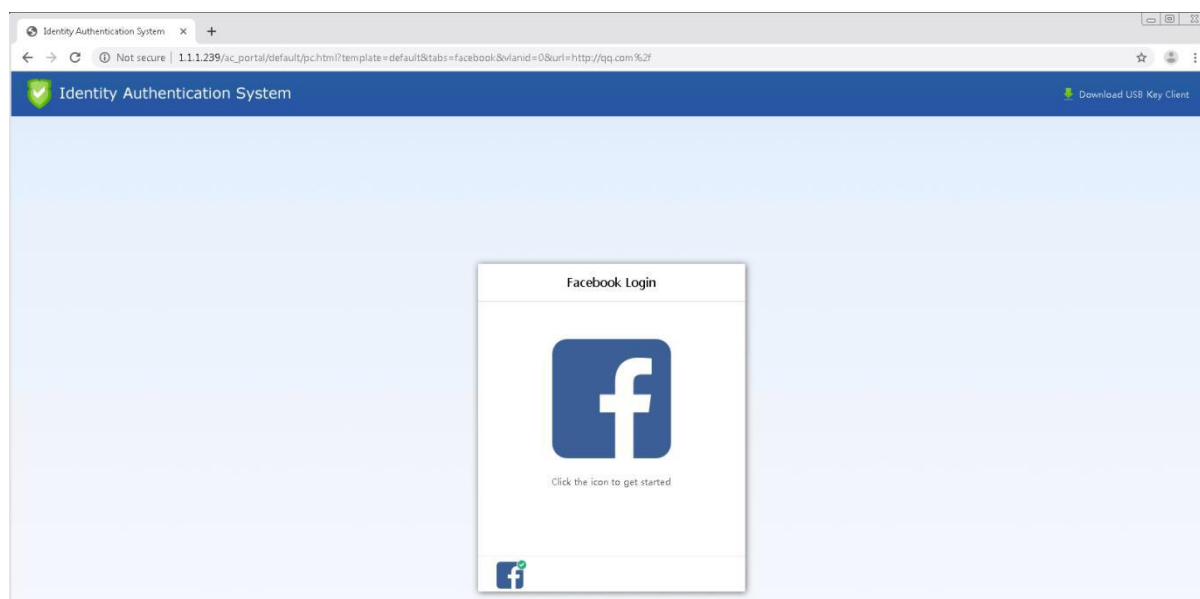
1. **External Auth Server** konfigurasi: hanya perlu diisi **AppID** dan **AppSecret**.



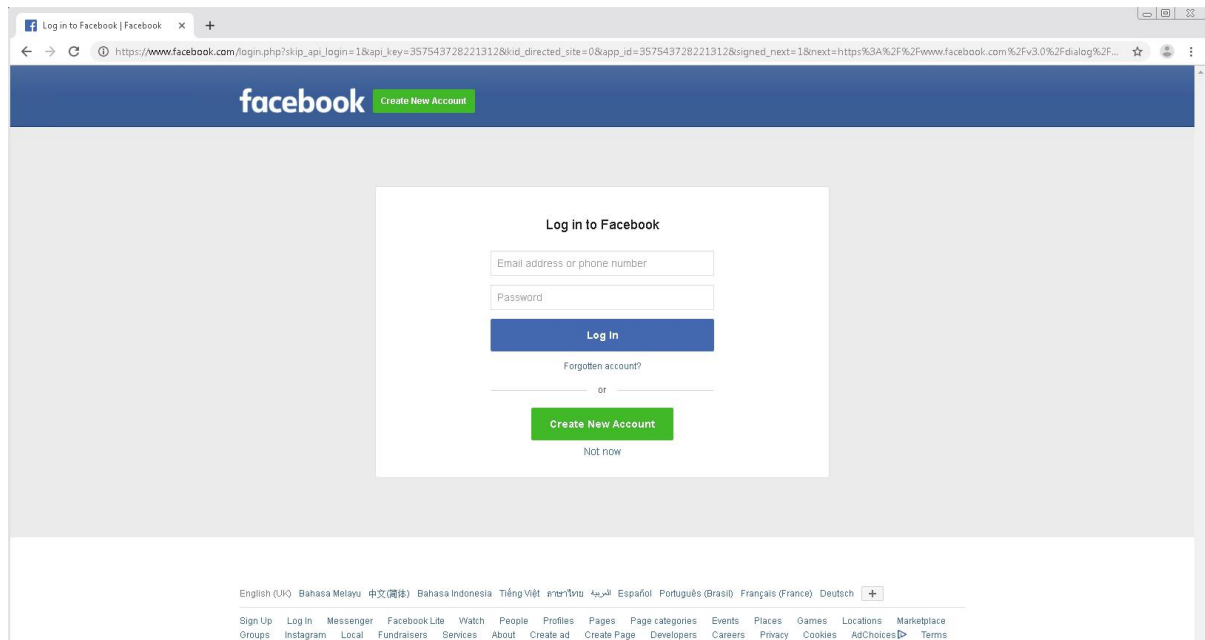
2. [User]-->[External Auth Server]-->[Authentication Policy]-->[Add Policy, isi Otentikasi range, Pilih Server Otentikasi Facebook yang Anda konfigurasi].

## 2.2.3 Proses Otentikasi

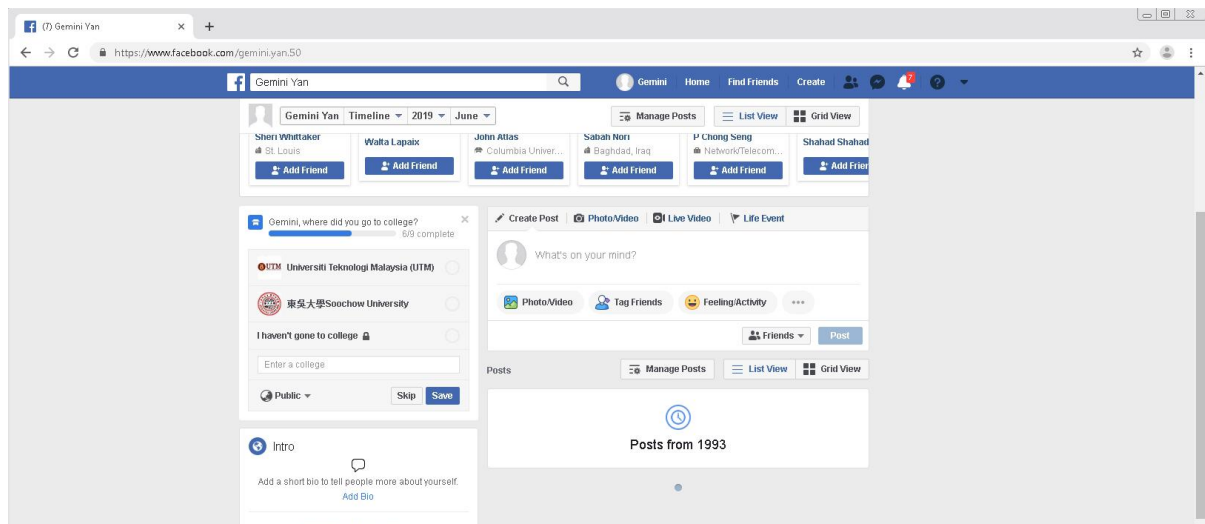
1. Klik Ikon Facebook.



2. Masukkan username dan password akun Facebook dan klik login:



### 3. Otentikasi selesai:



### 4. Anda dapat melihat nama pengguna di **Pengguna Online**:

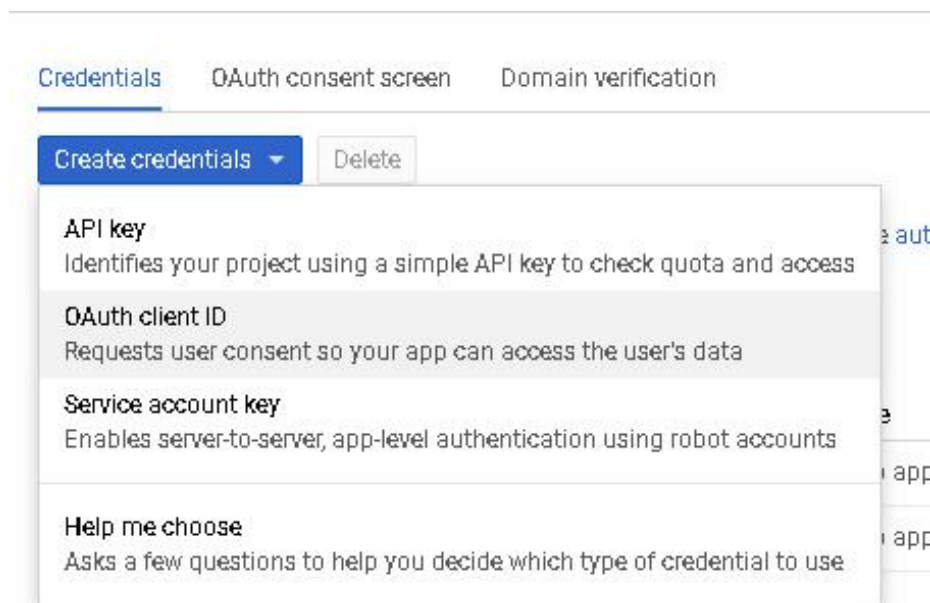
Online Users							
Auto Refresh: 5 second(s)   Refresh   Filter   Lock   Unlock   Logout   Export   Search by Username   Search							
Status: All Endpoint Device: All Objects: none							
User Group	No.	Username(Atlas)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Locked
Members	1	346335453@qq.com	/	192.168.19.208	Verifying...	OAuth Login	2019-06-24 14:38:19Login
							Online Duration: 03 minutes 01 seconds

## 2.3 Otentikasi Gmail

### 2.3.1 Platform Pengembang

1. Login ke platform pengembang google: <https://console.developers.google.com>
2. Periksa **Credentials**, periksa **Create credentials**, periksa **“OAuth Client ID”**.





3. Periksa “**Web Application**”, Isi URL pengalihan resmi :

[http://oauthservice.net/ac\\_portal/oauth\\_callback.html](http://oauthservice.net/ac_portal/oauth_callback.html) (Direkomendasikan untuk menyalin URL pengalihan langsung dari bagian belakang IAM.)

← Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

**Application type**

- ☒ Web application
- ☐ Android [Learn more](#)
- ☐ Chrome App [Learn more](#)
- ☐ iOS [Learn more](#)
- ☐ Other

**Name** ⓘ

oauth-18

**Restrictions**

Enter JavaScript origins, redirect URIs, or both [Learn More](#).

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

**Authorized JavaScript origins**

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard ([https://\\*.example.com](https://*.example.com)) or a path (<https://example.com/subdir>). If you're using a nonstandard port, you must include it in the origin URI.

<https://www.example.com>

Type in the domain and press Enter to add it

**Authorized redirect URIs**

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

<http://oauthservice.net>

<https://www.example.com>

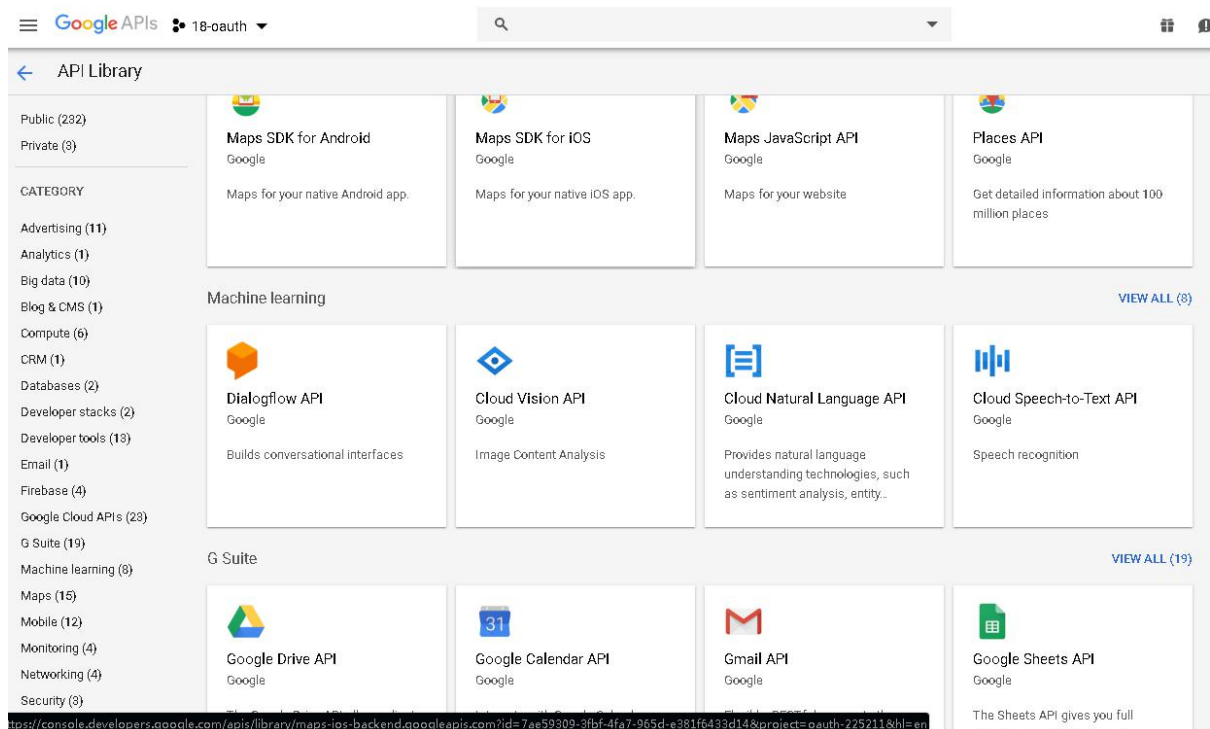
Type in the domain and press Enter to add it

Create Cancel

4. Isi **AppID** dan **AppSecret** yang Anda peroleh dari Situs Web Pengembang Google.

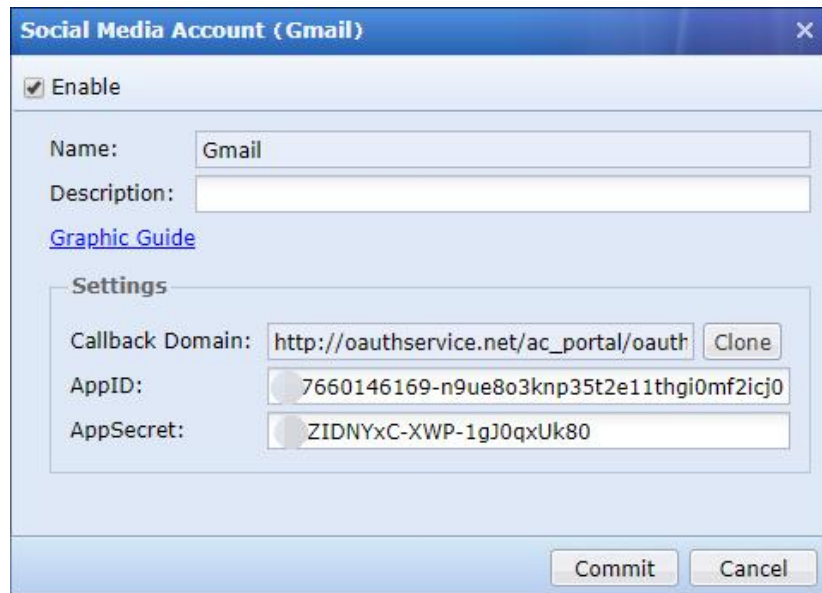
Client ID	687660146169-n9ue8o3knp35t2e11thgi0mf2kq0969.apps.googleusercontent.com
Client secret	yWZIDNYXC-XWP-1gJ0qxUk80
Creation date	Dec 11, 2018, 8:04:29 PM

5. Klik **Library**, Periksa “Gmail API” di “API Library”, Klik “Enable”.



## 2.3.2 Konfigurasi Otentikasi IAM

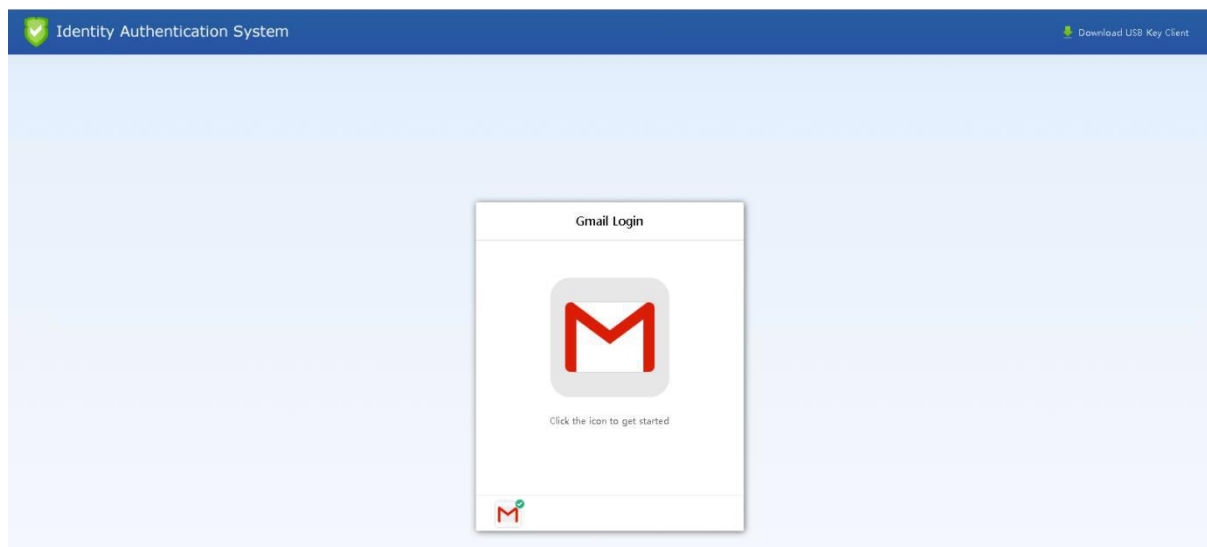
1. Konfigurasi External Auth Server: itu diperlukan untuk mengisi appid dan appsecret.



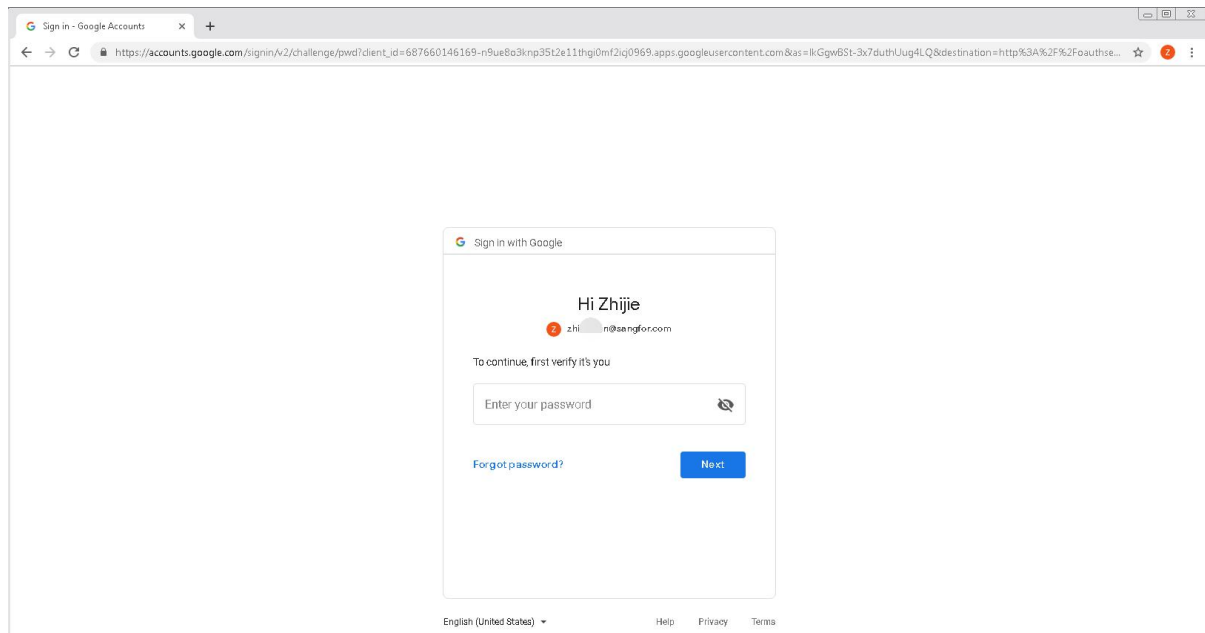
2. [User]-->[Authentication]-->[Authentication Policy]-->[Add new policy, Isi Segmen IP range, pilih Server Gmail].

### 2.3.3 Proses Otentikasi

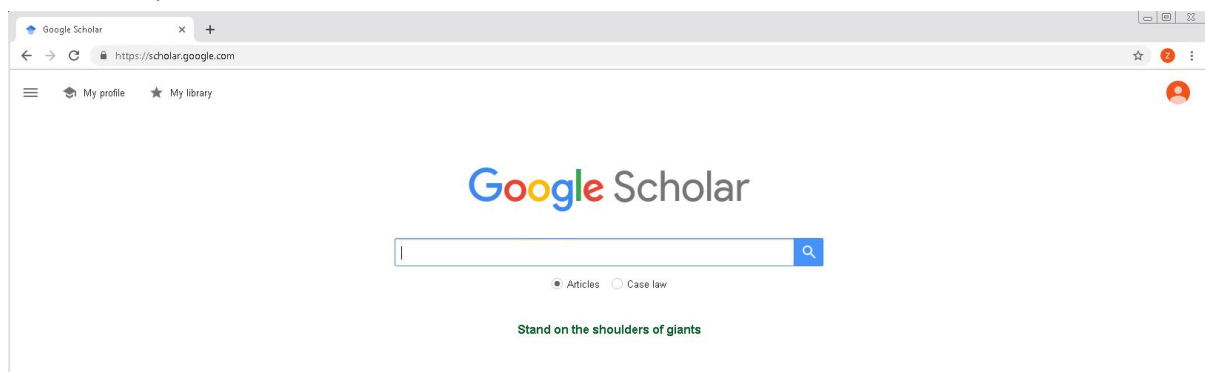
1. Klik ikon Gmail.



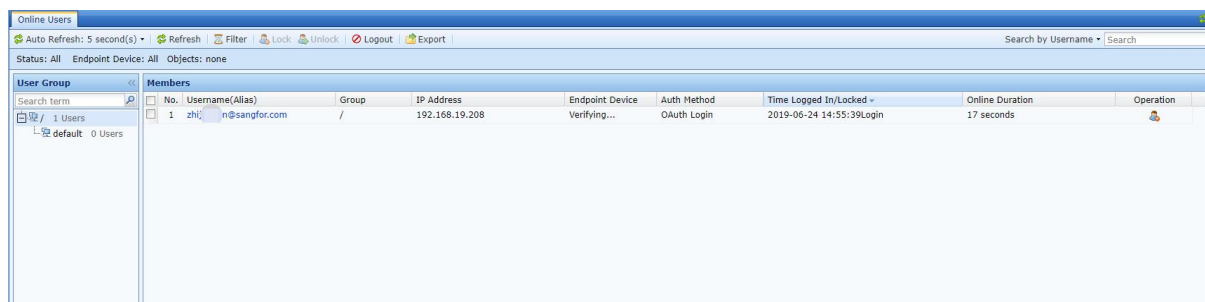
2. Masukkan username dan password.



3. Setelah otentikasi selesai, itu akan mengarahkan ke halaman web yang ingin Anda jelajahi sebelumnya.



4. Anda dapat melihat pengguna di Pengguna Online.

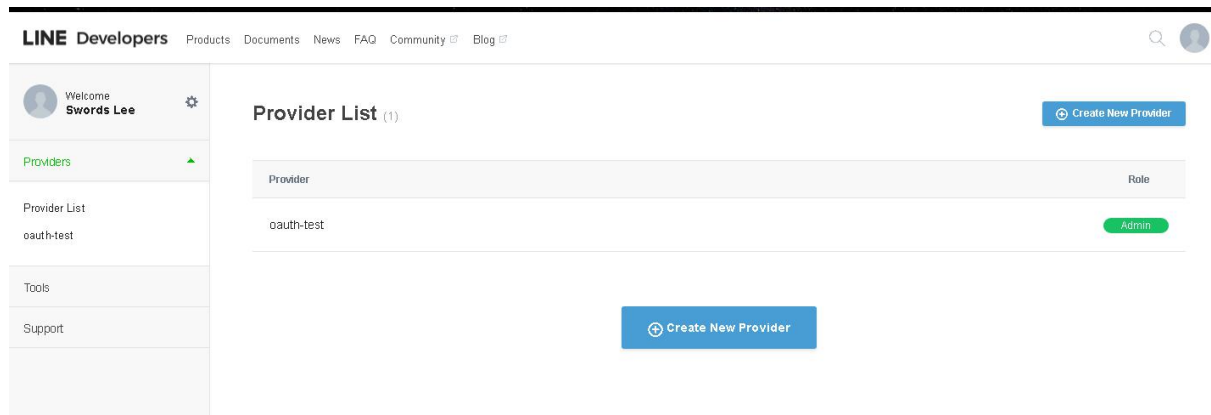


## 2.4 Otentikasi Line

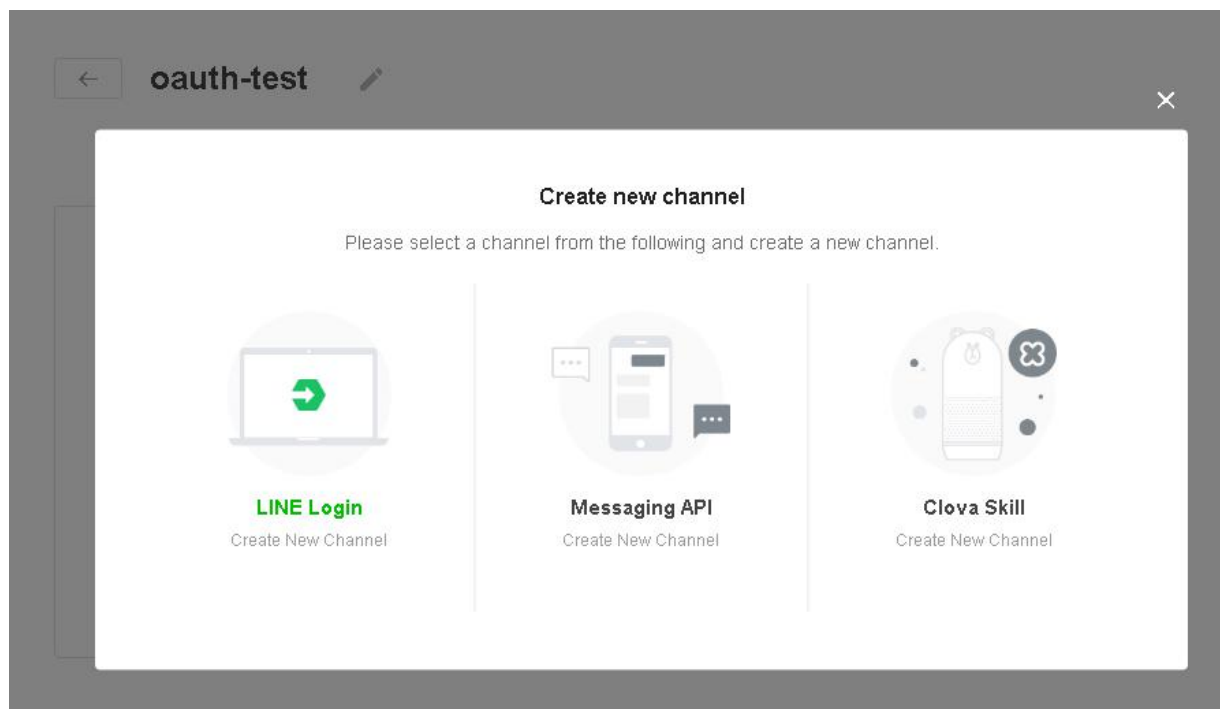
### 2.4.1 Platform Pengembang

1. Login ke platform pengembang Line: <https://developers.line.biz/console/>

Pilih penyedia, klik Create New Provider, ikuti instruksi untuk menyelesaikan pembuatan penyedia.



2. Buka penyedia yang dibuat, klik new channel, pilih LINE Login, ikuti petunjuk untuk menyelesaikan pembuatan saluran.



3. Klik untuk masuk ke saluran, dapatkan Channel ID, Channel secret, isi appid, appsecret dibawah channel setting, dan periksa LINE Login (NATIVE\_APP), LINE Login (WEB) dibawah App type.

**Channel ID** ⓘ  
1631365883

**Channel secret** ⓘ  
a8eab1b4391c1eef8290e169dea284cb Issue

**App type** ⓘ

☒ LINE Login (NATIVE\_APP)

☒ LINE Login (WEB)

Update Cancel

4. Setel Callback URL dibawah App Setting untuk menyalin di konsol web IAM.

### Redirect settings

Set the URL for where the user is redirected after logging in.

Callback URL [?](#)

http://oauthservice.net/ac\_portal/oauth\_callback.html

Edit

## 5. Ubah channel status ke published.

[TOP](#) > [Provider List](#) > [oauth-test](#) > [oauth-test](#) > [App settings](#)

[←](#)  **oauth-test** [LINE Login](#) [Admin](#) Published ...

[Channel settings](#) [App settings](#) [Roles](#) [Testers](#) [LIFF](#)

Configure the settings required for integrating LINE Login on iOS, Android, and web apps.

## 2.4.2 Konfigurasi Otentikasi IAM

1. External Auth Server: Ini diperlukan untuk mengisi appid dan appsecret parameter.

**Social Media Account (Line)** ×

☒ Enable

Name:

Description:

[Graphic Guide](#)

**Settings**

Callback Domain:  [Clone](#)

AppID:

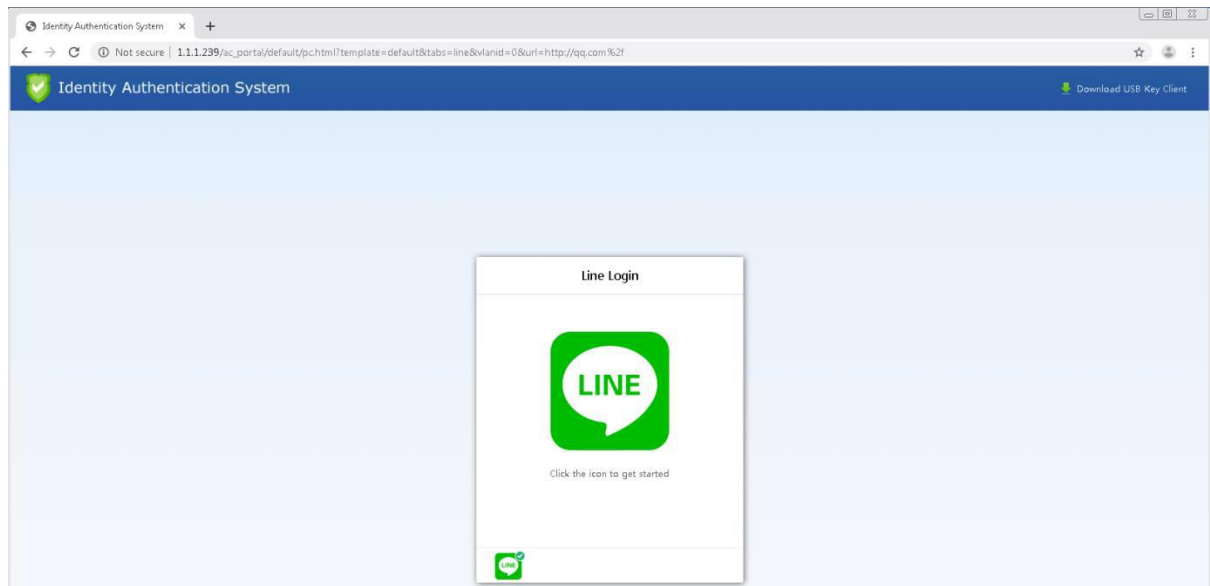
AppSecret:

[Commit](#) [Cancel](#)

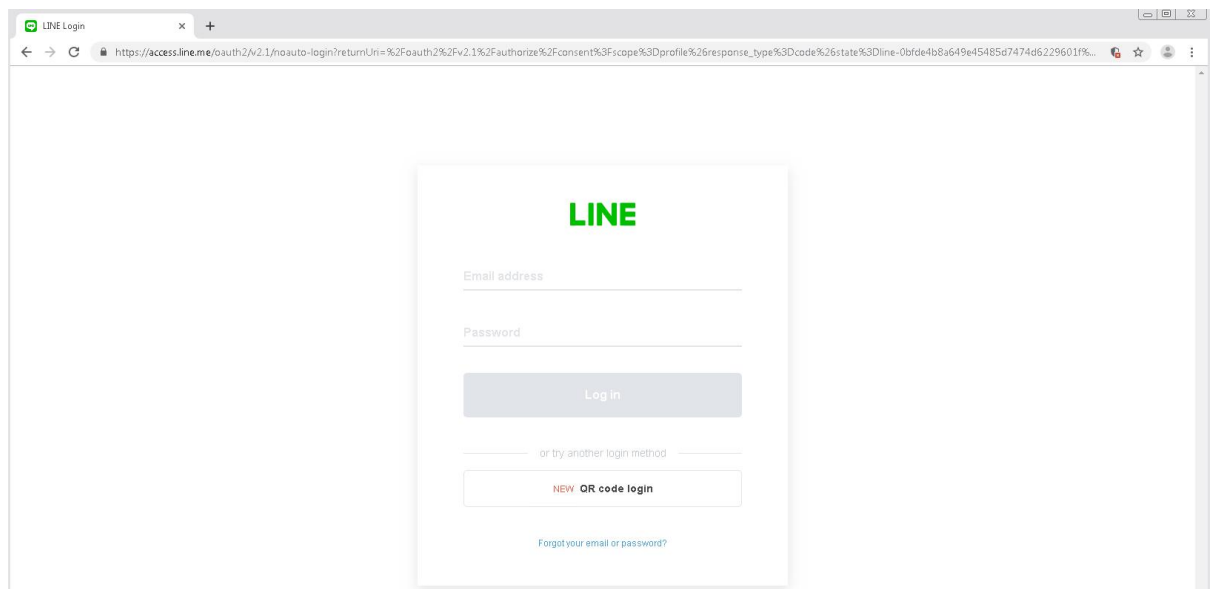
2. [User]-->[Authentication]-->[Authentication Policy]-->[Add new Policy, isi segmen IP range, pilih Line otentikasi Server yang Anda konfigurasi sebelumnya].

## 2.4.3 Proses Otentikasi

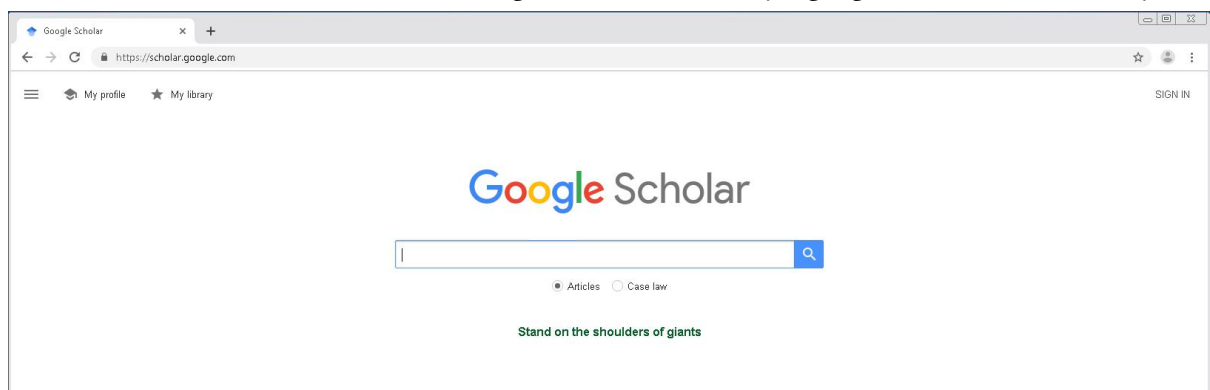
1. Klik pada ikon line.



2. Pergi ke halaman login line dan masukkan akun password:



3. Setelah otentikasi berhasil, itu akan mengarahkan ke halaman yang ingin Anda akses sebelumnya.



4. Dapat melihat pengguna online.

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Locked	Online Duration	Operation
1	sangfor	/	192.168.19.208	Verifying...	OAuth Login	2019-06-24 15:15:48Login	35 seconds	

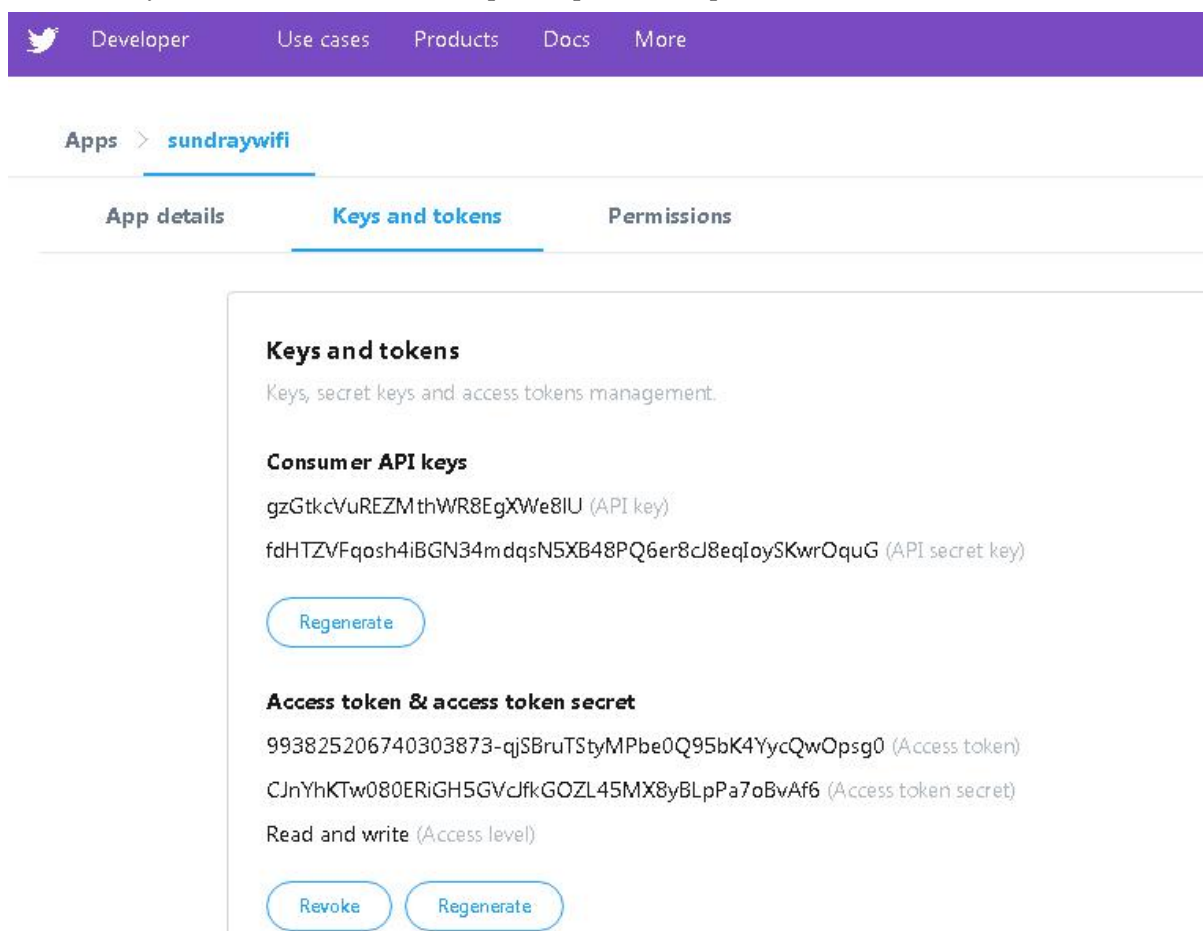
## 2.5 Otentikasi Twitter

### 2.5.1 Platfrom Pengembang

1. Masuk ke platform pengembang twitter: <https://developer.twitter.com/en/apps>
2. Pergi ke klik **Detail** dan pergi ke app.



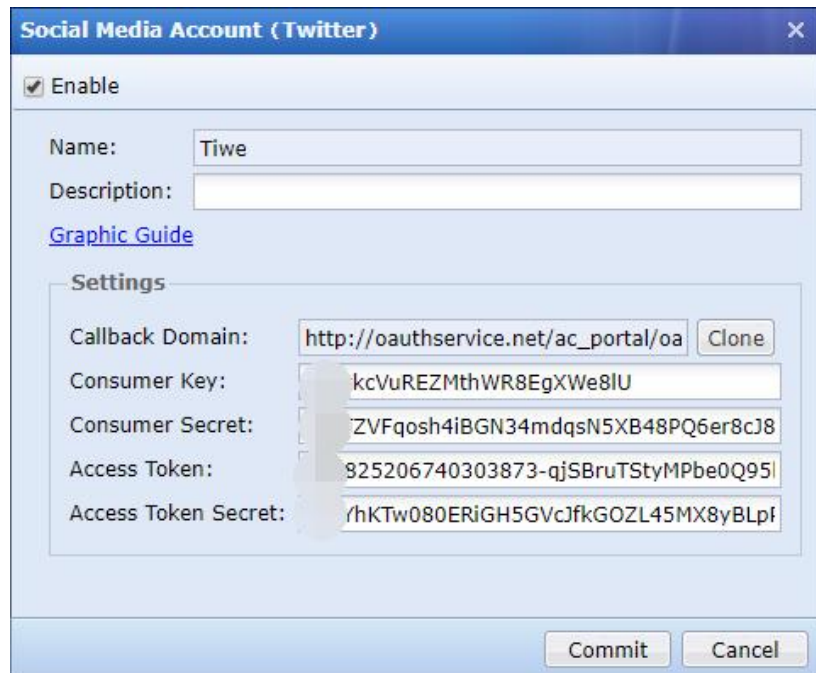
3. Klik **"Keys and tokens"** untuk mendapatkan parameter aplikasi;



### 2.5.2 Konfigurasi Otentikasi IAM

1. External Auth Server: Isi parameternya.

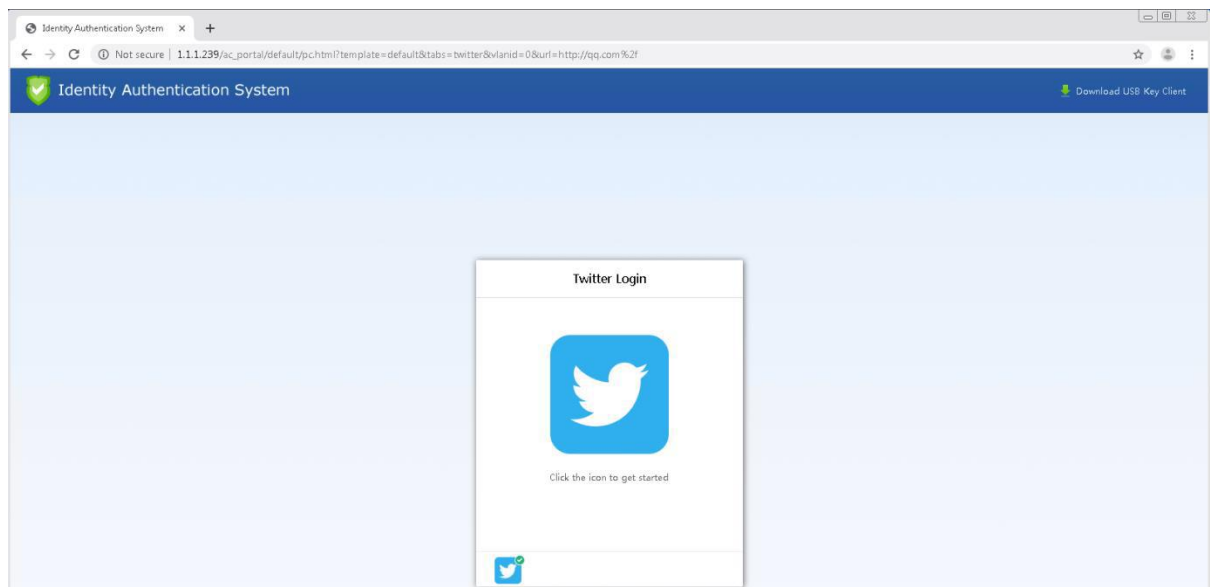




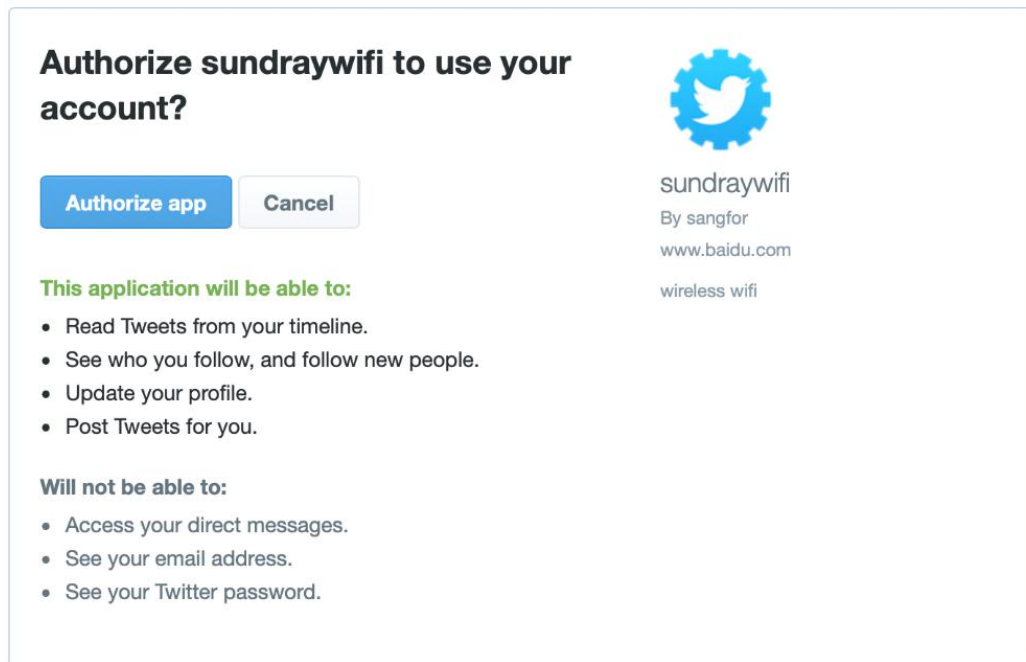
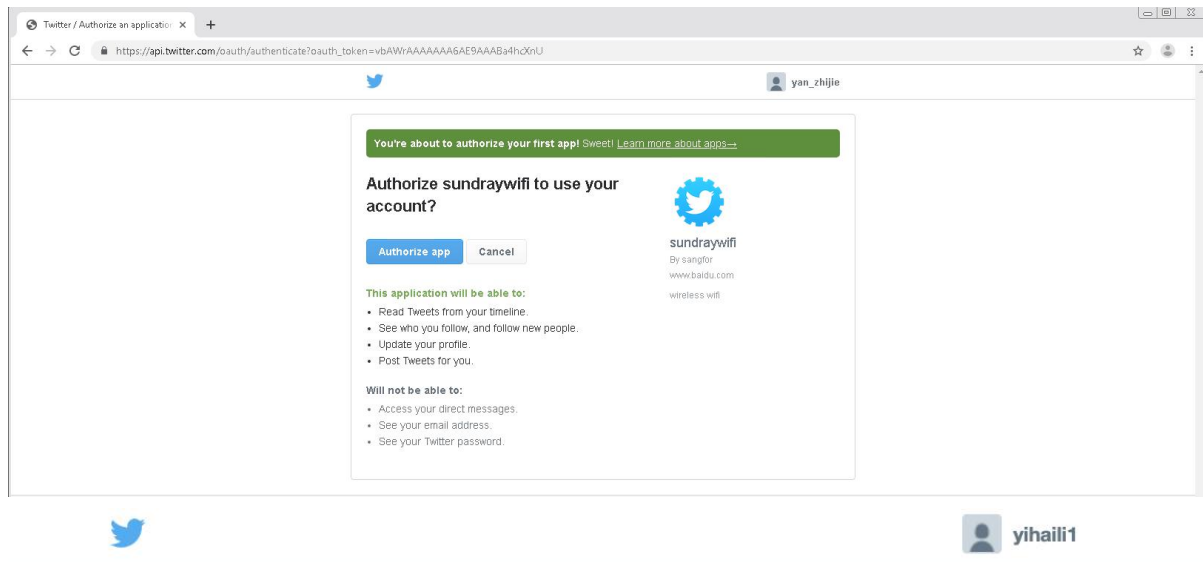
2. [User]-->[Authentication]-->[Authentication Policy]-->[Add new Policy, Masukkan otentikasi range, periksa Server Otentikasi Twitter]

### 2.5.3 Proses Otentikasi

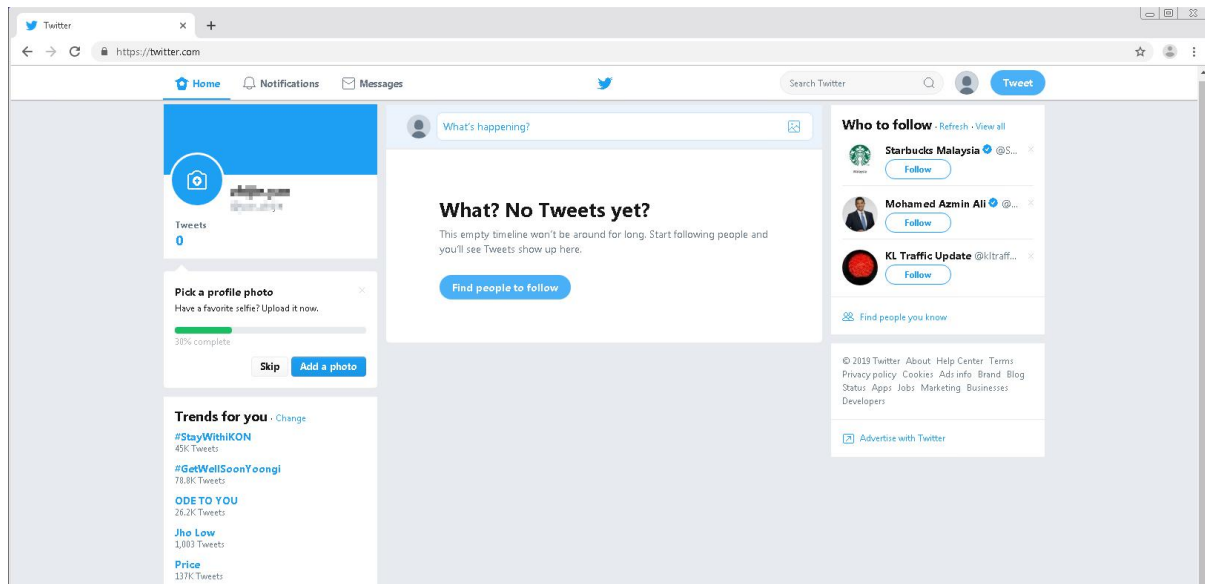
1. Klik ikon Twitter.



2. Masukkan akun Twitter.



3. Setelah diotentikasi, Anda bisa memakai Twitter.



4. Anda dapat melihat pengguna di Pengguna Online.

A screenshot of the 'Online Users' interface. It features a table with columns for 'No.', 'Username(Allas)', 'Group', 'IP Address', 'Endpoint Device', 'Auth Method', 'Time Logged In/Locked', 'Online Duration', and 'Operation'. The table contains one row of data for a user with IP address 192.168.19.208. The interface also includes a search bar, a refresh button, and a status filter.



Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc. SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing. Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.