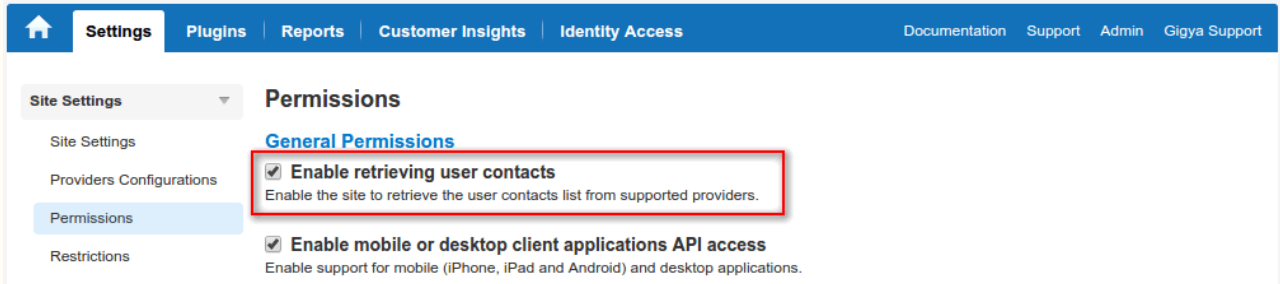


# Twitter

This page is a step-by-step guide for the process of opening and setting up an external application in Twitter as part of the [Gigya Setup](#) process.

When using any 3rd Party Apps with Gigya, it is important to ensure that you **Enable retrieving user contacts** from the [Permissions](#) page of the [Console](#) prior to making your app live. This enables the user's contacts retrieval from providers that don't consider this an elevated permission.



## Phase 1 - Opening an External Application in Twitter

1. Log into your Twitter account and click on the following URL: <https://dev.twitter.com/> or <https://apps.twitter.com/app/new> or <https://apps.twitter.com/>.
2. In the "Application Details" page:

- Fill in your application name, description and website address

**Application Details**

**Name \***

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

**Description \***

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

**Website \***

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.  
(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

**Callback URL**

Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth\_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

- Use the following callback URL: <https://socialize.gigya.com/GS/GSLogin.aspx>

Optional: If you are planning on configuring a domain alias (CNAME), please replace 'socialize.gigya.com' with your alias subdomain (CNAME value). i.e., <https://socialize.us1.gigya.com/GS/GSLogin.aspx>.

Important information for clients using anything other than the US Data Center:

**Note:** If your site is defined under one of Gigya's non-US data centers, replace domain references to "socialize.gigya.com" (or "socialize.us1.gigya.com") with **https://socialize.<data\_center>/**

Where <Data\_Center> is:

- **us1.gigya.com** - For the US data center.
- **eu1.gigya.com** - For the European data center.
- **au1.gigya.com** - For the Australian data center.
- **ru1.gigya.com** - For the Russian data center.
- **cn1.gigya-api.cn** - For the Chinese data center.

If you are not sure of your site's data center, see [Finding Your Data Center](#).

Domain references are defined in Gigya's [dashboard](#), externally in social network app definition pages, and when using Gigya's SDKs to set the domain (in particular the *APIDomain* field in class *GSRequest*).

This means that, for instance, if your API key is for the Chinese Data Center your Twitter Callback URL will be:

```
https://socialize.cn1.gigya-api.cn/GS/GSLogin.aspx
```

If you are using a CNAME (API Domain Prefix), the URI would be:

```
https://<YOUR-CNAME>/GS/GSLogin.aspx
```

- Read the "Developer Agreement" and check the "Yes, I agree" checkbox.
  - Click the "Create your Twitter application" button.
3. In the **Application Management** page, in the **Settings** tab:

## Application Details

### Name \*

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

### Description \*

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

### Website \*

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.

(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

### Callback URL

Where should we return after successfully authenticating? [OAuth 1.0a](#) applications should explicitly specify their `oauth_callback` URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

### Privacy Policy URL

The URL for your application or service's privacy policy. The URL will be shared with users authorizing this application.

### Terms of Service URL

The URL for your application or service's terms of service. The URL will be shared with users authorizing this application.

- Enable Callback Locking (It is recommended to enable callback locking to ensure apps cannot overwrite the callback url)
- Allow this application to be used to [Sign in with Twitter](#)

- Ensure "Allow this application to be used to Sign in with Twitter" is checked.
  - Upload your application icon (75x75 pixels, 700k max., JPG, GIF or PNG only). If no icon is uploaded Twitter will show its own logo.
  - Click the "Update Settings" button if you made any changes.
4. In the "Keys and Access Tokens" tab, copy the values in the "Consumer Key (API Key)" and "Consumer Secret (API Secret)" fields.

[Details](#)[Settings](#)[Keys and Access Tokens](#)[Permissions](#)

## Application Settings

Keep the "Consumer Secret" a secret. This key should never be human-readable in your application.

Consumer Key (API Key)

Consumer Secret (API Secret)

Access Level

Read-only ([modify app permissions](#))

Owner

Owner ID

5. In the "Permissions" tab:

- Under "Access", choose "Read only" if you are only using Twitter for sign-on purposes, or choose "Read and Write" if you will be sharing to Twitter.
- If you want to use the extended **Request email addresses from users** permission, select it here, under **Additional Permissions**.
- Click the "Update Settings" button if you made any changes.

## Gigya's Socialize App

[Test OAuth](#)[Details](#)[Settings](#)[Keys and Access Tokens](#)[Permissions](#)

### Access

What type of access does your application need?

[Read more about our Application Permission Model.](#)

- Read only
- Read and Write
- Read, Write and Access direct messages

**Note:**

Changes to the application permission model will only reflect in access tokens obtained after the permission model change is saved. You will need to re-negotiate existing access tokens to alter the permission level associated with each of your application's users.

### Additional Permissions

These additional permissions require that you provide URLs to your application or service's privacy policy and terms of service. You can configure these fields in your [Application Settings](#).

- Request email addresses from users

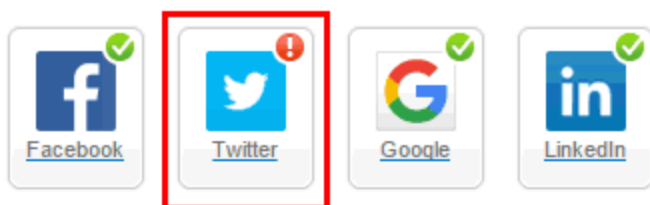
[Update Settings](#)

## Phase 2 - Configuring Twitter's Application Keys in Gigya's Website

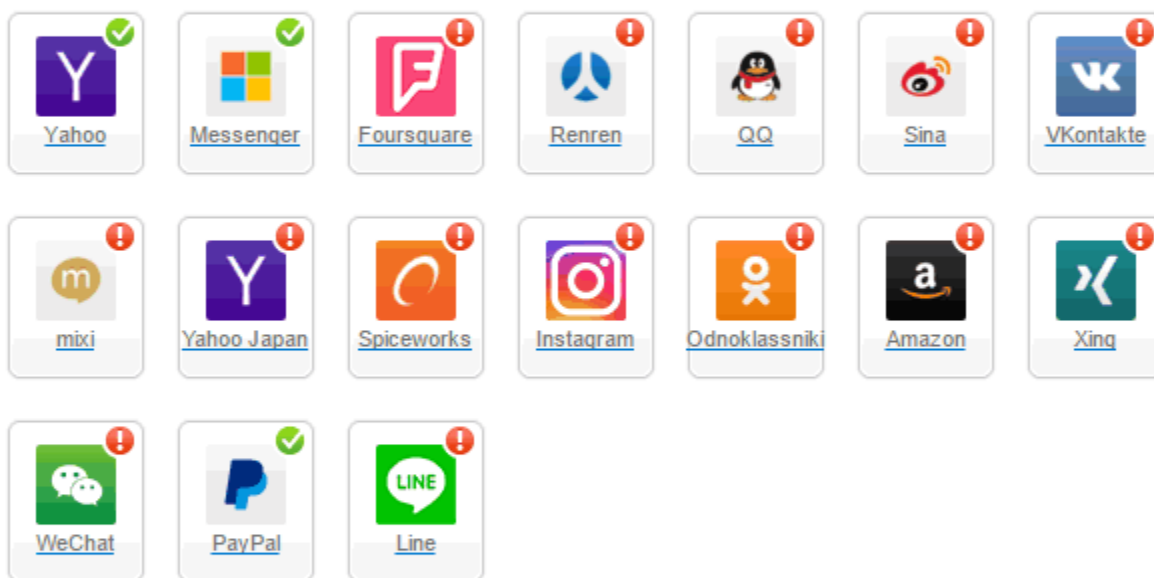
1. Open the [Providers Configuration](#) page of Gigya's Console.

2. Select Twitter from the list of providers:

### Main Social Networks

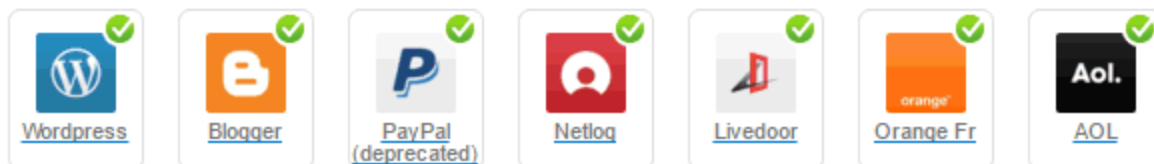


### More



### Providers that don't Require Configuration

Enable CNAME for all OpenID providers



3. Paste your "Consumer key" and "Consumer secret" from the end of phase 1.
4. If you are using a CNAME, be sure to select the "Enable CName" checkbox.
5. Select **Secure redirects only** to allow only HTTPS redirects from Twitter.
6. Click **Save Settings** on the lower right-hand corner.
7. If you have checked the **Request email addresses from users** permission in the Twitter app permissions section, navigate to the **Permissions** tab of the Gigya Console and ensure that the Twitter Permission **Enable retrieving email address** is checked, and then press **Save** at the bottom of the page.

**That's it, Twitters configuration is complete!** Please note that it might take up to 10 minutes for our system to become synchronized with Twitter.

Unable to render {include} The included page could not be found.

