SMS Login - OTP

> SAP Customer Data Cloud now offers Phone Number Login. This page describes a legacy solution.
>
> This feature is in maintenance-only mode. New customers will not have access to this feature.

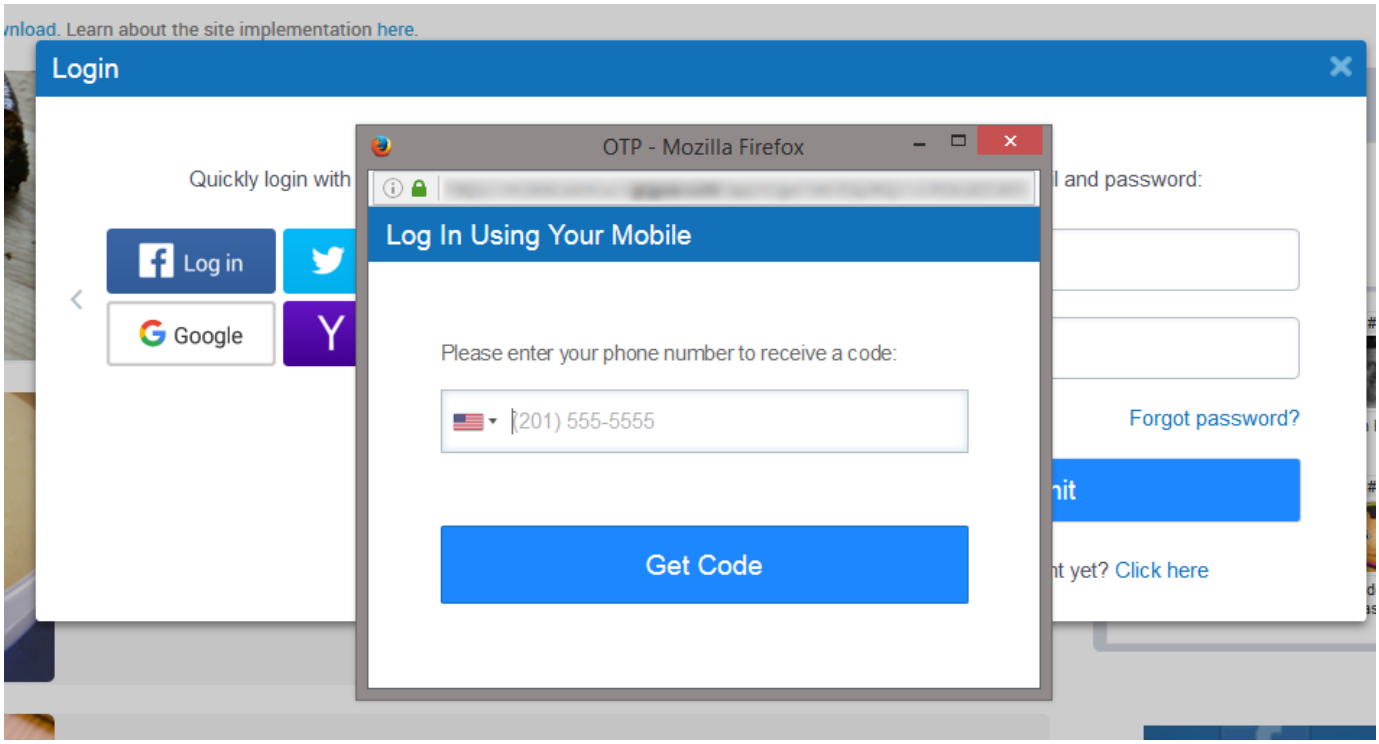
Introduction

Gigya offers **one-time password (OTP) authentication**, also known as **SMS Login,** as an additional login method that can be included in the Gigya login UI.

In websites with OTP, site users can enter their phone number to receive a one-time verification code to their mobile device. This code is entered in the website in order to log in or register immediately.

The benefits of this login method include:

- **Secure:** Strong identification.
- **Convenient:** No need to create or remember a username/password combination.
- **Global:** The service applies to users in all countries, and is particularly useful in countries where email addresses are less prevalent than mobile phones.
- **User-friendly:** Gigya's OTP functionality is set up as a custom third-party identity provider, through which users can log in, just like they can log in through Facebook or Twitter.



After users register to the site with their mobile device, they can be prompted to **link their social network identities** as additional authentication methods, providing the website with rich permission-based identity data. And conversely, if a user registering through OTP is already registered to the site through another authentication method, **the OTP identity can be added to the user's existing account** through Gigya's account linking functionality (see details below).

Implementation is mostly carried out by the Gigya team: all the customer has to do is add the custom OTP provider to the Gigya login UI (see Implementation section below for details).

Currently, verification codes are sent through SMS messaging only.

> - SMS Login (OTP) is a premium product that requires separate activation. If you are interested in adding it to your site package, please contact your Gigya Customer Engagement Executive.
> - SMS Login uses SAML, which is not supported natively on iOS. To use SMS Login on iOS, use a WebView.

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

Watch an Instructional Video

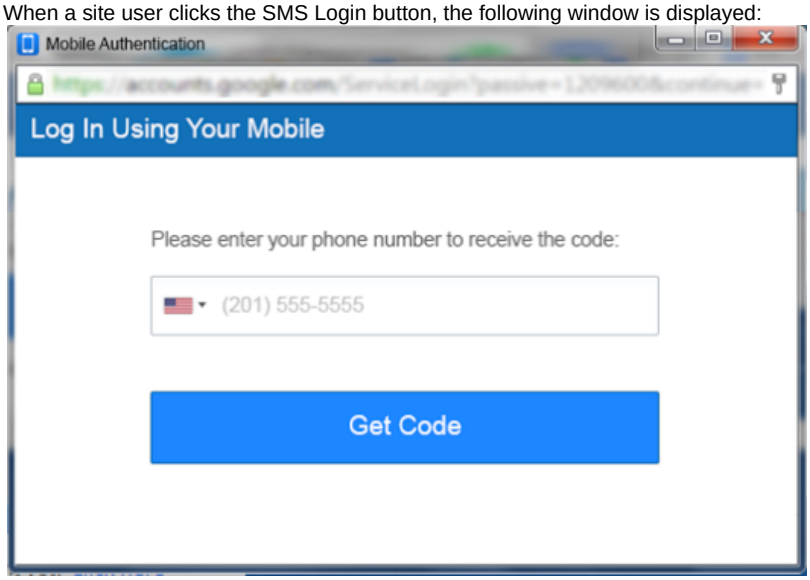
To watch a video about this subject, you can visit our Enablement portal with your approved SAP customer or partner ID (S user). Please visit the About page to find out how to get an S user.

User Flows

Basic Login/Registration Flow

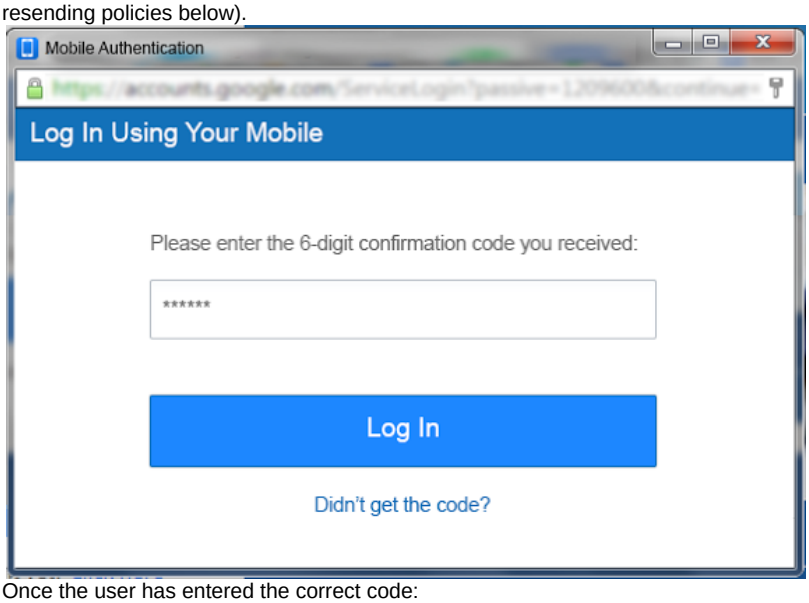
1. SMS Login is offered as another button in the Gigya social login UI. The custom button is fully customizable.

2. When a site user clicks the SMS Login button, the following window is displayed:



3. The user selects their country, enters their phone number and clicks the **Get Code** button.
4. If the phone number is valid, the user is sent an SMS message containing a random numeric code (by default the code is 6 digits long but this can be configured).

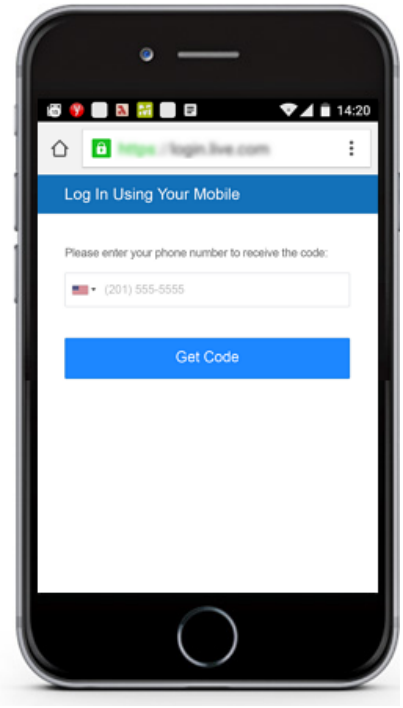
5. The system displays the following window in which the user can enter the code. There is also an option to request a resend (see resending policies below).

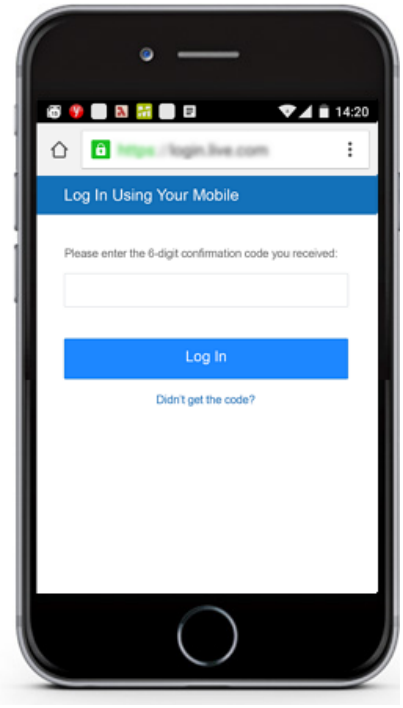


6. Once the user has entered the correct code:
    - **If the user exists in the website** (has already registered using mobile authentication with this phone number), they are logged in to their account.
    - **If this is a new user**, a new account is created.

Mobile Login/Registration Flow

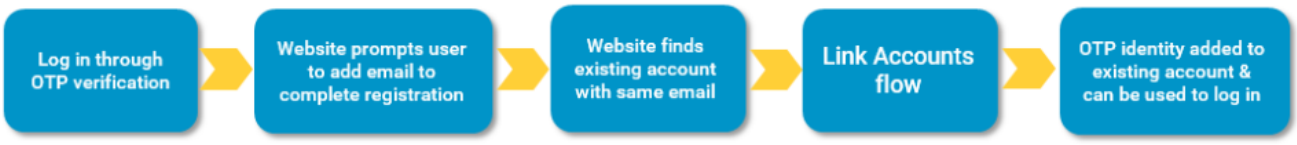
The flow when logging in with OTP in a mobile browser is identical to the desktop flow.





Account Linking Flow

This optional flow allows site users who are already registered to start using OTP to log into their existing accounts.



To enable the flow, the website has to:

1. Have Account Linking enabled through the Gigya console.
2. Make sure the federation policy is configured properly.
3. Require an email address for registration.

See more information about Gigya's Account Linking functionality.

SMS Gateway

Codes are sent by SMS through major, highly reliable SMS gateways. The service uses multiple gateways for optimal performance. When a user reports not having received the code, the service switches to a different gateway to resend the code.

Customization Options

The following OTP settings can be customized for each website. Discuss your preferences with your Customer Engagement Executive before implementation.

Language Settings

Gigya offers extensive language support in OTP imlementations. Error messages, and the actual SMS received by users, are available in the following languages:

Language	Language Code
English ***(default)***	en
Arabic	ar
Bulgarian	bg
Catalan	ca
Chinese (Mandarin)	zh-cn
Chinese (Hong Kong)	zh-hk
Chinese (Taiwan)	zh-tw
Croatian	hr
Czech	cs
Danish	da
Dutch	nl
Dutch Informal	nl-inf
Estonian	et-ee
Finnish	fi
French	fr
French Informal	fr-inf
German	de
German Informal	de-inf
Greek	el
Hebrew	he

Hindi (*SMS TFA Only)	hi
Hungarian	hu
Indonesian (Bahasa)	id
Italian	it
Japanese	ja
Kannada (*SMS TFA Only)	kn
Korean	ko
Latvian	lv-lv
Lithuanian	lt-lt
Malay	ms
Marathi (*SMS TFA Only)	mr
Norwegian	no
Persian (Farsi)	fa
Polish	pl
Portuguese	pt
Portuguese (Brazil)	pt-br
Romanian	ro
Russian	ru
Serbian (Cyrillic)	sr
Slovak	sk
Slovenian	sl
Spanish	es
Spanish Informal	es-inf
Spanish (Lat-Am)	es-mx
Swedish	sv
Tagalog	tl
Thai	th
Turkish	tr
Ukrainian	uk
Vietnamese	vi

Gigya currently supports locales out of the box.

In addition, the text and style of the OTP registration screen can be customised. For more information, see below.

Caps and Limitations

The following service caps and limitations can be configured based on the website's requirements:

- Code expiration
- How many code resends can be requested by a user
- SMS messages per IP

- Code requests per phone number
- Authentication attempts by a user (how many times they can retry entering the code)

To learn about adjusting the default settings please contact your Customer Engagement Executive.

> All codes are valid until their default expiration time, new codes will not invalidate any previous codes received that are still valid.

Custom HTML Style (CSS)

You can change the look and feel of the OTP screens using custom CSS.

These are the relevant HTML elements that may be involved:

```
<body>

<!-- Enter Phone Number form -->
<form class="form-enter-tel responsive-form" id="phase1">

    <div class="form-group">
        <label for="mobile-number"></label>
        <input type="tel" name="phone" id="mobile-number">
        <div class="help-block nv"></div>
    </div>

    <button type="submit" class="btn-submit"></button>

</form>

<!-- Enter Code form -->
<!-- Add the 'has-error' class to display validation error styles -->
<form class="form-enter-tel responsive-form hidden" id="phase2">

    <div class="form-group">
        <label for="code"></label>
        <input type="tel" id="code" name="code">
        <div class="help-block"></div>
    </div>

    <button type="submit" class="btn-submit"></button>

 <!-- Link to resend code to phone -->
    <div class="help-link">
        <a href="#" class="resend"></a>
    </div>
</body>
```

Sample CSS:

```
.responsive-form label {
    color: transparent;
    position: relative;
    margin-bottom:25px;
}

.responsive-form label:after {
    content: 'Enter your phone number to receive a code';
    color: blue;
    position: absolute;
    width: 100%;
    left: 0;
}
```

Implementation

The license could not be verified: License Certificate has expired!

Gigya's OTP offering is set up in the website as a SAML-based identity provider through which users can log in, just like they can log in through Facebook or Twitter.

The SAML setup will be carried out by your Customer Engagement Executive.

The customer will only have to do the following:

1. Provide Required Details to Gigya

In order to set up your OTP implementation, your Customer Engagement Executive needs the following information:

- Which site(s) you want to implement OTP in, if you have more than one site set up with a Gigya API Key
- Your desired OTP service settings, such as interface language, rate limits, etc. See the Customization Options section for the available settings. To learn about the default rate limits. please contact your Customer Engagement Executive.

2. Add SMS Login Button

After the custom SAML identity provider is created, you need to edit your Gigya login UI to add a custom button for SMS Login/OTP (see customButtons).

To build the button object:

- Set the **idpName** property to the name of the custom IDP provider created by Gigya for the purpose (ask your Gigya Customer Engagement Executive for the correct name).
- Set the **type** property to "saml".
- Set the **iconURL** and **lastLoginIconURL** properties to the default images created by Gigya or create icons of your own.

Download default OTP button graphics (all sizes)

Note:

- Your login UI may include multiple custom button objects, each representing a different SAML-based identity provider.

- A user cannot be connected to more than one SAML identity provider for the life of their account. Therefore, if the user connects through OTP, they will not be able to add a connection to another SAML identity provider in the future.

Best Practice: Add Prompt for Social Identities

An optional (but recommended) function is to ask users who have registered through OTP to add another login method to their account.

This prompt should appear after registration is finished.

This has several benefits:

- Added security for the user: if their mobile device is lost or temporarily unavailable, they can use another identity to log in.
- Added value for the website: users who add a social network connection provide the website with all the rich permission-based identity data Gigya usually offers.