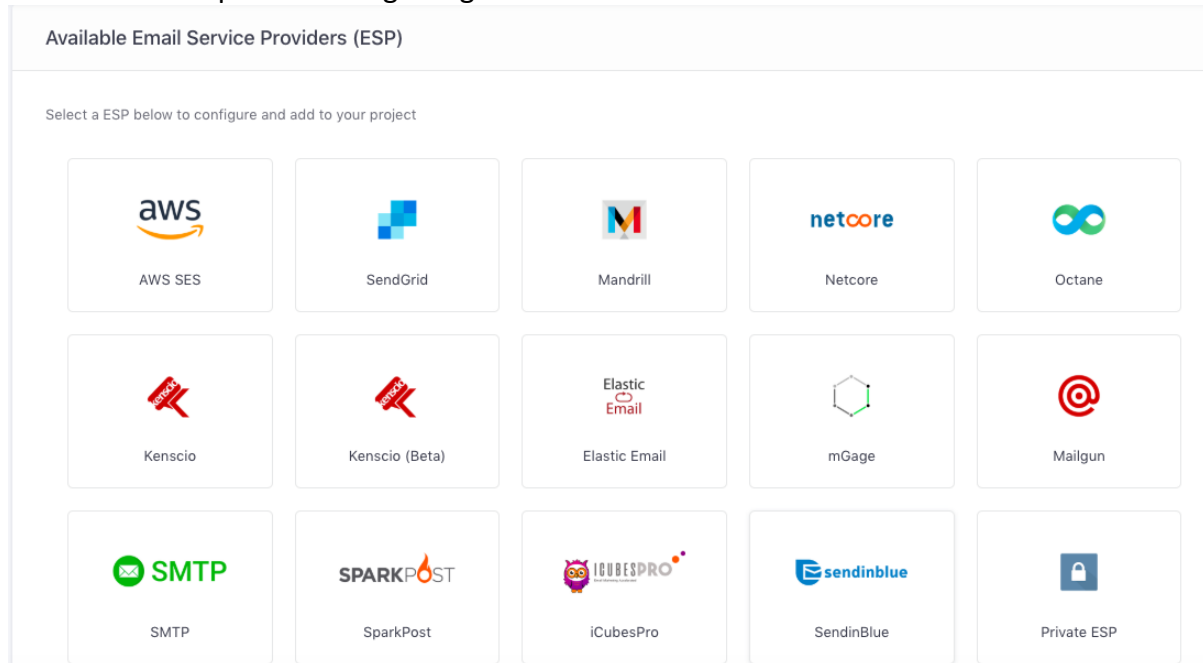


**For SMS & EMAIL, one can select their respective vendors from our platform and put the API Access code or Username & Password , thus getting connected to the platform.**

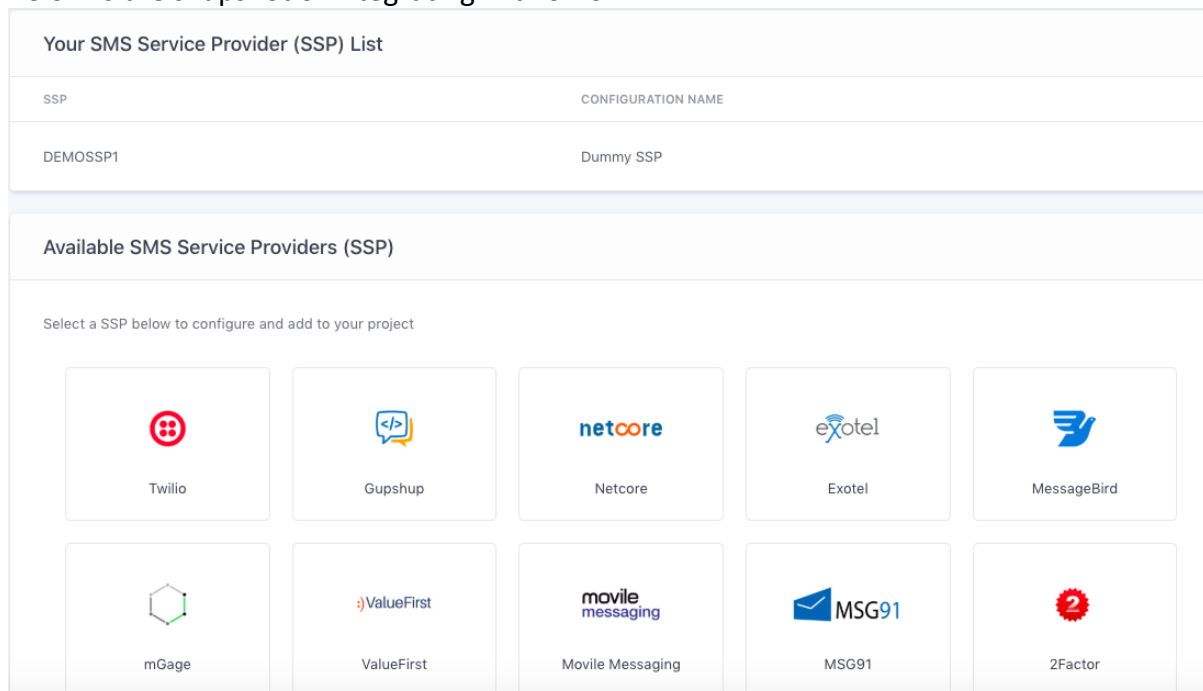
It's just plug and play which relieves the pressure of tedious integration with SMS & Email Provider.

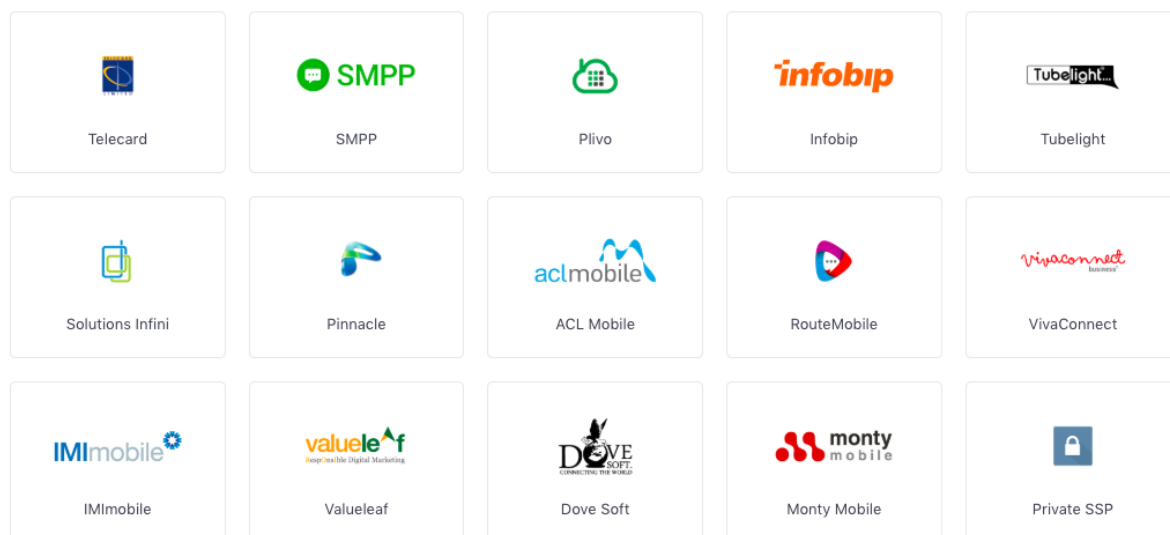
Below is the snapshot of integrating with Email:



You can also connect with your inhouse Email Solution without any hassles by choosing Private ESP

Below is the snapshot of integrating with SMS:





The ease of integrating with any providers along with in-house systems , is just a click. Below is the process. Click on the provider , the below window will open (eg: ACL Mobile for SMS)

Put in the username and Password and good to go.

The same way Email will work where you can integrate to your in house solution.  
Choose the SMTP or Private ESP:

For SMTP , below is the snapshot:

Configure ESP

ESP

SMTP

NAME YOUR CONFIGURATION ⓘ

HOST

PORT

SECURITY PROTOCOL

Select an Option

USERNAME

PASSWORD

ADD ESP

For Private ESP, below is the snapshot:

Configure ESP

ESP

Private ESP

NAME YOUR CONFIGURATION ⓘ

URL

CUSTOM HEADERS

+

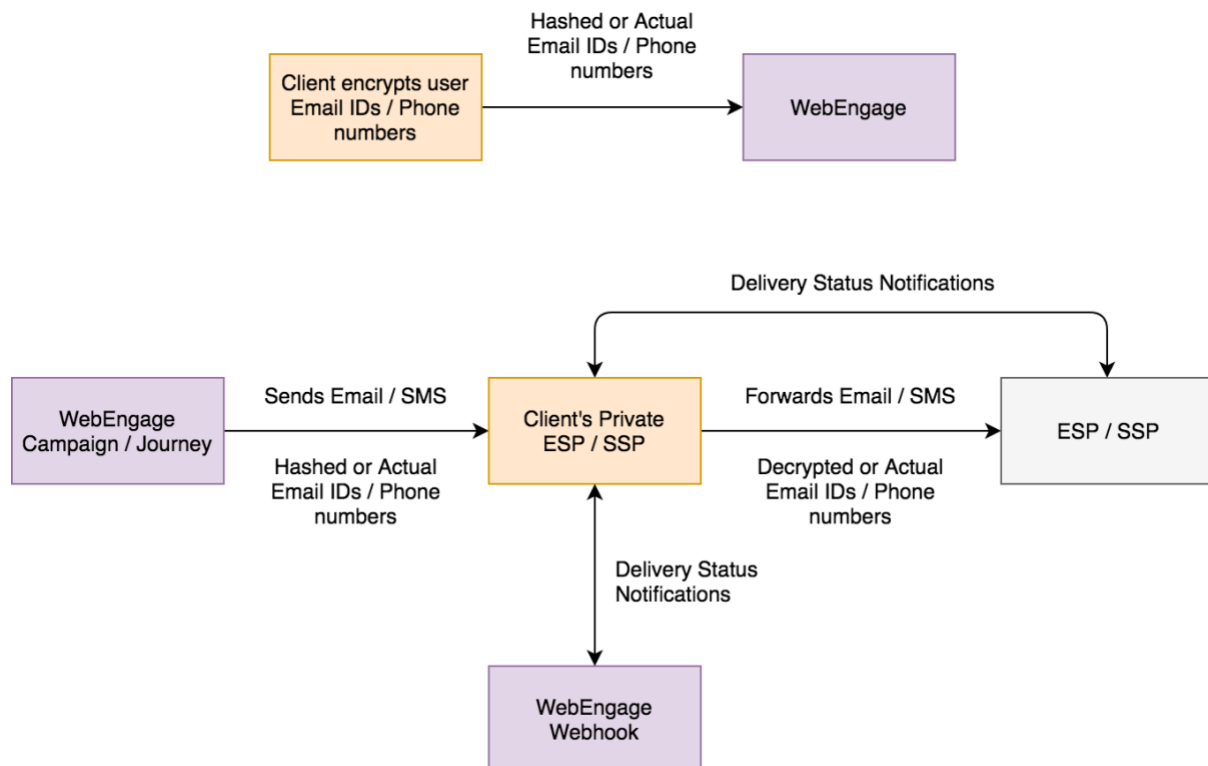
ADD HEADER

ADD ESP

## PII Hashing

For customers that are averse to passing their users' PII (Personally Identifiable Information) to third-party systems, WebEngage still enables user engagement over SMS without you ever having to pass the users' actual phone number. This involves two steps - passing hashed PII data and setting up private SSP API endpoints at your end.

Private SSP works as shown in the below flowchart.



## PII Hashing

### Which attributes are PII?

WebEngage recognizes phone and email user profile attributes as PII (Personally Identifiable Information).

If you opt for PII hashing, instead of passing the raw phone or email attributes to WebEngage, you need to pass the corresponding hashed values: `hashed_phone`, `hashed_email`.

WebEngage supports both hashed and non-hashed values of phone numbers for Private SSP setup, with hashed values always taking a precedence over non-hashed ones.

### Passing hashed PII values

Each SDK ([Website](#), [Android](#), [iOS](#)) exposes methods for you to pass hashed phone or email attributes against user profiles. Here's an example of how you would do that using the Website SDK.

Javascript:

```
Copy
webengage.user.setAttribute({
  'we_hashed_phone': 'e0ec043b3f9e198ec09041687e4d4e8d',
  'we_hashed_email': '144e0424883546e07dcd727057fd3b62'
});
```

You can pass and update hashed PII attributes using WebEngage [REST API](#) as well.

The values you pass against these attributes need to be already hashed or encrypted in a format that you can decrypt later on your infrastructure. Never pass the actual email or phone number values to these methods.

### Private SMS Service Provider Basics

WebEngage supports a plethora of SMS service providers for message delivery, including Twilio, Plivo, Gupshup and many more. When you opt to go the hashed PII route though, you'll need to set up - what we call a *Private SSP*.

A private SSP is an API endpoint that you expose for WebEngage to call, which essentially acts as a proxy between WebEngage and your actual service provider. WebEngage hits your Private SSP endpoint with a payload containing the hashed phone identifiers, the message body and some other data. WebEngage expects a JSON response at that instance denoting synchronous result (request success / failure). WebEngage also subscribes to your Webhooks and expects later hits, passing the subsequent Delivery Status Notifications: delivery (sent, bounced etc.) and interaction (clicked etc.) events.

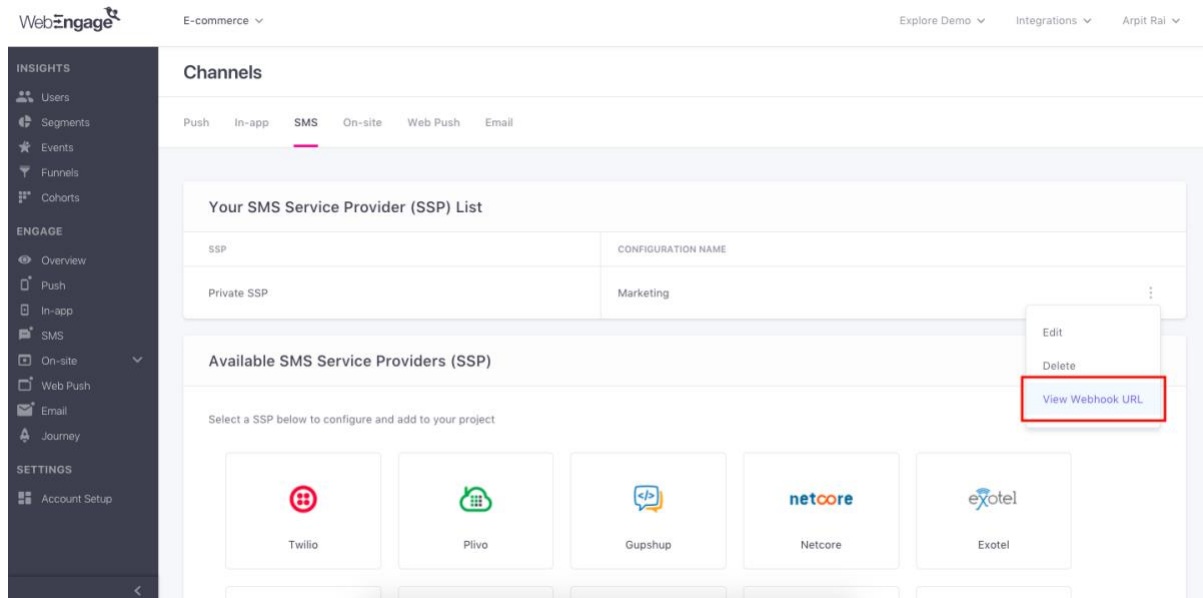
Here's a summary of how this works.

1. WebEngage POSTs to an API endpoint URL you provide us.
2. You can configure on WebEngage dashboard to pass custom data (key-value pair in headers) with this POST request.
  - a. Some headers cannot be overridden (e.g. "Content-Type": "application/json").
  - b. Custom headers can be used for authentication.
3. A unique ID will always be passed in custom data: UUID in case of SMS.
4. Body of the POST request will be in JSON format.

5. Response for the message request should be passed in the predefined format shown below.

6. Webhook settings:

a. URL to be set on your side for real-time delivery reports. This URL can be accessed on WebEngage dashboard under **Integrations > Channels** in your SSP list as shown below.



b. Delivery Status Notification request to be a POST (predefined JSON format).

c. Delivery Status Notification parameters must include the previously passed UUID.

d. errorCode and errorMessage parameters and values in case of failure should be passed in the predefined format shown below.

If your Private SSP is performing additional link wrapping on the links already wrapped by WebEngage (original URL) anywhere in the request payload, the wrapped domain must ask the caller to follow the original URL-encoded location.

For example:

Assume the SMS body has the below hyperlink:

`<a href="https://google.co.in/?param=%3D%3D%2B%20%20abcd"> Link </a>`

We have a parameter named param with a value of ==+ abcd here.

If you are further wrapping this link, the wrapped domain must ask the caller to follow the URL-encoded location (`https://google.co.in/?param=%3D%3D%2B%20%20abcd`), **not** the decoded one (`https://google.co.in/?param===+ abcd`).

## PII Masking

You can mark any system attribute, or any custom attribute of a user profile or an event as PII (personally identifiable field). Just head over to the *Data Management* section to get started. As you can see below, you can easily mark any attribute as PII to mask the value of the attribute on the dashboard and in the CSV files you download from WebEngage. In order to unmask the information such that all your team members can view the information, you can mark the item as *Not PII*.

Select Data management:

IP	Not PII	String	⋮
Landing Page	Not PII	String	⋮
Last Name	Not PII	String	⋮
Latitude	Not PII	Number	⋮
Longitude	Not PII	Number	⋮
Phone Number	Not PII	String	⋮
Referrer Host	Not PII	String	⋮
Referrer URL	Not PII	String	⋮
Vendor ID	Not PII	String	⋮

Mark as PII

Once you mark the item as PII, the value of the attribute will be masked on the WebEngage dashboard (and also in the CSV files you download) for all your team members who don't have access to the *View PII* functionality. You can set these permissions in the *Account Admins* section in WebEngage. By default, all your team members have access to the *View PII* functionality.

Live

## INSIGHTS

Users

Segments

Events

Funnels

Cohorts

## ENGAGE

Overview

Push

In-app

SMS

On-site ▾

Web Push

Email

Journey

## SETTINGS

Account Setup

## Users

Overview

Analyze

List of Users

All Users ▾

Search by email, user ID, phone

⌵ ⌵

USER ID	NAME	EMAIL	PHONE	COUNTRY	TOTAL SESSIONS
2384708	John Knowles	****	****	Singapore	--
6750447	Ron Lowes	****	****	India	--
1123414	Adam Smith	****	****	US	--