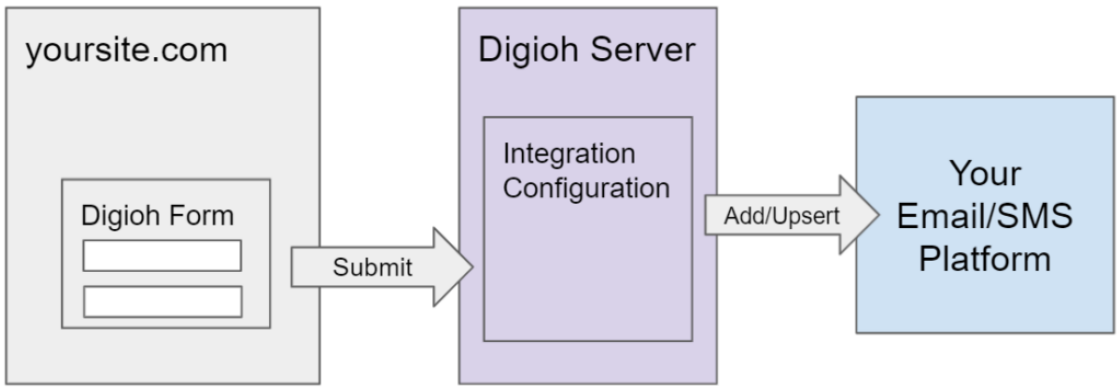
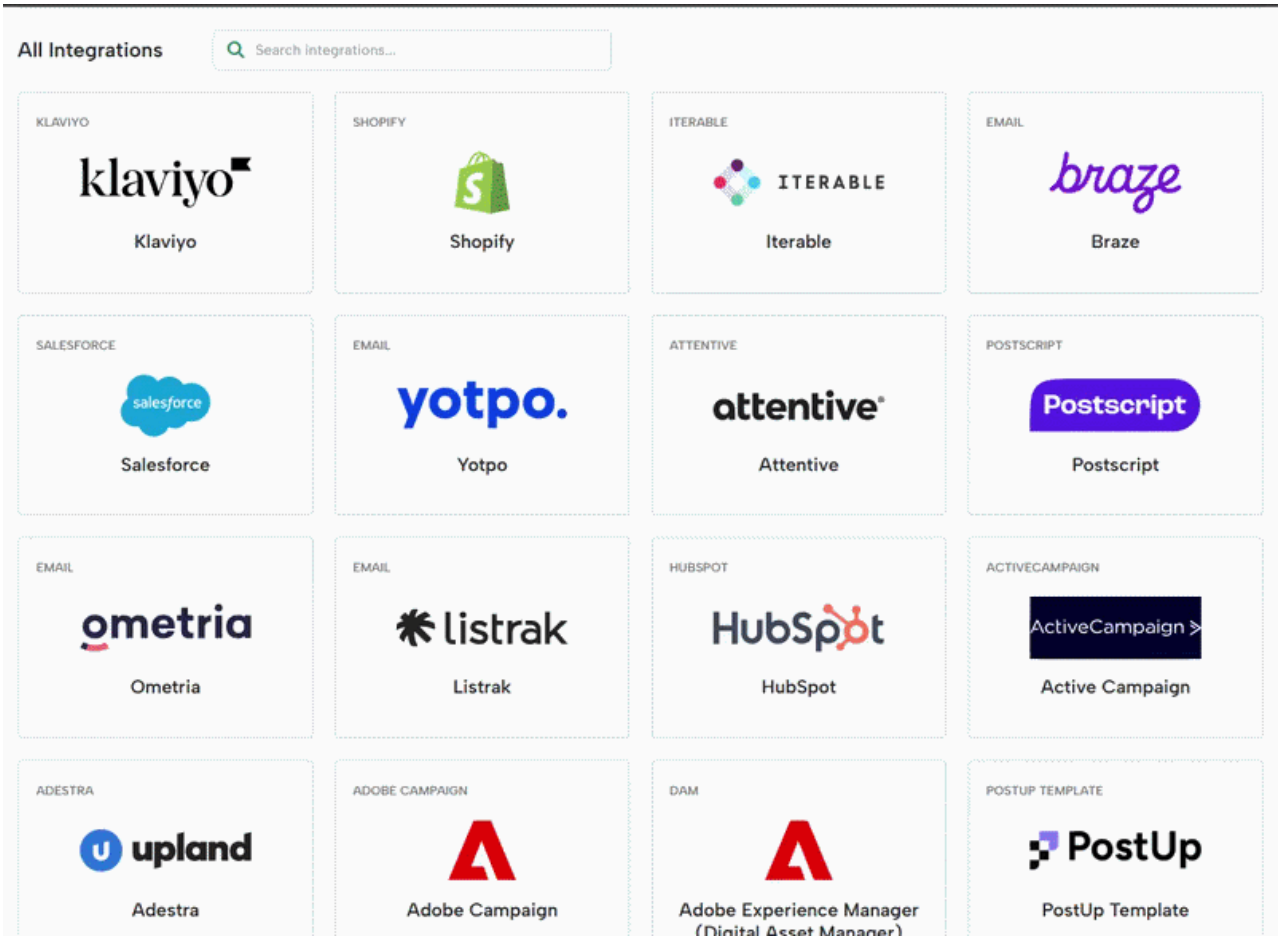
Integration Basics & Setup

Last Modified on 07/07/2026 1:51 pm EDT

In a nutshell, Digioh *Integrations* map Digioh form data into a format that can be sent to one of hundreds of third-party systems, like your email/SMS platform, CRM, CDP, BI systems, or really anything with a database. Integrations also store any API credentials securely on our server; these are never exposed to the Internet.



For all Digioh form submissions, data flows back to the Digioh server in a standard format. With an Integration which runs on the Digioh server, you can configure where this data is forwarded (i.e. an API endpoint) and how it is transformed (i.e. how Digioh data fields map to data fields in the 3rd party system). We provide hundreds of ready-to-go integration templates and tools to easily create new integrations for your custom in-house systems, if needed.



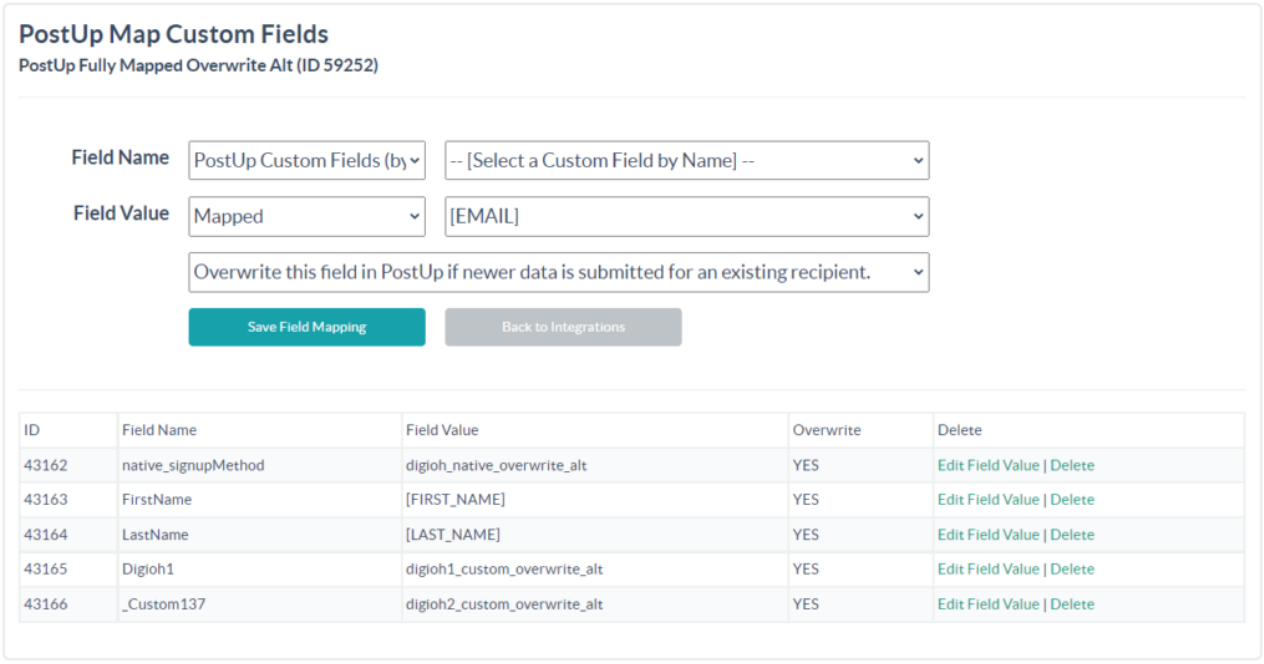
You can create any number of Integrations, which you can assign to any number of Digioh Campaigns, and Campaigns can have more than one Integration (e.g. for sending data to multiple 3rd party systems or subscribing to multiple email lists). Usually, for email signups you'll need a distinct Integration for each list where you want to add the email. For Campaigns with multiple Integrations assigned, they will run sequentially in the order shown. Integration order can be important when, for example, you need separate API calls to create an email record, then add it to a specific list.

If this sounds complicated, don't worry, we have many Integration templates that make this simple. Chances are that Digioh already has a turnkey Integration for your Email Platform (or other system).

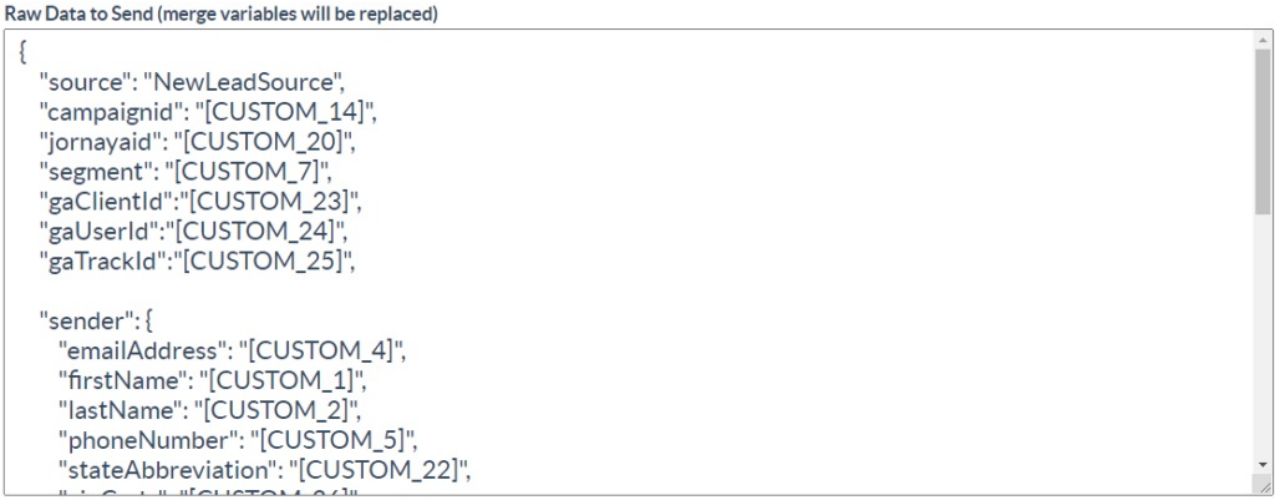
Integration Templates and Merge Tags

Generally, Digioh pre-built Integrations separate into two categories: Field Mapped and JSON template.

With field mapped, you add explicit mappings for each form field to a specific field in your system:



JSON templates are a bit more technical, and require you to edit JSON using Digioh *Merge Tags*:



When working with JSON, it's important to make sure that the syntax is valid. We recommend JSON Lint for validation.

Here's a complete list of all the Merge Tags you can use in your Integrations.

The Digioh team is happy to help you get this set up. Don't struggle! Just reach out to us at support@digioh.com.

Integration Security

Digioh Integrations are a means to pass information from the browser to your "end-platform" such as an ESP, CDP, or CRM. Usually, end-platforms require a secret API key to authenticate, so this must be provided to Digioh. Here's how we protect your keys:

- You enter the secret key when creating an Integration while logged into the Digioh HQ
- The Digioh HQ is secured by username, password with minimum complexity requirements, and

multi-factor verification every 30 days (by email).
- Secret keys are encrypted at rest on the Digioh Server, which is itself protected by Microsoft Cloud Defender (in Azure) and firewalls.
- Secret keys are **never** exposed on the client side (browser)
- We require that customers create a dedicated secret key exclusively for Digioh, if your end-platform supports that.

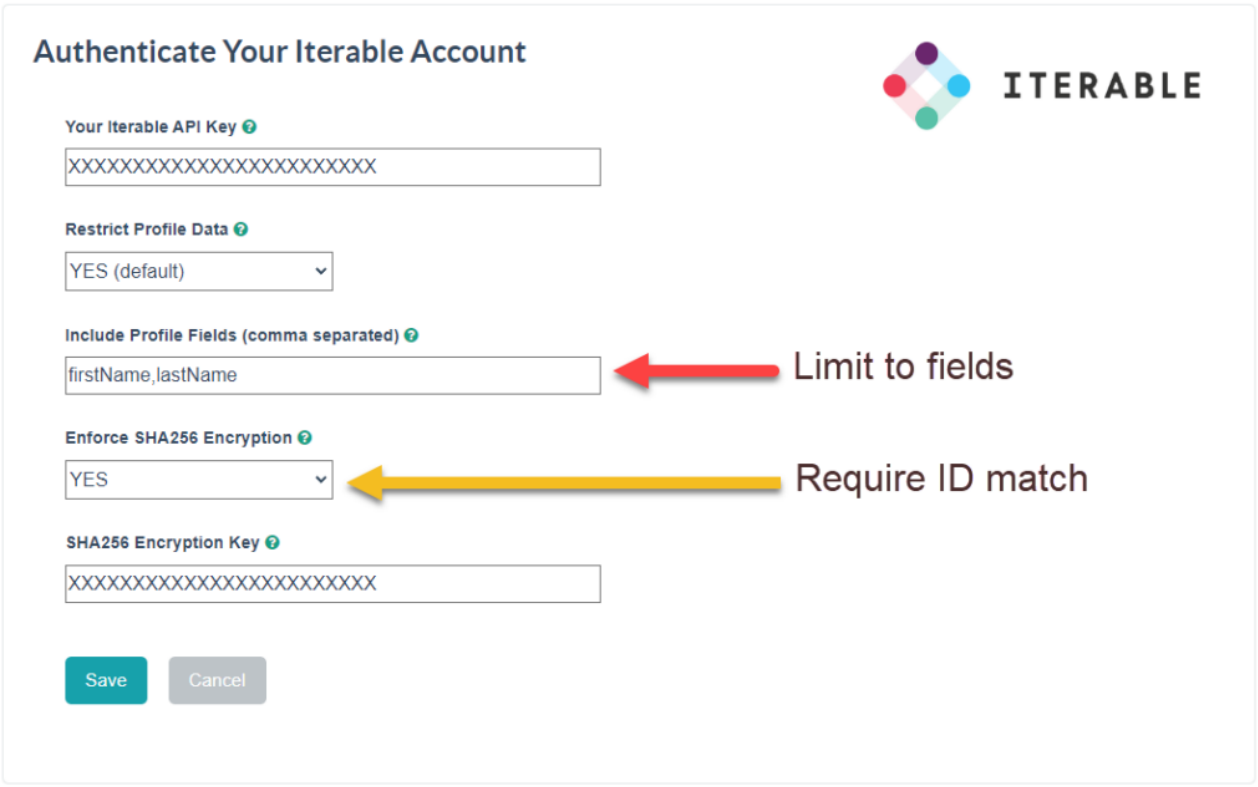
Digioh Integrations are the "middle men" between the (untrusted) browser and your end-platform. Here's how they protect your end-platform data:

- Integrations define the mapping of user input to stored data, so nothing more than the data fields you configure can be written to the end-platform via Digioh.
- They pass all input data through modern sanitization filters to prevent XSS and script-based database attacks.
- They use HTTPS, and TLS 1.2 at a minimum, to ensure data security in transit.
- Digioh endpoints are protected by Cloudflare CDN-level IP Rate Limiting and a Firewall, limiting damage if you come under attack.
- To prevent vandalism on a smaller scale vandalism, our server enforces Digioh Campaign / IP Rate limiting on form submissions

More information here: DDoS and Bot Protection

Some Integration use cases (e.g. preference centers and Targeting/Personalization) require two way data transfer, to and from the end-platform. If your end-platform supports it, you can enable additional data read security within Digioh:

- Identity authentication: when asking Digioh to read data for a specific email address, e.g. for preference centers, we authenticate that the requested email matches the encrypted email of the original requestor. The preference center must be accessed by a link that includes the email and the same email strongly encrypted. The encryption key is a shared secret between Digioh and the end-platform, so this prevents identity substitution attacks.
- Profile limiting: when used to read data, your API Key normally grants Digioh Integrations full access to the data associated with customer records in your end-platform. However, you can configure Integrations to limit the data passed back to the browser fields to only those necessary for the use case. For example, if your end-platform records contain sensitive information such as SSN or DOB, you can ensure that this information is never passed to the untrusted browser.



Finally, for Digioh customers in the EU, we provide an EU-based Digioh instance, so your customer data never leaves the EU while in transit.