Get data into Skyflow

Skyflow offers diverse options to easily get data into vaults, providing various ways to control data ingestion. You can seamlessly transfer data into vaults with Skyflow Studio or with APIs and SDKs. Vaults support multiple protocols and formats, ensuring compatibility with different systems and third-party service providers.

Skyflow simplifies data storage and workflows, enabling you to maximize the security of your data assets.

Client-side SDKs

Client-side SDKs are a secure way to manage sensitive data within your clients, including web or mobile applications. They shield your backend infrastructure from potential exposure to confidential information. When you use SDK-based forms to gather sensitive data, you can seamlessly ingest the data into the vault, generate tokens for the data, and send the tokens back to your client.

You can use client-side SDKs to collect data in the following ways:

- Build mobile apps using iOS and Android SDKs that collect sensitive data and store it in a vault.
- Use web apps developed with JS, React, and React Native SDKs to collect and insert data from front-end applications into your vault.
- Construct data collection interfaces with composable skyflow elements, where sensitive information bypasses your infrastructure entirely. This feature is useful for remaining PCI compliant.

Data APIs

Skyflow's Data APIs are the main way to interact with your vaults. They let you insert data directly enable backend integrations, SaaS app integrations, and analytics and warehousing solutions like Salesforce or Snowflake.

You can use Data APIs to perform the following integrations:

- Append data from pre-existing sources before inserting it into Skyflow using backend integration with server-side SDKs.
- Insert and tokenize data with analytics software like Snowflake, Databricks, and Big Query to apply User Defined Functions (UDFs) for invoking Skyflow REST APIs.
- Interact with third-party APIs using SaaS app integrations like Salesforce, Segment, and HubSpot. For example, to integrate with Salesforce, you can use Lightning Web Components and APEX code.
- Use existing tokens to import sensitive data and externally generated tokens into Skyflow. This feature is useful when migrating from an existing tokenization vendor or a locally developed system into Skyflow.

Connections and functions

Connections is an HTTPS gateway solution that you can use in two modes:

- **Inbound**: Inbound connections serve as an intermediary between your client and server.
- **Outbound**: Outbound connections bridge the integration between your backend server and a third-party service provider.

Functions execute custom logic with Node.js. When you invoke a connection, it runs your function and uses the Data APIs to insert data into the vault.

You can use connections and functions to apply the following solutions.

- Establish an inbound connection to tokenize sensitive data and send it to your server, preventing downstream services from handling the sensitive data. For instance, with a MuleSoft integration, you can use the Mule Skyflow Connector to tokenize sensitive data from payloads that pass through your API gateways.
- Tokenize responses from third-party payment service providers (PSPs) using outbound connections before forwarding them to your backend. For example, when requesting a new card number from Visa, the number can undergo tokenization within the vault before transmission to your backend system.
- Tokenize sensitive data in webhook events generated by third-party services. You can use inbound connections with API keys to tokenize the data into a vault before forwarding the event to your backend.

Pipelines

Pipelines enable batch workflows that securely transfer large volumes of sensitive data from a source system to a vault. Pipelines support the following features:

- **Data sources**: SFTP and S3
- **Data formats**: CSV, JSON, ACH, and METRO2

You can use pipelines to migrate data in the following ways:

- Migrate PCI data in bulk from existing PSPs to prevent PCI vendor lock-in.
- Tokenize data in Skyflow vaults when consuming ACH and METRO2 financial services files so that you don't expose your backend to any PCI data.
- Migrate PII data in bulk from existing customer data sources into a vault.
- Migrate PII data tokens from existing tokenization vendors.

Data migration

You can migrate data into Skyflow using one or more methods to streamline the process. By implementing a well-planned migration strategy, you can avoid disruptions, decrease risks, and maintain data integrity.

Migration considerations

Before you migrate your data, it's essential to have a clear understanding of your current system's dependencies and data flows. This knowledge helps you assess how future data usage and access roles may impact your migration strategy. By familiarizing yourself with different approaches, you can improve the success of your data transfer. Consider the following when planning your migration:

- Analysis of data sources
  - Identify the various data sources you want to collect and manage using Skyflow.
  - Understand the structure, format of the data, and the sensitivity of your data.
  - Map out how data flows within your organization. Identify the origin of data, trace its movement between systems, and evaluate secure storage or sharing locations.
- Compliance and data residency
  - Familiarize yourself with the relevant data protection (GDPR, CCPA, or PCI-DSS) and privacy regulations that apply to your industry.
  - Consider the regions where you store your data and where you'll need to store it in the future.
- Governance and roles
  - Identify your internal policies that govern the handling of sensitive information.
  - Define the roles and permissions you require to access and manage data within Skyflow. Decide who should have read, write, or administrative access to the data.
- Data management
  - Determine the internal and external applications and the systems interacting with Skyflow.
  - Assess your data encryption and tokenization strategy for the data you store in Skyflow.

How to migrate your data

When considering a data migration project, it's essential to identify which data you want to transfer, such as bringing your own data or bringing your own tokens. Understanding the source of your data or tokens, such as third-party ownership or direct ownership, is also crucial. The following table outlines how you can migrate your data.

Note: You can perform each method in parallel if you're transitioning from one system to another or if you instantly need to switch from an old system to Skyflow.

Method	Description
Parallel	Skyflow inserts new data into the vault while keeping the old data updated. Post-migration, both systems receive updates until the process is complete. After you verify your vault is operational, the old system is deactivated or shut down.
Divisible by business criteria (Product lines, business units, or regions)	A phase migration that moves data into Skyflow by a specific division of data.
Trickle approach	Skyflow accepts new data while historical migration of existing data occurs post-implementation. The need to migrate historical data lessens over time, enabling upsert to update new data in Skyflow.
Multiple migrations for data cleansing	Data is migrated into Skyflow and cleansed using upsert.
Bulk all at once (Big bang)	You can use the Bulk API to transfer large volumes of data from your legacy system into Skyflow.

Next steps

Skyflow offers secure data migration to privacy vaults using client-side SDKs, APIs, and custom integrations. Our team analyzes your data landscape, compliance needs, and policies to ensure a strategic migration, minimizing risks and maximizing value. Explore what Skyflow can do, learn more about data governance, or familiarize yourself with tokenization and compliance.