Migration Guide: UPGRADING from Accertify to Sift

A Step-by-Step Guide to Implementing AI-Powered Fraud Decisioning

Proven Science & Scalability with AI-Powered Digital Fraud Decisioning

As your business grows and digital risk operations scale, sustaining early-stage performance becomes increasingly difficult. Static rules and point solutions lead to an over-reliance on manual review, taking a massive toll on efficiency and security.

Sift eliminates the need for optimized static rulesets, and doesn't require weeks to months of waiting for models to analyze signals and adapt. Instead, Sift continuously ingests your unique business data, instantly adapting custom models to protect your users and revenue.

Our AI-powered platform also incorporates all analyst decisions across our entire customer base, directly informing the global model. Decisions made by your own fraud team help to fine-tune your custom model, tailoring it precisely to your specific circumstances, company size, and level of risk.

Sift's intuitive Console also delivers advanced digital risk decisioning, improving analyst productivity and accuracy by highlighting different areas to focus on when performing an investigation.

Rather than processing multiple conflicting scores that require fraud analysts to jump from page to page in a digital scavenger hunt, Sift surfaces clear, user-deep risk signals. Coupled with advanced link analysis and bulk decisioning capabilities, Sift helps fraud teams turn risk operations into a scalable, secure revenue center.

Below, we've laid out the platform migration process step-by-step, so you can be prepared for an easy and effective transition to an AI-powered solution.

Integration overview

Sift's integration is flexible and easy to understand, and our documentation is all available on our website. There are four main components:

1 **JS snippet (FE)**
Used to capture device and IP

2 **Mobile SDK (FE)**
Designed to capture device and app

3 **Rest API events (BE)**
Captures interaction along the user journey (logins, transactions, orders, account updates)

4 **Decisions (BE)**
Ingests feedback to customize ML models

Our team of Integration Consultants specialize in getting customers up and running with Sift. They'll walk you through the below five steps to ensure you're set up for success, while our Solutions Engineers will provide technical expertise, industry guidance, and platform strategy for the duration of your post-implementation lifecycle.

Step 1

Digital Risk Assessment

Using our Digital Risk Assessment, Sift's expert Trust and Safety Architects will help you create a fraud prevention and mitigation strategy that's built to perform at scale. This workshop is designed to align risk and revenue considerations throughout your organization, enabling a holistic approach that grows with your business and supports its specific needs.

Step 2

Designing Your Integration

Sales Engineers will work with you to design a custom integration. This includes any data points you'll need to send to Sift, as well as which actions will get a Score or Workflows request. If you're implementing MFA for the first time, we'll help map out the solution that works best.

Step 3

Building and Testing

During this phase, your team will implement the Sift integration on your end and test it out within the sandbox environment, otherwise known as a software testing environment, test server, development server, or working directory. This enables the isolated execution of software or programs for independent evaluation, monitoring, and testing. We will need to feed production data from your site into the sandbox environment to ensure we're testing your system exactly.

Step 4

Model Training

Within the model training, the most critical rules will be included in the migration. Our team of Trust and Safety Architects, Customer Success Managers, and Customer Onboarding Managers can help you determine what should and shouldn't stay in place.

Once testing in the sandbox environment is complete, we'll push the data into Sift's production environment. At this stage, you'll work with us to make decisions that will improve the live learning and your custom models.

Step 5

Going Live

Once your custom model has been trained, we can begin automating score thresholds based on your unique goals.

Fraud Prevention Rules: To Keep or Not to Keep?

When switching to Sift, you can choose to do one of the following:

1 Remove all rules and rely only on the Sift Score for automated decisions.

2 Migrate a selection of effective rules into Sift Workflows.

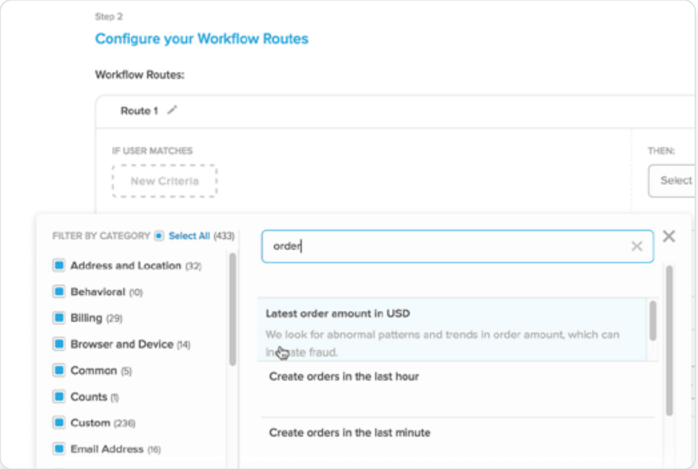
Sift exposes thousands of signals that can be leveraged in rules. If you're using specific rules in your legacy solution today that you'd like to continue using, chances are we can support them.

Both options are good ones, and it's up to you to decide whether you'd like to start from scratch or keep some of your most successful rules in place.

Preparing to Launch

Before you make final decisions about existing rules, review them with your trust and safety team to gather context. It's common to migrate from Accertify with a large amount of rules, and you may be left wondering how you should decide which rules are most important. Ask straightforward questions and seek clear answers:

1. *Why was the rule put in place?*
2. *Who created it?*
3. *Is it still helping more than hindering?*
4. *Do we want to think about this rule and its function differently?*



Step 2

Configure your Workflow Routes

Workflow Routes:

Route 1

order

Latest order amount in USD

We look for abnormal patterns and trends in order amount, which can indicate fraud.

Create orders in the last hour

Create orders in the last minute

Examples of rules worth examining include:

- **Order amount thresholds.** At what amount should high-value transactions be flagged? When, and what are the exceptions?
- **Velocity rules.** These are key to detecting emerging, rapid attacks by measuring velocity on details like login attempts, payment account, device and more—but how are they impacting order acceptance rates for legitimate users?
- **Product-specific rules.** Should you apply thresholds to specific products or services that are commonly targeted by bad actors? What data can support how these rules are built?
- **List-based rules.** Creating negative or positive lists to reference in rule sets speeds up the process, but a lack of consistency and organization can quickly become a bottleneck. How will your team keep lists up to date and curated?
- **Flexibility with MFA and Security Notifications.** Leverage Sift's Authentications service for prompting MFA and Security Notification responses from your customers. What rules are currently in place to defend accounts from ATO?

Sift will walk you through this exercise, and help to determine any data points necessary to remove a current rule. We'll also help your risk team figure out where those insights need to come from, and who needs to monitor the change.

Because of the accuracy of the Sift Score, you can rely on fewer rules and make operations much more manageable. Here are some things to consider:

Option 1

Starting fresh

If you decide to remove all existing rules and start fresh with Sift, your Account Manager and Sales Engineer will be there to help, providing best practices and advice for your company's unique needs, the markets you operate in, and the size of your customer base.

Every customer also becomes a member of our global Sifters Community, where your team can connect 1:1 with in-house risk and product experts, knowledge-share with industry peers, and access exclusive educational resources and Workflow Templates.

Option 2

Migrating successful rules

If you'd like to keep some of your existing rules, we'll take the following steps:

1. During the integration design process, we'll request that you send the rules you'd like to keep to your Sales Engineer. This will ensure that we correctly capture all data points and can effectively run these rules in Sift Workflows.
2. While the integration is taking place, your Account Manager and Sales Engineer will hold conversations with your company's team of fraud analysts to determine which rules and watchlists are the most important ones to import to Sift.
3. After the integration is complete, your AM and SE will train your fraud analysts on how to import existing rules into Sift Workflows. During the Sift Console training, your fraud analysts will input some of the high-priority rules into the Workflow with assistance from your AM and SE.

Contact us

To learn more about migrating from Accertify to Sift, or if you have any outstanding questions, please schedule time with us.