Knowledge Base: Anura Best Practices

Welcome to Anura! Ready to crush ad fraud?
Here are some best practices to help you get started.

Step 1: Select Anura Script or Anura Direct

We recommend clients use Anura Script whenever possible because it collects more data, enabling us to find more sophisticated (SIVT) levels of fraud and beyond. Anura Script can be found here. For a faster than one second response time use Anura Direct, which can be found here.

Step 2: Complete Integration

All the information needed to integrate Anura's Script and Direct solutions, Anura's Reporting API, and our connected partners can be found in Anura Docs.

After integration is complete, we recommend enabling Domain Locking to secure your instance ID, which prevents others from using it. With Anura Script, we can lock down your domain. With Anura Direct, we can lock down to your server IP address(es). Once you're set up and configured, send an email to Support, and we'll put those safeguards in place.

Step 3: Enter Monitoring Mode

Our goal is to first identify how much fraud you're dealing with before making any real-time decisions. We don't want to cripple your business by shutting off a majority (or all) of your traffic. Therefore, we recommend clients go into Monitoring Mode.

Focus on separating traffic into Source (where the traffic is coming from) and Campaign (where the traffic is going) variables to pass on to Support. Source variables can include publisher ID, affiliate ID, etc., and campaign variables can be client ID, campaign ID, etc. By passing along the variables to us, we can help you granularly identify the good, warning, and bad source(s) of traffic.

Good. You'll want more of these sources of traffic.

Warning. These sources are what we consider in between traffic. You're going to zero in on them using our Dashboard and work with them to reduce fraud.

Bad. These are the sources that need to be surgically removed because all they're doing is hurting your network. Some clients redirect bad traffic to a 404 page, others tag the form as bad, and if you're dealing with credit card transactions, you don't process them to keep your fraud rate down. How you choose to handle bad traffic is entirely up to you.

Why Monitor?

You may have 5-10% fraud and think that isn't a lot of fraud. However, you may have certain campaigns, clients, or advertisers that are being targeted, and discover 70-80% fraud going to them. Monitoring will enable you to catch the fraud and stop it before the client chargebacks or cancels on you.

How Long Does Monitoring Mode Last?

It's subjective and depends on the client. Once you get down to an acceptable level and are ready to make real-time decisions then you can begin actively blocking.

Anura detects bad traffic, it doesn't block bad traffic. By providing you with the data to help you decide which sources of traffic to eliminate and how to remove them, you'll be opening up resources (e.g. band budget) to obtain better traffic.

Step 4: Rinse & Repeat

Pick a time frame and focus where you are at with fraud and cut it in half while maintaining/growing your overall traffic volume. Once you reach that goal, rinse and repeat.

As you surgically remove bad traffic, you'll see a lift in performance, reflected in the metrics you're tracking, and an increase in client demand. This is how we help grow companies like Digital Media Solutions.

For additional questions on best practices, contact Support.