cleartrust

SafeAPI

Blocking Invalid and Fraudulent Traffic in Real Time

V3.1

cleartrust

Table of Contents

Introduction 3
- Purpose 3
- About the API 4
- Traffic Quality Scoring 4

Integration 5
- API Request Endpoint 5
  - 1st endpoint 5
  - 2nd endpoint 5
- Returns 5

Sample Call 5
- API Response (JSON) 6
- Success 6
- Error 6
- Fraud 6
- Sample API Call 7
  - Macros 7
  - Suggested Macros 7
- Sample API Call with dummy values 8
  - Web (with GAID) 8
  - App (with IDFA) 8
  - Notes on Macros 8

cleartrust

Introduction

ClearTrust introduces a cutting-edge fraud detection platform designed to assist AdOps teams in identifying and combating Ad Fraud / Invalid Traffic instantly, while also providing insights into the risks within their traffic. It encourages a proactive approach within the digital advertising landscape by advocating for the use of ClearTrust's secure solutions.

The SafeAPI by ClearTrust is integrated through a REST S2S API, dubbed the ClearTrust SafeAPI. This tool enables transparent, real-time monitoring and risk classification using APIs in real-time. It empowers platforms to analyze traffic according to filter preferences and implement optimization strategies.

Purpose

This document is designed to facilitate your team's effortless integration of this solution into your websites/apps, enabling you to begin measuring traffic risks in real-time. Utilizing Cleartrust's extensive fraud detection filters, this solution categorizes traffic into high, medium, and low-risk levels.

Following the measurement and classification of traffic, insights and reports are accessible through a real-time dashboard and, if required, a reporting API endpoint.

cleartrust

About the API

It is an API solution that offers transparent measurement of the traffic as it comes, with detailed classifications. The traffic is analyzed in real-time and a score between 0 to 3 is returned. This score can be used to make business decisions in real-time, for example, blocking on a score of 1 (High Risk), or allowing on a score of 0 (Clean).

Traffic Quality Scoring

ClearTrust scores the event (click or a page/app view or a bid request) based on the filters configured in the system. Every customer is assigned a business id and this id can configure a set of filters for scanning. The configuration of filters is available in the ClearTrust dashboard console under the Threat Control Center. These filters can be switched on / off and tweaked to achieve the exact traffic quality needed for the advertisers.

ClearTrust also offers the following types of advanced filter settings

- **Global filter settings**

Applicable to the traffic going to all advertisers

- **Advertiser specific filter setting**

A set of filters is enabled for only a specific advertiser and multiple advertisers can have different filter settings

- **Publisher / Affiliate / Supply specific filter setting**

A set of filters is enabled for only a specific supplier and multiple suppliers can have different filter settings

cleartrust

Integration

API Request Endpoint

There are two available endpoints. The API requester can choose one of them, based on performance.

1st endpoint

`https://api-pw.fst.onl/tinycode`

2nd endpoint

`https://api-pe.fst.onl/tinycode`

tinycode = ClearTrust Tiny Code
This value would be provided in your console, or provided by the relationship manager.

Returns

Traffic Quality Score and Reason Code (The Filter Code is specified in the Reason Code)

Sample Call

https://api-pw.fst.onl/tinycode?ip=49.207.233.107

Based on this traffic quality score , the API requester can either allow , drop or redirect the click / event.

cleartrust

API Response (JSON)

https://api-pw.fst.onl/**tinycode**?ip=49.207.233.107

Returns both traffic quality score and reason code (Filter code)

Success
{"tqs":{"score":0,"reason":"CL"}}

Error
{"tqs":{"score":-1,"reason":"ERR"}}

Fraud
{"tqs":{"score":1,"reason":"BN"}}

Traffic Quality Score is a value between 0, 1 to 3 or -1

1 = **High Risk Traffic**
2 = **Medium Risk Traffic**
3 = **Low Risk Traffic**
-1 = **Error**
0 = **Clean Traffic**

cleartrust

Sample API Call

```
https://api-pw.fst.onl/ctnp1LSD5tLS?cid=CIDMACRO&ip=4
9.207.233.107&s1=S1MACRO&s2=S2MACRO&s3=S3MACRO&s4=S4MACRO&s5=S5MACRO&s6=S6
MACRO&s7=S7MACRO&s8=S8MACRO&s9=S9MACRO&s10=S10MACRO&s11=S11MACRO
```

Macros

You can leverage macro support to send in additional information. The optional macros help Cleartrust to generate reports and in some cases apply more filters.

Suggested Macros

Mandatory macros are needed in every API call.

S.No	Parameters (case sensitive)	Mandatory (M) / Optional (O)	Description	Default
1	tinycode	M	ClearTrust Tiny Code	Provided by ClearTrust
5	Ip	M	IP Address (v4/v6)	None
6	cid	M	Request ID	CIDMACRO
7	s1	O	Publisher ID / Source ID	S1MACRO
8	s2	O	Sub Publisher/ Sub ID	S2MACRO
9	s3	M (for Web)	Referer Domain	S3MACRO
10	s4	M (for App)	App Bundle	S4MACRO
11	s5	M (for App)	App Version	S5MACRO
12	s6	M	User Agent	S6MACRO
13	s7	O	Geo City	S7MACRO
14	s8	O	XFF/ Query	S8MACRO
15	s9	O	Device ID	S9MACRO
16	s10	O	GAID	S10MACRO
19	s11	O	IDFA	S11MACRO

cleartrust

Sample API Call with dummy values

Web (with GAID)

```
https://api-pw.fst.onl/ctnp1LSD5tLS?cid=19819383&ip=3
1.13.127.18&s1=10001&s2=20001&s3=www.geniee.jp&s4=S4MACRO&s5=S5MACRO&s6=Mozilla%
2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%29%20AppleWebKit%2F537.36%20%
28KHTML%2C%20like%20Gecko%29%20Chrome%2F42.0.2311.135%20Safari%2F537.36%20Edge%2
F12.246&s7=tokyo&s8=31.13.127.18,70.41.3.18&s9=12345678-1234-1234-1234-
1234567890AB&s10=a3c5fde82f234907b9bed958f0d6bd69&s11=S11MACRO
```

App (with IDFA)

```
https://api-pw.fst.onl/ctnp1LSD5tLS?cid=19819383&ip=3
1.13.127.18&s1=10001&s2=20001&s3=S3MACRO&s4=com.myexample.app&s5=1.5.3&s6=
Mozilla%2F5.0%20%28iPhone%3B%20CPU%20iPhone%20OS%2013_2_3%20like%20Mac%20
OS%20X%29AppleWebKit%2F607&s7=tokyo&s8=31.13.127.18,70.41.3.18&s9=12345678-
1234-1234-1234-1234567890AB&s10=S10MACRO&s11=AEBE52E7-03EE-455A-B3C4-
E57283966239
```

Notes on Macros

Macros such as Referrer Domain are mandatorily needed , when a pre-bid request is being verified for desktop open web inventory.

Macros such as AppBundle / Version are mandatorily needed, when a pre-bid request is being verified for mobile inventory

Macros of Device ID, GAID, IDFA are preferred when a pre-bid request is being verified for mobile inventory.

CIDMACRO can be used for sending in the pre-bid request ID.