cleartrust

Post Bid Measurement

Monitoring and Blocking for Invalid Traffic

V2.9

cleartrust

Table of Contents

Introduction 3
Purpose 3
Integration 4
Monitoring Only 5
Code 5
Macros 5
Monitoring with Blocking 7
Code 8
Macros 9
Monitoring, Blocking and Authentication 10
Blocklists 11
IP Blocklists 11
Domain Blocklists 11

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 Post bid solution by ClearTrust is deployed through a JavaScript pixel technology, dubbed the ClearTrust SafePixel. This tool enables transparent, real-time monitoring and risk classification of web traffic. It empowers you to analyze your traffic according to your preferences and implement optimization strategies effectively..

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

Integration

You can activate this measurement by incorporating the specified one-line JavaScript tag. This approach keeps your code organized and avoids the need for multiple script tags, making the setup process easy.

There are three ways this measurement can be leveraged.

- **Only Monitoring**
- **Monitoring and Blocking**
- **Monitoring , Blocking and Authentication**

cleartrust

Monitoring Only

Using this mode, the following tag can only monitor the traffic quality score. This tag is to be pasted before the end of <head> tag

Code

```
<script id='_ctbase' src="https://admd.ink/js/spsm.min.js?ak=AUTHKEY
&tc=TINYCODE&tty=IMPR&dg=0&ci=1&gv=1&s1=S1MACRO&s2=S2MACRO&s3=S3MACRO&
s4=S4MACRO&s5=S5MACRO&s6=S6MACRO&s7=S7MACRO&s8=S8MACRO&s9=S9MACRO&s10=
S10MACRO"/></script>
```

This code uses macros which can be leveraged for reporting and analysis.

Macros

The following macros are suggested as mandatory and optional

S.No	Parameters (case sensitive)	Mandatory (M) / Optional (O)	Description	Default
1	ak	M	Auth Key	Provided by CT
2	tc	M	Tiny Code	Provided by CT
3	s1	O	Publisher ID Placeholder	Pub Macro / Pub ID
4	s2	O	Sub Publisher Placeholder	Sub Pub Macro / Sub ID
5	utm_source	O	UTM Source Placeholder	Source URL
6	s4	O	s4	Custom Macro
7	s5	O	s5	Custom Macro
8	s6	O	App Bundle Id Placeholder	App Bundle Id
9	utm_campaign	O	UTM Campaign Placeholder	Campaign Id
10	s8	O	s8	Custom Macro
11	s9	O	Creative Id Placeholder	Creative Id
12	s10	O	s10	Custom Macro
13	s11	O	Advertiser Placeholder	Advertiser
14	s12	O	Click id Placeholder	Click Id

15	s13	O	Keyword placeholder	Medium
16	utm_medium	O	UTM Medium Placeholder	Custom Macro
17	utm_content	O	UTM Content Placeholder	Content
18	utm_term	O	UTM Term Placeholder	Term
19	s17	O	Site Id Placeholder	Site Id
20	s18	O	s18	Custom Macro
21	s19	O	s19	Custom Macro
22	s20	O	s20	Custom Macro

cleartrust

Monitoring with Blocking

This mode, designed for monitoring and blocking, consists of a single-line JavaScript tag featuring a callback function. This script can be easily incorporated into any existing JavaScript you may already have in use.

Upon execution, this tag communicates a Traffic Quality Score to a specified callback function (bqswitch), located at the start of the wrapper code in the subsequent section.

This callback function provides the flexibility to tailor the application's response based on the received score. For instance, a score of 1, signaling Non-Human traffic, might prompt the action to divert this traffic to either a blank or sink page.

The system can return score values ranging from 0 to 3, with -1 indicating an error.

- **0: Clear traffic**
- **1: High Risk**
- **2: Medium Risk**
- **3: Low Risk**
- **-1: Points to an Error**

Each score category is associated with specific traps, which can be customized via the ClearTrust panel. For example, achieving a Non-Human traffic score may involve the identification of traps such as Data Centers, Emulators, or Fake Devices.

cleartrust

Code

```
<!-- Cleartrust SafePixel STARTS -->
<script type="text/javascript">

function __bqswitch(bqprms)
{

      var _bqs = String(bqprms[0]);
      switch(_bqs)
      {
      case "0":
      console.log("zero");
     // Action for clean traffic
      break;

      case "1":
      console.log("one");
     // Action for HighRisk traffic
      break;

      case "2":
      console.log("two");
     // Action for MediumRisk traffic
      break;

      case "3":
      console.log("three");
     // Action for LowRisk traffic
      break;

      case "-1":
      console.log("error");
     // Action for Error response
      break;


      }
            }


</script>


<script id='_ctbase'
src="https://admd.ink/js/spsb.min.js?ak=AUTHKEY&tc=TINYCODE&tty=IMPR&
dg=0&ci=1&gv=1&s1=S1MACRO&s2=S2MACRO&s3=S3MACRO&s4=S4MACRO&s5=S5MACRO
&s6=S6MACRO&s7=S7MACRO&s8=S8MACRO&s9=S9MACRO&s10=S10MACRO"/></script>


<!-- Cleartrust SafePixel API ENDS -->
```

cleartrust

Macros

The following macros are suggested as mandatory and optional

S.No	Parameters (case sensitive)	Mandatory (M) / Optional (O)	Description	Default
1	ak	M	Auth Key	Provided by CT
2	tc	M	Tiny Code	Provided by CT
3	s1	O	Publisher ID Placeholder	Pub Macro / Pub ID
4	s2	O	Sub Publisher Placeholder	Sub Pub Macro / Sub ID
5	utm_source	O	UTM Source Placeholder	Source URL
6	s4	O	s4	Custom Macro
7	s5	O	s5	Custom Macro
8	s6	O	App Bundle Id Placeholder	App Bundle Id
9	utm_campaign	O	UTM Campaign Placeholder	Campaign Id
10	s8	O	s8	Custom Macro
11	s9	O	Creative Id Placeholder	Creative Id
12	s10	O	s10	Custom Macro
13	s11	O	Advertiser Placeholder	Advertiser
14	s12	O	Click id Placeholder	Click Id
15	s13	O	Keyword placeholder	Medium
16	utm_medium	O	UTM Medium Placeholder	Custom Macro
17	utm_content	O	UTM Content Placeholder	Content
18	utm_term	O	UTM Term Placeholder	Term
19	s17	O	Site Id Placeholder	Site Id
20	s18	O	s18	Custom Macro
21	s19	O	s19	Custom Macro
22	s20	O	s20	Custom Macro

Monitoring, Blocking and Authentication

This mode is a 2 step process typically used when there is a stop page on which the cleartrust javascript tag is placed and there is one more page where additional verification is done, before sending the user to the advertisers page.

The code to be used for this mode is same as the previous section

Step 1
A unique session id is returned in the javascript callback in the bqprms variable. It's expected that this session id is preserved. This step is executed on the first stop page.

The session id is returned in the parameter `bqprms[2]`

Step 2
This session id is verified using our session authentication API endpoint. This is executed on the next page.

The session authentication API endpoint is
https://rapidapi.cleartrust.app/api/apigw.php?bizid=12345&apicode=VALCHECK&token=<sessionid>&dimname=ac&dimvalue=abcd1234

Response values
0 if the key is not found
Traffic quality score of the session ID.

Blocklists

The system also generates blocklists of bad IPs and referrer domains which can be leveraged in the infrastructure to block traffic in real time at your end. These blocklists can be automated to a S3 bucket or a custom SFTP location with a daily upload frequency.

The blocklists comprise of

IP Blocklists

List of invalid, tampered and fraudulent IP Addresses (both IPV4 and IPv6)

Domain Blocklists

List of referrer domains which are either erroneous, sources of fraudulent and invalid traffic etc.

To enable these blocklists for your account, please get in touch with your respective account manager.