

Bot Feedback Loop



- [Availability](#)
 - [False Positive](#)
 - [False Negative](#)
 - [Subtypes](#)
 - [Submit a report](#)
 - [Via the API](#)
 - [Create a feedback report](#)
 - [List feedback reports](#)
 - [API Fields](#)
 - [Expression fields](#)
 - [Recommendations when submitting a report](#)
 - [Recommendations after submitting a false positive](#)
 - [Recommendations after submitting a false negative](#)
-

```
import { GlossaryTooltip, Steps, DashButton } from "~/components";
```

The Bot Feedback Loop allows you to report requests that Bot Management scored incorrectly. When you submit a false negative or false positive report, Cloudflare analyzes the data and uses it to train the next machine learning model.

Availability

Bot Feedback Loop is available for Enterprise Bot Management customers. Visit [Plans](#) for more information.

False Positive

A false positive can happen if Cloudflare scores a request from a person using a browser, mobile application or desktop application in the *automated* or *likely automated* range.

False Negative

If Cloudflare is unable to detect a portion of automated traffic on your site, submitting a False Negative report will help us catch it in the future.

Subtypes

Subtype	Definition
Account Creation Abuse	The automated creation of many new accounts in order to gain access to site resources.
Ad Fraud	Fraudulent increase in the number of times an advertisement is clicked on or displayed.
Credit Card Abuse	Attempts to repeatedly validate many credit card numbers or the same credit card number with different validation details.
Cashing Out	Abusing the target Internet application to obtain valuable goods.
Login Abuse	Attempts to gain access to a password protected portion of an Internet application using many different combinations of usernames and passwords.
Inventory Abuse	Automated abuse related to purchasing limited stock inventory or holding inventory to prevent others from making transactions.
Denial of Service	Automated requests with the intent of exhausting server resources to prevent the Internet application from functioning.
Expediting	Automating the use of an Internet application to make transactions faster than a human visitor to gain unfair advantage.
Fuzzing	Finding implementation bugs through the use of malformed data injection in an automated fashion.
Scraping	Automated retrieval of valuable or proprietary information from an Internet application.
Spamming	The abuse of content forms to send spam.
Token Cracking	Identification of valid token codes providing some form of user benefit within the application.

Subtype	Definition
Vulnerability Scanning	Systematic enumeration and examination of identifiable, guessable and unknown content locations, paths, file names, parameters, to find weaknesses and points where a security vulnerability might exist.

Submit a report

1. In the Cloudflare dashboard, go to the **Security Analytics** page.

```
<DashButton url="/?to=:account/:zone/security/analytics" />
```

2. Apply one or more filters.
3. Under **Request activity**, filter by **Bot analysis**.
4. Select **Report incorrect data** and fill out the form.
5. Select **Submit**.

Via the API

Create a feedback report

```
curl 'https://api.cloudflare.com/client/v4/zones/{zone_id}/bot_management/feedback' \
--header "X-Auth-Email: <EMAIL>" \
--header "X-Auth-Key: <API_KEY>" \
--header "Content-Type: application/json" \
--data '{
  "type": "false_positive",
  "description": "Legitimate customers having low score",
  "expression": "(cf.bot_management.score le 46 and ip.src.asnum eq 132892 and http.host eq
\"api-discovery.theburritobot.com\" and cf.bot_management.ja3_hash eq
\"3fed133de60c35724739b913924b6c24\")",
  "first_request_seen_at": "2022-08-01T00:00:00Z",
  "last_request_seen_at": "2022-08-10T00:00:00Z",
  "requests": 100,
  "requests_by_score": {
    "1": 50,
    "10": 50
```

```

},
"requests_by_score_src": {
  "heuristics": 25,
  "machine_learning": 75
},
"requests_by_attribute": {
  "topIPs": [
    {
      "metric": "10.75.34.1",
      "requests": 100
    }
  ],
  "topUserAgents": [
    {
      "metric": "curl/7.68.0",
      "requests": 100
    }
  ]
}
}'

```

List feedback reports

```

curl 'https://api.cloudflare.com/client/v4/zones/{zone_id}/bot_management/feedback' \
--header "X-Auth-Email: <EMAIL>" \
--header "X-Auth-Key: <API_KEY>"

```

```

[
  {
    "created_at": "2022-08-19T00:05:24.749712Z",
    "type": "false_positive",
    "description": "Legitimate customers having low score",
    "expression": "(cf.bot_management.score le 46 and ip.src.asnum eq 132892 and http.host eq \"api-discovery.theburritobot.com\" and cf.bot_management.ja3_hash eq \"3fed133de60c35724739b913924b6c24\")",
    "first_request_seen_at": "2022-08-01T00:00:00Z",
    "last_request_seen_at": "2022-08-10T00:00:00Z",
    "requests": 100,
  }
]

```

```
{
  "requests_by_score": {
    "1": 50,
    "10": 50
  },
  "requests_by_score_src": {
    "heuristics": 25,
    "machine_learning": 75
  },
  "requests_by_attribute": {
    "topIPs": [
      {
        "metric": "10.75.34.1",
        "requests": 100
      }
    ],
    "topUserAgents": [
      {
        "metric": "curl/7.68.0",
        "requests": 100
      }
    ]
  }
}
```

API Fields

Field	Type	Description	Value Example
type	string	The feedback report type.	false_positive
description	string	The feedback report description with more details on the issue.	Legitimate customers having low scores.
expression	string	The wirefilter expression matching reported requests.	(cf.bot_management.score le 46 and ip.src.asnum eq 132892 and http.host eq "app.example.com" and cf.bot_management.ja3_hash eq "3fed133de60c35724739b913924b6c24")

Field	Type	Description	Value Example
first_request_seen_at	string	The time range start when the first request has been seen, RFC 3339 format.	2022-08-01T00:00:00Z
last_request_seen_at	string	The time range end when the last request has been seen, RFC 3339 format.	2022-08-10T00:00:00Z
requests	integer	The total number of reported requests.	100
requests_by_score	object	The requests breakdown by score.	See example below.
requests_by_score_src	object	Requests breakdown by score source.	See example below.
requests_by_attribute	object	Requests breakdown by attribute (optional).	See example below.

requests_by_score

```
{
  "1": 50,
  "10": 50
}
```

requests_by_score_src

```
{
  "machine_learning": 75,
  "heuristics": 25
}
```

requests_by_attribute

```
{
  "topIPs": [
    {
      "metric": "10.75.34.1"
      "requests": 100
    }
  ],
  "topUserAgents": [
    {
      "metric": "curl/7.68.0",
```

```
{
  "requests": 100
}
```

Expression fields

Field	Type	Description
<code>cf.bot_management.ja3_hash</code>	string	This provides an SSL/TLS fingerprint to help you identify potential bot requests.
<code>cf.bot_management.score</code>	integer	This represents the likelihood that a request originates from a bot using a score from 1-99.
<code>http.host</code>	string	This represents the hostname used in the full request URI.
<code>http.request.uri.path</code>	string	This represents the URI path of the request.
<code>http.user_agent</code>	string	This represents the HTTP user agent which is a request header that contains a characteristic string to allow identification of the client operating system and web browser.
<code>ip.src.asnum</code>	integer	This represents the 16- or 32-bit integer representing the Autonomous System (AS) number associated with client IP address.
<code>ip.src.country</code>	string	This represents the 2-letter country code in ISO 3166-1 Alpha 2 format.
<code>ip.src</code>	string	The source address of the IP.

Recommendations when submitting a report

When you submit a report, use the filters available in the Bot Analytics dashboard to ensure that your report includes only the traffic that received an incorrect score. In addition to filtering by a score (required), you may want to filter by user-agent, IP, ASN or JA3 to more precisely highlight the section of traffic that was scored incorrectly.

If you are not certain if some traffic received an incorrect score, keep this traffic in the report.

We appreciate any comments you wish to leave in the description field that might help our team better understand these requests in the context of typical traffic to your domain.

Recommendations after submitting a false positive

:::note The instructions below apply to Enterprise subscription with Bot Management only. :::

After submitting a false positive, you can explicitly allow the traffic if you are confident that this traffic source cannot be used for abuse in the future. To allow traffic, you can create a WAF custom rule with a [Skip the remaining custom rules](#) action that matches the characteristics of your false positive report. We recommend any skip rule that you create uses the most narrow possible scope, including restricting the request methods and URIs that the expected traffic has access to, to limit potential abuse.

- Allowing a [JA3/JA4 fingerprint](#): If you want to allow access to a stable software client that does not come from a dedicated IP, you can do so by looking up the JA3 fingerprint(s) used by that client in the Bot Analytics dashboard, and creating a WAF custom rule to allow traffic based on that JA3 fingerprint. JA3 fingerprints will only match a client's TLS library, so be cautious in looking for both overlap with other clients and with variation based on the operating system.

Cloudflare does not recommend relying on JA3 rules for mobile applications that may be abused. If you have questions about how to securely allow traffic from your mobile application, please contact your account team.

:::note The instructions below apply to Enterprise subscription with Bot Management, Bot Fight Mode and Super Bot Fight Mode. :::

- Allowing an **IP address**: Only use an IP address to allow traffic if the IP is a dedicated resource that belongs only to the traffic source you wish to allow. If the traffic you want to allow shares an IP with other traffic sources, or if the IP changes frequently, consider an alternative to allowing by IP address.

Recommendations after submitting a false negative

After submitting a false negative report, you can explicitly block or rate-limit the incorrectly scored traffic using a combination of characteristics such as IP address, JA3 fingerprint, ASN, and user-agent. Before blocking or rate-limiting based on JA3 fingerprint, please use Bot Analytics to confirm that fingerprint is not being used by legitimate traffic sources.

🔍	#2		
📅	📅	🕒	2026-11-01 00:05:53 UTC
📅	📅	🕒	2026-11-01 00:05:55 UTC