Cloudflare Docs

Search ⌘ K

Copy page ▼

Changelog

[Subscribe to RSS 🔊](#)

2026-02-09

Analytics enhancements

AI Crawl Control metrics have been enhanced with new views, improved filtering, and better data visualization.

Select crawler ⌄	OpenAI ✕ ⌄	+ Add filter	Path contains /ai ✕	Clear all		Last 7 days (CST) 📅

Path patterns
All · Patterns · Content · Media 📤
Analyze path patterns to identify which sections of your site are most crawled.

Path	Host	↓ Allowed requests
/*	developers.cloudflare.com	37,475
/ai-gateway/*	developers.cloudflare.com	24,229
/ai-gateway/usage/*	developers.cloudflare.com	9,421
/ai-search/*	developers.cloudflare.com	4,329
/ai-gateway/features/*	developers.cloudflare.com	2,963
/api/*	developers.cloudflare.com	2,583
/ai-crawl-control/*	developers.cloudflare.com	2,408
/ai-gateway/configuration/*	developers.cloudflare.com	2,243
/ai-gateway/llms-full.txt	developers.cloudflare.com	1,997
/ai-search/configuration/*	developers.cloudflare.com	1,978

1 - 10 of 63 items

Page 1 ⌄ of 7 ‹ ›

Path pattern grouping

- In the **Metrics** tab > **Most popular paths** table, use the new **Patterns** tab that groups requests by URI pattern (`/blog/*`, `/api/v1/*`, `/docs/*`) to identify which site areas crawlers target most. Refer to the screenshot above.

Enhanced referral analytics

- Destination patterns show which site areas receive AI-driven referral traffic.
- In the **Metrics** tab, a new **Referrals over time** chart shows trends by operator or source.

Data transfer metrics

- In the **Metrics** tab > **Allowed requests over time** chart, toggle **Bytes** to show bandwidth consumption.
- In the **Crawlers** tab, a new **Bytes Transferred** column shows bandwidth per crawler.

Image exports

- Export charts and tables as images for reports and presentations.

Learn more about [analyzing AI traffic](#).

2026-02-04

New reference documentation

New reference documentation is now available for AI Crawl Control:

- [**GraphQL API reference**](#) — Query examples for crawler requests, top paths, referral traffic, and data transfer. Includes key filters for detection IDs, user agents, and referrer domains.

- **[Bot reference](#)** — Detection IDs and user agents for major AI crawlers from OpenAI, Anthropic, Google, Meta, and others.
- **[Worker templates](#)** — Deploy the x402 Payment-Gated Proxy to monetize crawler access or charge bots while letting humans through free.

2026-01-13

AI Crawl Control Read Only role now available

Account administrators can now assign the **AI Crawl Control Read Only** role to provide read-only access to AI Crawl Control at the domain level.

Users with this role can view the **Overview**, **Crawlers**, **Metrics**, **Robots.txt**, and **Settings** tabs but cannot modify crawler actions or settings.

This role is specific for AI Crawl Control. You still require correct permissions to access other areas / features of the dashboard.

To assign, go to **Manage Account** > **Members** and add a policy with the **AI Crawl Control Read Only** role scoped to the desired domain.

2025-12-18

New AI Crawl Control Overview tab

The **Overview** tab is now the default view in AI Crawl Control. The previous default view with controls for individual AI crawlers is available in the **Crawlers** tab.

What's new

- **Executive summary** — Monitor total requests, volume change, most common status code, most popular path, and high-volume activity
- **Operator grouping** — Track crawlers by their operating companies (OpenAI, Microsoft, Google, ByteDance, Anthropic, Meta)
- **Customizable filters** — Filter your snapshot by date range, crawler, operator, hostname, or path
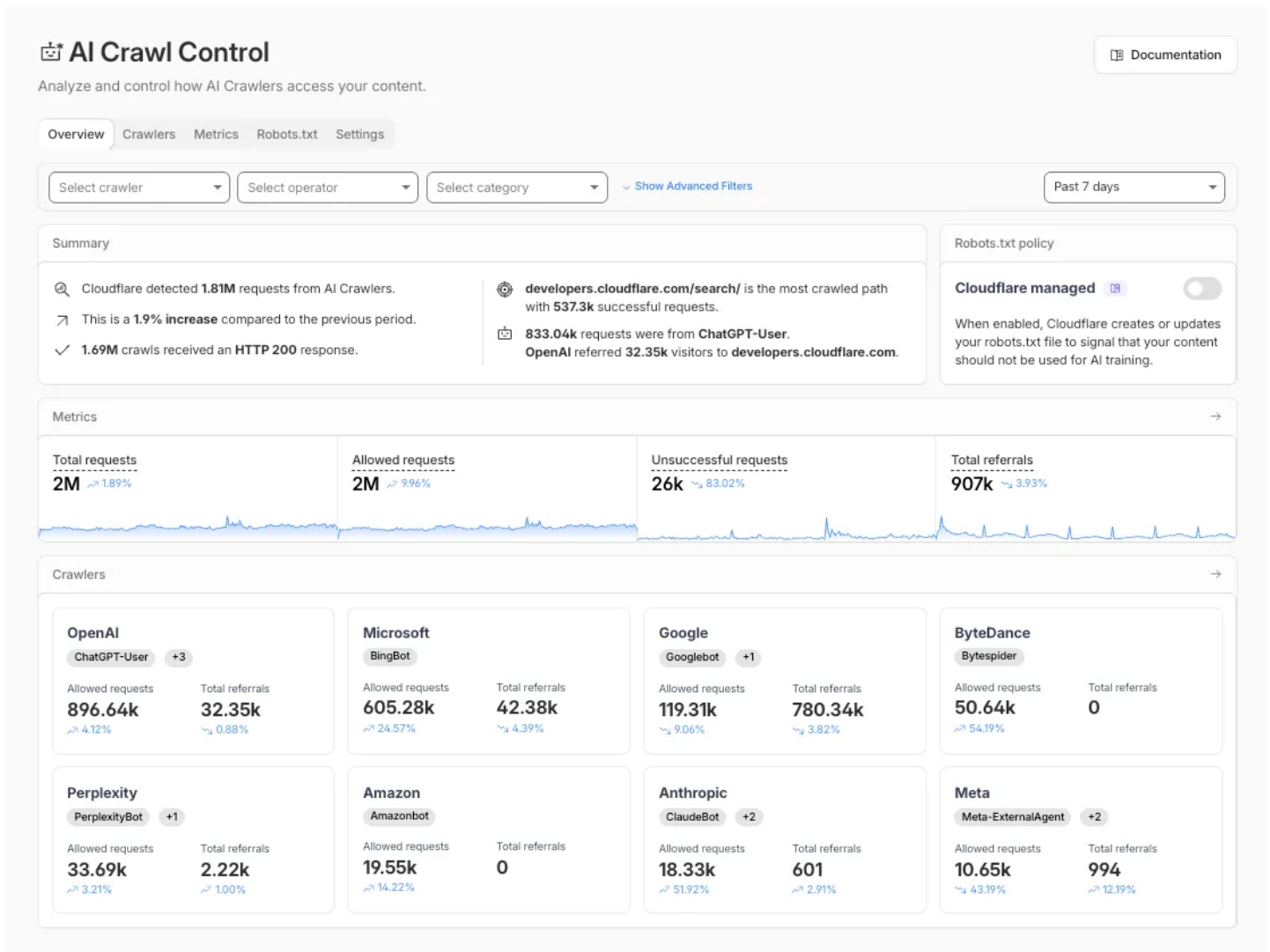
Get started

1. Log in to the Cloudflare dashboard and select your account and domain.

2. Go to **AI Crawl Control**, where the **Overview** tab opens by default with your activity snapshot.

3. Use filters to customize your view by date range, crawler, operator, hostname, or path.

4. Navigate to the **Crawlers** tab to manage controls for individual crawlers.

Learn more about [analyzing AI traffic](#) and [managing AI crawlers](#).

2025-12-10

Pay Per Crawl (Private beta) - Discovery API, custom pricing, and advanced configuration
Pay Per Crawl is introducing enhancements for both AI crawler operators and site owners, focusing on programmatic discovery, flexible pricing models, and granular configuration control.

For AI crawler operators

Discovery API

A new authenticated API endpoint allows verified crawlers to programmatically discover domains participating in Pay Per Crawl. Crawlers can use this to build optimized crawl queues, cache domain lists, and identify new participating sites. This eliminates the need to discover payable content through trial requests.

The API endpoint is `GET https://crawlers-api.ai-audit.cfdata.org/charged_zones` and requires Web Bot Auth authentication. Refer to [Discover payable content](#) for authentication steps, request parameters, and response schema.

Payment header signature requirement

Payment headers (`crawler-exact-price` or `crawler-max-price`) must now be included in the Web Bot Auth `signature-input` header components. This security enhancement prevents payment header tampering, ensures authenticated payment intent, validates crawler identity with payment commitment, and protects against replay attacks with modified pricing. Crawlers must add their payment header to the list of signed components when [constructing the signature-input header](#).

New `crawler-error` header

Pay Per Crawl error responses now include a new `crawler-error` header with 11 specific [error codes](#) for programmatic handling. Error response bodies remain unchanged for compatibility. These codes enable robust error handling, automated retry logic, and accurate spending tracking.

For site owners

Configure free pages

Site owners can now offer free access to specific pages like homepages, navigation, or discovery pages while charging for other content. Create a [Configuration Rule](#) in **Rules** > **Configuration Rules**, set your URI pattern using wildcard, exact, or prefix matching on the **URI Full** field, and enable the **Disable Pay Per Crawl** setting. When disabled for a URI pattern, crawler requests pass through without blocking or charging.

Some paths are always free to crawl. These paths are: `/robots.txt`, `/sitemap.xml`, `/security.txt`, `/.well-known/security.txt`, `/crawlers.json`.

Get started

AI crawler operators: [Discover payable content](#) | [Crawl pages](#)

Site owners: [Advanced configuration](#)
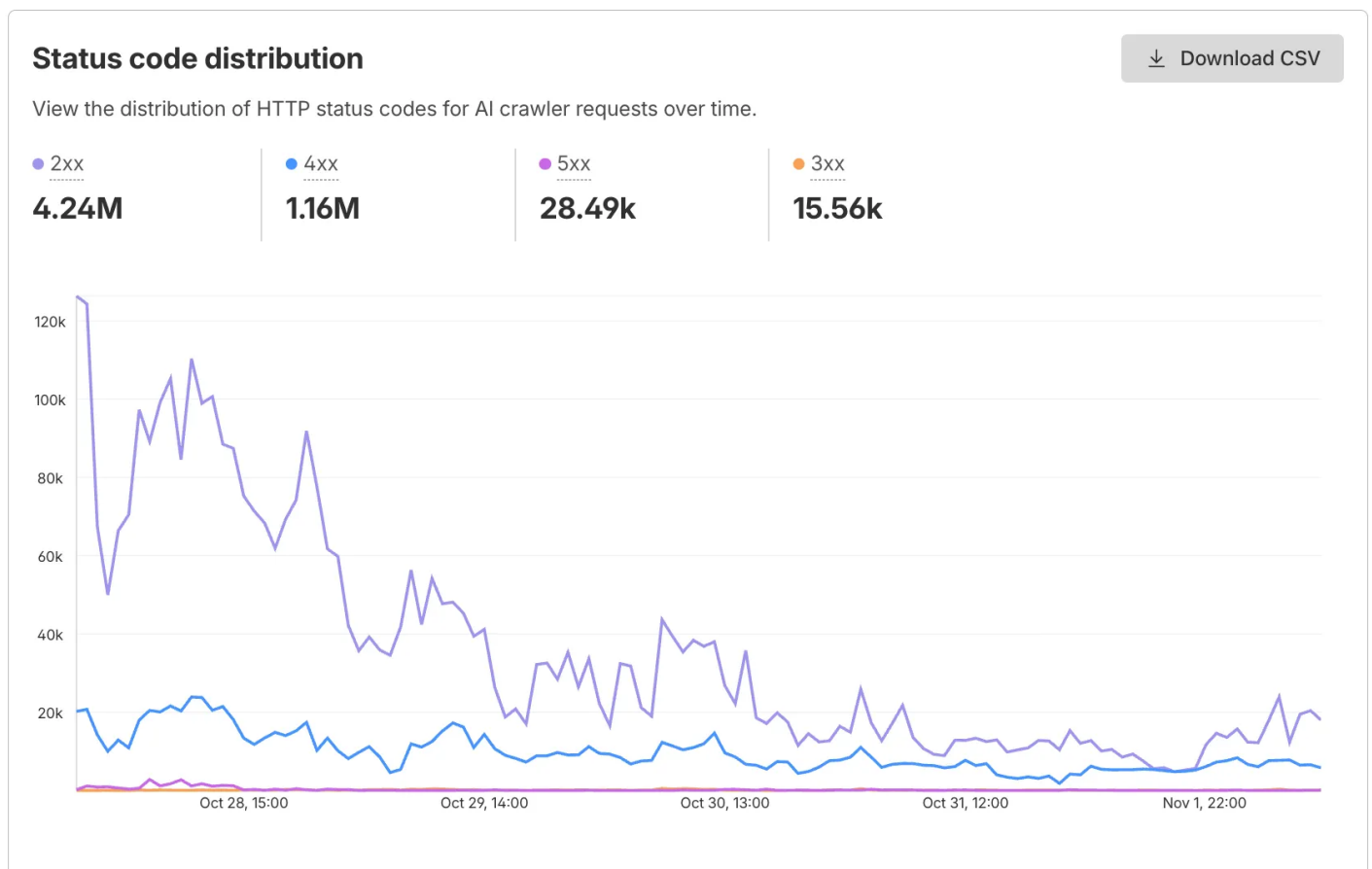
2025-11-10

Crawler drilldowns with extended actions menu

AI Crawl Control now supports per-crawler drilldowns with an extended actions menu and status code analytics. Drill down into Metrics, Cloudflare Radar, and Security Analytics, or export crawler data for use in WAF custom rules, Redirect Rules, and robots.txt files.

What's new

Status code distribution chart

The **Metrics** tab includes a status code distribution chart showing HTTP response codes (2xx, 3xx, 4xx, 5xx) over time. Filter by individual crawler, category, operator, or time range to analyze how specific crawlers interact with your site.

Status code distribution   ⬇ Download CSV

View the distribution of HTTP status codes for AI crawler requests over time.

● 2xx   ● 4xx   ● 5xx   ● 3xx
4.24M   **1.16M**   **28.49k**   **15.56k**

Oct 28, 15:00   Oct 29, 14:00   Oct 30, 13:00   Oct 31, 12:00   Nov 1, 22:00

Extended actions menu

Each crawler row includes a three-dot menu with per-crawler actions:

- **View Metrics** — Filter the AI Crawl Control Metrics page to the selected crawler.

- **View on Cloudflare Radar** — Access verified crawler details on Cloudflare Radar.

- **Copy User Agent** — Copy user agent strings for use in WAF custom rules, Redirect Rules, or robots.txt files.

- **View in Security Analytics** — Filter Security Analytics by detection IDs (Bot Management customers).

- **Copy Detection ID** — Copy detection IDs for use in WAF custom rules (Bot Management customers).

Get started

1. Log in to the Cloudflare dashboard, and select your account and domain.

2. Go to **AI Crawl Control** > **Metrics** to access the status code distribution chart.

3. Go to **AI Crawl Control** > **Crawlers** and select the three-dot menu for any crawler to access per-crawler actions.

4. Select multiple crawlers to use bulk copy buttons for user agents or detection IDs.

Learn more about AI Crawl Control.

2025-10-21

New Robots.txt tab for tracking crawler compliance

AI Crawl Control now includes a **Robots.txt** tab that provides insights into how AI crawlers interact with your `robots.txt` files.

What's new

The Robots.txt tab allows you to:

- Monitor the health status of `robots.txt` files across all your hostnames, including HTTP status codes, and identify hostnames that need a `robots.txt` file.

- Track the total number of requests to each `robots.txt` file, with breakdowns of successful versus unsuccessful requests.

- Check whether your `robots.txt` files contain [Content Signals ↗](#) directives for AI training, search, and AI input.

- Identify crawlers that request paths explicitly disallowed by your `robots.txt` directives, including the crawler name, operator, violated path, specific directive, and violation count.

- Filter `robots.txt` request data by crawler, operator, category, and custom time ranges.

Take action

When you identify non-compliant crawlers, you can:

- Block the crawler in the [Crawlers tab](#)

- Create custom [WAF rules](#) for path-specific security

- Use [Redirect Rules](#) to guide crawlers to appropriate areas of your site

To get started, go to **AI Crawl Control** > **Robots.txt** in the Cloudflare dashboard. Learn more in the [Track robots.txt documentation](#).

2025-10-14

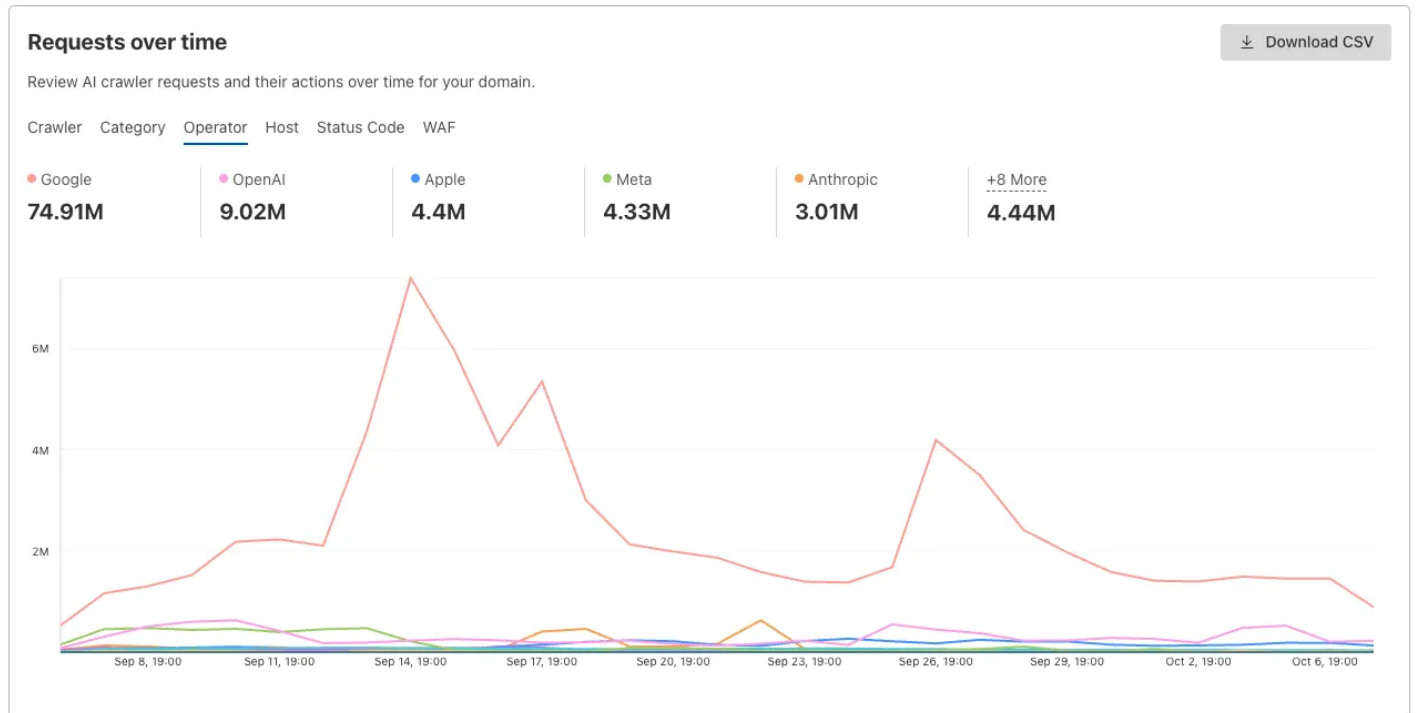**Enhanced AI Crawl Control metrics with new drilldowns and filters**
AI Crawl Control now provides enhanced metrics and CSV data exports to help you better understand AI crawler activity across your sites.

What's new

Track crawler requests over time

Visualize crawler activity patterns over time, and group data by different dimensions:

- **By Crawler** — Track activity from individual AI crawlers (GPTBot, ClaudeBot, Bytespider)
- **By Category** — Analyze crawler purpose or type
- **By Operator** — Discover which companies (OpenAI, Anthropic, ByteDance) are crawling your site
- **By Host** — Break down activity across multiple subdomains
- **By Status Code** — Monitor HTTP response codes to crawlers (200s, 300s, 400s, 500s)

Requests over time

Review AI crawler requests and their actions over time for your domain.

⬇ Download CSV

Crawler Category Operator Host Status Code WAF

● Google   ● OpenAI   ● Apple   ● Meta   ● Anthropic   +8 More
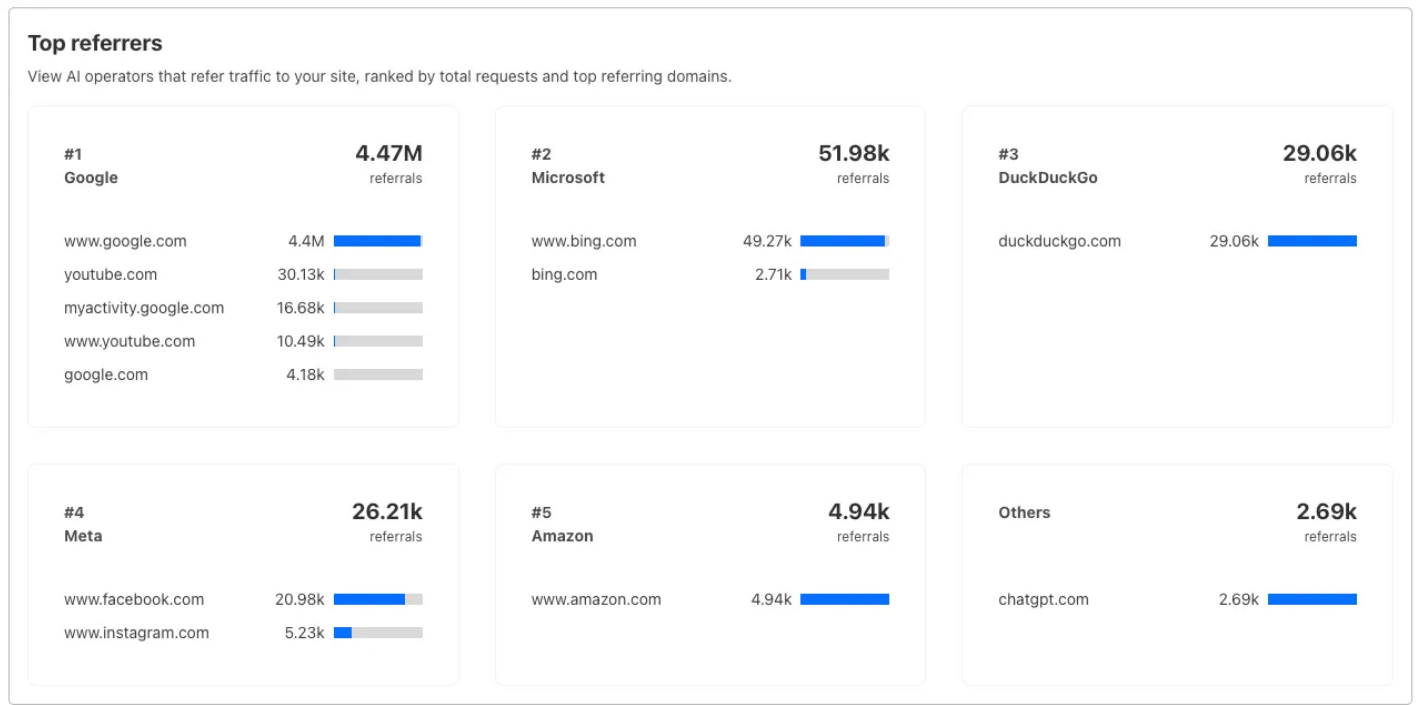**74.91M**   **9.02M**   **4.4M**   **4.33M**   **3.01M**   **4.44M**

Interactive chart showing crawler requests over time with filterable dimensions

Analyze referrer data (Paid plans)

Identify traffic sources with referrer analytics:

- View top referrers driving traffic to your site
- Understand discovery patterns and content popularity from AI operators

Bar chart showing top referrers and their respective traffic volumes

Export data

Download your filtered view as a CSV:

- Includes all applied filters and groupings

- Useful for custom reporting and deeper analysis

Get started

1. Log in to the Cloudflare dashboard, and select your account and domain.

2. Go to **AI Crawl Control** > **Metrics**.

3. Use the grouping tabs to explore different views of your data.

4. Apply filters to focus on specific crawlers, time ranges, or response codes.

5. Select **Download CSV** to export your filtered data for further analysis.

Learn more about [AI Crawl Control](#).

2025-08-27

Enhanced crawler insights and custom 402 responses

We improved AI crawler management with detailed analytics and introduced custom HTTP 402 responses for blocked crawlers. AI Audit has been renamed to AI Crawl Control and is now generally available.

Enhanced Crawlers tab:

- View total allowed and blocked requests for each AI crawler

- Trend charts show crawler activity over your selected time range per crawler

Custom block responses (paid plans): You can now return HTTP 402 "Payment Required" responses when blocking AI crawlers, enabling direct communication with crawler operators about licensing terms.

For users on paid plans, when blocking AI crawlers you can configure:

- **Response code:** Choose between 403 Forbidden or 402 Payment Required
- **Response body:** Add a custom message with your licensing contact information

Example 402 response:

```
HTTP 402 Payment Required
Date: Mon, 24 Aug 2025 12:56:49 GMT
Content-type: application/json
Server: cloudflare
Cf-Ray: 967e8da599d0c3fa-EWR
Cf-Team: 2902f6db750000c3fa1e2ef400000001


{
  "message": "Please contact the site owner for access."
}
```

2025-07-01

Introducing Pay Per Crawl (private beta)

We are introducing a new feature of [AI Crawl Control](#) — Pay Per Crawl. [Pay Per Crawl](#) enables site owners to require payment from AI crawlers every time the crawlers access their content, thereby fostering a fairer Internet by enabling site owners to control and monetize how their content gets used by AI.

For Site Owners:

- Set pricing and select which crawlers to charge for content access

- Manage payments via Stripe

- Monitor analytics on successful content deliveries

For AI Crawler Owners:

- Use HTTP headers to request and accept pricing

- Receive clear confirmations on charges for accessed content

Learn more in the [Pay Per Crawl documentation](#).

2025-07-01

AI Crawl Control refresh

We redesigned the AI Crawl Control dashboard to provide more intuitive and granular control over AI crawlers.

- From the new **AI Crawlers** tab: block specific AI crawlers.
- From the new **Metrics** tab: view AI Crawl Control metrics.

To get started, explore:

- [Manage AI crawlers](#).

- [Analyze AI traffic](#).

2024-09-23

AI Crawl Control

Every site on Cloudflare now has access to **AI Audit**, which summarizes the crawling behavior of popular and known AI services.

You can use this data to:

- Understand how and how often crawlers access your site (and which content is the most popular).
- Block specific AI bots accessing your site.

- Use Cloudflare to enforce your `robots.txt` policy via an automatic WAF rule.

To get started, explore [AI audit](#).

Previous

← **Glossary**

Last updated: Aug 27, 2025

Resources

API

New to
Cloudflare?

Directory

Sponsorships

Open Source

Support

Help Center

System Status

Compliance

GDPR

Company

cloudflare.com

Our team

Careers

Tools

Cloudflare Radar

Speed Test

Is BGP Safe Yet?

RPKI Toolkit

Certificate
Transparency

Community

X X

Discord

YouTube

GitHub

© 2026 Cloudflare, Inc.   •   Privacy Policy   •   Terms of Use   •   Report Security Issues   •   Trademark

•   Cookie Preferences