Automatic request headers

- User-Agent
- Non-configurable headers
  - About Web Bot Auth
  - Bot detection

Cloudflare automatically attaches headers to every request made through Browser Run. These headers make it easy for destination servers to identify that these requests came from Cloudflare.

User-Agent

The default User-Agent depends on how you access Browser Run:

Method	Default User-Agent	Customizable
Quick Actions	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/152.0.0.0 Safari/537.36`	Yes, using the `userAgent` parameter
Crawl endpoint	`CloudflareBrowserRenderingCrawler/1.0`	No
CDP (Puppeteer, Playwright)	The default User-Agent of the underlying Chrome version	Yes, via Puppeteer/Playwright configuration

:::note The User-Agent header is not a reliable way to identify Browser Run requests. It is configurable for most Browser Run methods, changes when the underlying Chrome version updates, and any HTTP client can send any User-Agent string. Destination servers should use the non-configurable headers and Web Bot Auth signatures below, which provide cryptographic proof that a request originated from Cloudflare Browser Run. :::

Non-configurable headers

:::note The following headers are meant to ensure transparency and cannot be removed or overridden (with `setExtraHTTPHeaders`, for example). :::

Header	Description
`cf-brapi-request-id`	A unique identifier for the Browser Run request when using Quick Actions
`cf-brapi-devtools`	A unique identifier for the Browser Run request when using Puppeteer, Playwright, or CDP
`cf-biso-devtools`	A flag indicating the request originated from Cloudflare's rendering infrastructure
`Signature-agent`	The location of the bot public keys, used to sign the request and verify it came from Cloudflare
`Signature` and `Signature-input`	A digital signature, used to validate requests, as shown in this architecture document

About Web Bot Auth

The `Signature` headers use an authentication method called Web Bot Auth. Web Bot Auth leverages cryptographic signatures in HTTP messages to verify that a request comes from an automated bot. To verify a request originated from Cloudflare Browser Run, use the keys found on this directory to verify the `Signature` and `Signature-Input` found in the headers from the incoming request. A successful verification proves that the request originated from Cloudflare Browser Run and has not been tampered with in transit.

Bot detection

Browser Run uses different bot detection IDs depending on the method. Quick Actions (excluding the crawl endpoint), Puppeteer, Playwright, and CDP share one ID, while the crawl endpoint has its own.

Method	Bot detection ID
Quick Actions, Puppeteer, Playwright, CDP	`119853733`
Crawl endpoint	`128292352`

If you are attempting to scan your own zone and want Browser Run to access your website freely without your bot protection configuration interfering, you can create a WAF skip rule to allowlist Browser Run.

□□□ #2
□ □□□ □□□ 2026-11-01 00:10:48 UTC
□ □□□ □□□ 2026-11-01 00:10:50 UTC