IP Access rules

- Important remarks about allowing/blocking by country
- Recommendation: Use custom rules instead
- Availability
- Final remarks
- Related resources

import { GlossaryTooltip } from "~/components";

Use IP Access rules to allowlist, block, and challenge traffic based on the visitor's IP address, Autonomous System Number (ASN), or country.

IP Access rules are commonly used to block or challenge suspected malicious traffic. Another common use of IP Access rules is to allow services that regularly access your site, such as APIs, crawlers, and payment providers.

:::caution

Allowing an IP or ASN will bypass any configured custom rules, rate limiting rules, WAF Managed Rules, and firewall rules (deprecated).

For important notes about allowing or blocking traffic by country, refer to Important remarks about allowing/blocking by country.

:::

Important remarks about allowing/blocking by country

Block by country is only available on Enterprise plans.

IP addresses globally allowed by Cloudflare will override an IP Access rule country block, but they will not override a country block via custom rules.

Allowing a country will:

- Bypass any configured custom rules, rate limiting rules, and firewall rules (deprecated).
- Not bypass WAF Managed Rules or WAF managed rules (previous version).

Recommendation: Use custom rules instead

Cloudflare recommends that you create custom rules instead of IP Access rules to perform IP-based or geography-based blocking (geoblocking):

- For IP-based blocking, use an IP list in the custom rule expression. Refer to Allow traffic from IP addresses in allowlist only for an example.
- For geoblocking, use fields such as *AS Num*, *Country*, and *Continent* in the custom rule expression. Refer to Block traffic from specific countries for an example.

When upgrading to custom rules, consider replacing the *Allow* action supported by IP Access rules with the *Skip* action. Note that the *Skip* action does not bypass all of Cloudflare's app security features.

Availability

IP Access rules are available to all customers.

	Free	Pro	Business	Enterprise
Availability	Yes	Yes	Yes	Yes
Number of rules	50,000	50,000	50,000	50,000, but can purchase more
Block by country	No	No	No	Yes

Each Cloudflare account can have a maximum of 50,000 rules. If you are an Enterprise customer and need more rules, contact your account team.

Block by country is only available on Enterprise plans. Other customers may perform country blocking using WAF custom rules.

Final remarks

- By design, IP Access rules configured to *Allow* traffic do not show up in Security Events.
- Requests containing certain attack patterns in the `User-Agent` field are checked before being processed by the general firewall pipeline. Therefore, such requests are blocked before any allowlist logic takes place. When this occurs, security events downloaded from the API show `rule_id` as `security_level` and action as `drop`.
- Cloudflare supports use of `fail2ban` to block IPs on your server. However, to prevent `fail2ban` from inadvertently blocking Cloudflare IPs and causing errors for some visitors, ensure you restore original visitor IP in your origin server logs. For details, refer to Restoring original visitor IPs.

Related resources

To learn more about protection options provided by Cloudflare to protect your website against malicious traffic and bad actors, refer to Account security.

□□□ #2
□ □□□ □□□ 2026-11-01 05:18:07 UTC
□ □□□ □□□ 2026-11-01 05:18:09 UTC