

X-Forwarded-For

The `x-Forwarded-For` (XFF) request header is a de-facto standard header for identifying the originating IP address of a client connecting to a web server through a proxy server.

Warning: Improper use of this header can be a security risk. For details, see the [Security and privacy concerns](#) section.

When a client connects directly to a server, the client's IP address is sent to the server (and is often written to server access logs). But if a client connection passes through any [forward or reverse](#) proxies, the server only sees the final proxy's IP address, which is often of little use. That's especially true if the final proxy is a load balancer which is part of the same installation as the server. So, to provide a more-useful client IP address to the server, the `x-Forwarded-For` request header is used.

For detailed guidance on using this header, see the [Parsing](#) and [Selecting an IP address](#) sections.

Header type	Request header
Forbidden header name	no

A standardized version of this header is the HTTP [Forwarded](#) header.

Security and privacy concerns

This header, by design, exposes privacy-sensitive information, such as the IP address of the client. Therefore the user's privacy must be kept in mind when deploying this header.

The `X-Forwarded-For` header is untrustworthy when no trusted reverse proxy (e.g., a load balancer) is between the client and server. If the client and all proxies are benign and well-behaved, then the list of IP addresses in the header has the meaning described in the [Directives](#) section. But if there's a risk the client or any proxy is malicious or misconfigured, then it's possible any part (or the entirety) of the header may have been spoofed (and may not be a list or contain IP addresses at all).

If any trusted reverse proxies are between the client and server, the final `X-Forwarded-For` IP addresses (one for each trusted proxy) are trustworthy, as they were added by trusted proxies. (That's true as long as the server is *only* accessible through those proxies and not also directly).

Any security-related use of `X-Forwarded-For` (such as for rate limiting or IP-based access control) *must only* use IP addresses added by a trusted proxy. Using untrustworthy values can result in rate-limiter avoidance, access-control bypass, memory exhaustion, or other negative security or availability consequences.

Conversely, leftmost (untrusted) values must only be used where there will be no negative impact from the possibility of using spoofed values.

Syntax

HTTP

`X-Forwarded-For`: <client>, <proxy1>, <proxy2>

Elements are comma-separated, with optional whitespace surrounding the commas.

Directives

<client>

The client IP address

<proxy1>, <proxy2>

If a request goes through multiple proxies, the IP addresses of each successive proxy is listed. This means that, given well-behaved client and proxies, the rightmost IP address is the IP address of the most recent proxy and the leftmost IP address is the IP address of the originating client.

Examples

HTTP

`X-Forwarded-For: 2001:db8:85a3:8d3:1319:8a2e:370:7348`

`X-Forwarded-For: 203.0.113.195`

`X-Forwarded-For: 203.0.113.195, 2001:db8:85a3:8d3:1319:8a2e:370:7348`

`X-Forwarded-For: 203.0.113.195, 2001:db8:85a3:8d3:1319:8a2e:370:7348, 198.51.100.178`

Parsing

Improper parsing of the `X-Forwarded-For` header can result in spoofed values being used for security-related purposes, resulting in the negative consequences mentioned above.

There may be multiple `X-Forwarded-For` headers present in a request. The IP addresses in these headers must be treated as a single list, starting with the first IP address of the first header and continuing to the last IP address of the last header. There are two ways of making this single list:

- join the `X-Forwarded-For` full header values with commas and then split by comma into a list, or
- split each `X-Forwarded-For` header by comma into lists and then join the lists

It is insufficient to use only one of multiple `X-Forwarded-For` headers.

(Some reverse proxies will automatically join multiple `X-Forwarded-For` headers into one, but it is safest to not assume that this is the case.)

Selecting an IP address

When selecting an address, the full list of IPs — from all `X-Forwarded-For` headers — must be used.

When choosing the `X-Forwarded-For` client IP address closest to the client (untrustworthy and *not* for security-related purposes), the first IP from the leftmost that is a *valid address* and *not private/internal* should be selected. ("Valid" because spoofed values may not be IP addresses at all; "not internal/private" because clients may have used proxies on their internal network, which may have added addresses from the [private IP space](#) .)

When choosing the first *trustworthy* `X-Forwarded-For` client IP address, additional configuration is required. There are two common methods:

- **Trusted proxy count:** The count of reverse proxies between the internet and the server is configured. The `X-Forwarded-For` IP list is searched from the rightmost by that count minus one. (For example, if there is only one reverse proxy, that proxy will add the client's IP address, so the rightmost address should be used. If there are three reverse proxies, the last two IP addresses will be internal.)
- **Trusted proxy list:** The IPs or IP ranges of the trusted reverse proxies are configured. The `X-Forwarded-For` IP list is searched from the rightmost, skipping all addresses that are on the trusted proxy list. The first non-matching address is the target address.

The first trustworthy `X-Forwarded-For` IP address may belong to an untrusted intermediate proxy rather than the actual client computer, but it is the only IP suitable for security uses.

Note that if the server is directly connectable from the internet — even if it is also behind a trusted reverse proxy — *no part* of the `X-Forwarded-For` IP list can be considered trustworthy or safe for security-related uses.

Specifications

Not part of any current specification. The standardized version of this header is [Forwarded](#) .

See also

- [Forwarded](#)
- [X-Forwarded-Host](#)
- [X-Forwarded-Proto](#)
- [Via](#)

This page was last modified on Jul 24, 2023 by [MDN contributors](#).