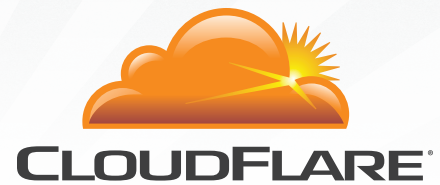# Frequently asked questions and technical support

What is CloudFlare?

CloudFlare is a performance and security service that we provide to our customers. On average, a website on CloudFlare loads twice as fast, uses 60% less bandwidth, has 65% fewer requests and is way more secure.

What is the association between your hosting provider offering and CloudFlare?

CloudFlare is a third-party vendor that is offering the CloudFlare service to your customers through a partnership.

How does CloudFlare's technology work?

CloudFlare is a CDN (content delivery network) with a security layer. Once a website is part of the CloudFlare community, its web traffic is routed through CloudFlare's global network.

CloudFlare's network stores a copy of static files closer to web visitors, which means they are delivered more quickly than before. CloudFlare caches resources such as CSS, JavaScript and images. CloudFlare's technology automatically decides which resources to cache based on file extension names so there is zero configuration. CloudFlare also does compression for every request.

CloudFlare's network also blocks threats and limits abusive bots before they hit the server, which means less wasted bandwidth and server resources.

Where are CloudFlare's data centers located?

CloudFlare's network currently has 13 locations where it does caching and traffic filtering:

- **Six in the US:** San Jose, Los Angeles, Chicago, Washington D.C., New Jersey, Dallas
- **Four in Europe:** Amsterdam, Paris, Frankfurt, London
- **Three in Asia:** Hong Kong, Singapore, Tokyo

What types of websites can use CloudFlare?

Almost all websites can use CloudFlare. CloudFlare works for both static and dynamic websites.

CloudFlare is not suitable for websites that stream video or audio directly from their origin server. If a website uses YouTube or Vimeo for the videos embedded on your website, then that is compatible with CloudFlare.

A website has SSL. Is CloudFlare compatible?

If a website has SSL, the site can use CloudFlare, however there is an extra step. If the SSL is on its own sub-domain (i.e. SSL), then ensure that this sub-domain is marked with a gray cloud. If the SSL is on www, then the user has to upgrade to a paid service (either Basic or Pro) and follow the directions at http://www.cloudflare.com/wiki/How_do_I_add_SSL_support_for_a_domain%3F.

Are there sub-domains that shouldn't be enabled with CloudFlare?

Sub-domains on CloudFlare are marked with an orange cloud. Sub-domains not on CloudFlare are marked with a gray cloud.

The CloudFlare network can only proxy web traffic over ports 80 and 443. The following sub-domains should be marked with a gray cloud to prevent performance issues:

- cpanel
- direct

- ftp
- ghs.google.com
- mail and webmail
- mysql
- nameservers (NS1, NS2)
- secure* (unless you enable CloudFlare SSL)

View the full list of sub-domains here:

- http://www.cloudflare.com/wiki/What_subdomains_are_appropriate_for_orange_/_gray_clouds

Can I enable CloudFlare on a wildcard (*) sub-domain?

No, for security reasons, CloudFlare does not proxy traffic to a wildcard sub-domain. You have to explicitly list the sub-domain as a CNAME in your DNS records to be able to activate CloudFlare.

Can I enable CloudFlare on my root domain (i.e. mywebsite.com) that is an A record?

CloudFlare can only accelerate and protect CNAMEs, not A records, which often includes the root domain. If traffic goes to a root domain and you want to accelerate and protect the traffic using CloudFlare, you can add a redirect to 'www' in your .htaccess file.

If the user does not forward the traffic, then any traffic to www.mydomain.com will be accelerated and protected by CloudFlare (and shown in the statistics) and any traffic to mydomain.com will not be served by CloudFlare.

```
RewriteEngine On
# Rewrite added for CloudflareInstall – mysite.com
# Wednesday 25th of August 2010 04:59:42 AM
RewriteCond %{HTTP_HOST} ^mysite.com$ [NC]
RewriteCond %{SERVER_PORT} ^80$
RewriteRule ^(.*)$ http://www.mysite.com/$1 [R=301,L]
```

The user activated CloudFlare from my control panel. Do they also get an account on cloudflare.com? What is the difference?

Once CloudFlare is activated through you, the customer also gets an account at www.cloudflare.com. The basic statistics and settings are shown in your control panel. To see more statistics, threat control panel and all the CloudFlare settings, the customer has to log in to their www.cloudflare.com account. Please instruct the customer to use the 'Forgot password' link the first time that they try to log in.

Troubleshooting

I activated CloudFlare, but do not see any statistics.

There are two main reasons why this would happen.

1. No traffic to subdomain

- CloudFlare is enabled for a subdomain that does not get traffic. Through the hosting providers, CloudFlare can only protect traffic going to certain subdomains, specifically CNAMEs. If your traffic all goes to an A record like your root domain, mydomain.com, rather than www.mydomain.com, then even if you've enabled CloudFlare, the traffic is not passing through our network.

- To resolve this issue, you can setup a redirect in your .htaccess file from the root domain to the 'www' subdomain. You will want to make sure the cloud is orange for the 'www' subdomain.

2. CloudFlare not turned on for subdomain

- You have not turned CloudFlare on for the subdomain. CloudFlare 'on' is indicated by an orange cloud, rather than gray cloud. You want to toggle the cloud to orange in your control panel next to the subdomain.

- You can easily test for #1 and #2 by running the following command in Terminal (Mac) or Command Prompt (PC):

    - `dig www.mywebsite.com`

- You want to see an output with "cdn.cloudflare.net" attached to it. If there is no ".cdn.cloudflare.net" attached to the output, then traffic is not flowing through CloudFlare's network.

The customer tried CloudFlare and has an issue. What should I do?

When one of your hosting customers enables CloudFlare, there should be no noticeable difference to their website. If the site is loading slowly after enabling CloudFlare or there is an error page, there is most likely a problem. First, the customer should disable CloudFlare by clicking the orange cloud so it becomes gray. Second, your support team should contact CloudFlare's support to resolve the issue.

In the Support Ticket to CloudFlare, include:

- The domain

- Details about the issue

- Error page description

- Email the ticket to support@cloudflare.com

The customer cannot access their website. They are seeing a:

502 Bad gateway cloudflare-nginx error page

- CloudFlare's network is having an issue. We monitor for errors like these very closely. Our most up to date network system status is on our CloudFlareSys Twitter handle: http://twitter.com/#!/search/cloudflaresys

- CloudFlare runs 13 data centers and often issues are isolated to one server in one data center so even though some visitors are affected, other visitors around the world will not see the same error. Our Technical Operations team clears issues very quickly.

- If one of your users is seeing this type of error page, they can:

    - File a report to help@cloudflare.com with the geographic location of where the error page was seen

    - It is best if an output of a traceroute is included

    - Temporarily toggle CloudFlare to off (gray cloud)

My website is currently unavailable page

- This error page appears when CloudFlare cannot connect to the origin server and CloudFlare does not have a copy of the website in its cache.

- CloudFlare cannot connect to the origin server in two situations:

    - **1. The server is online, but something on the server is blocking CloudFlare's requests.** The most typical culprit is a firewall.

    - If the origin server is online, but this error page is displaying, something is blocking CloudFlare's requests. The most common cause is a firewall. The website owner should make sure all of CloudFlare's IP addresses are whitelisted.

    - **2. The origin server is offline.** When the origin server goes offline, CloudFlare tries to serve a copy of the webpage from its cache. If CloudFlare does not have a copy in its cache, then this standard error page appears. The website owner should work with you to determine why their server is offline.

1004 error – DNS is still propagating

If one of your customers activates CloudFlare through the control panel and immediately visits their website, they may see a "DNS is propagating" error page. This will not happen frequently. The issue should resolve itself within 5 to 10 minutes. If not, contact CloudFlare support team at support@cloudflare.com.

www.cloudflare.com
support@cloudflare.com
650.319.8930