

Creating a Cloudflare account and adding a website

Create a Cloudflare account

1. Visit <https://dash.cloudflare.com/sign-up>.
2. Enter your Email address and Password.
3. Click Create Account.
 - a. Use an email alias or distribution list (i.e. cloudflare@example.com) This email alias is the main point of contact for Cloudflare billing and service-related email notifications. Ensure that the email alias **can both send and receive emails for account recovery and troubleshooting**.
4. The Cloudflare UI asks you to [add a site to Cloudflare](#).
5. Follow the steps till you've reached the "Changing Name-servers" modal, at this point, do not do anything yet. Refer to the steps below if on CNAME or FULL setup.
6. Consider setting up the features on the dashboard before the CNAME (Partial DNS) or nameserver (full) change.
7. For CNAME (Partial DNS) setup, after the initial Nameserver Check (without actually doing the migration), scroll down on the Overview page to click the link to convert to Partial DNS setup.

Related resources

- [Changing your domain nameservers to Cloudflare](#)
- [Why can't I add my domain to Cloudflare?](#)
- [Getting started with Cloudflare](#)
- [Contacting Cloudflare support](#)
- [Cloudflare Community: Getting started](#)

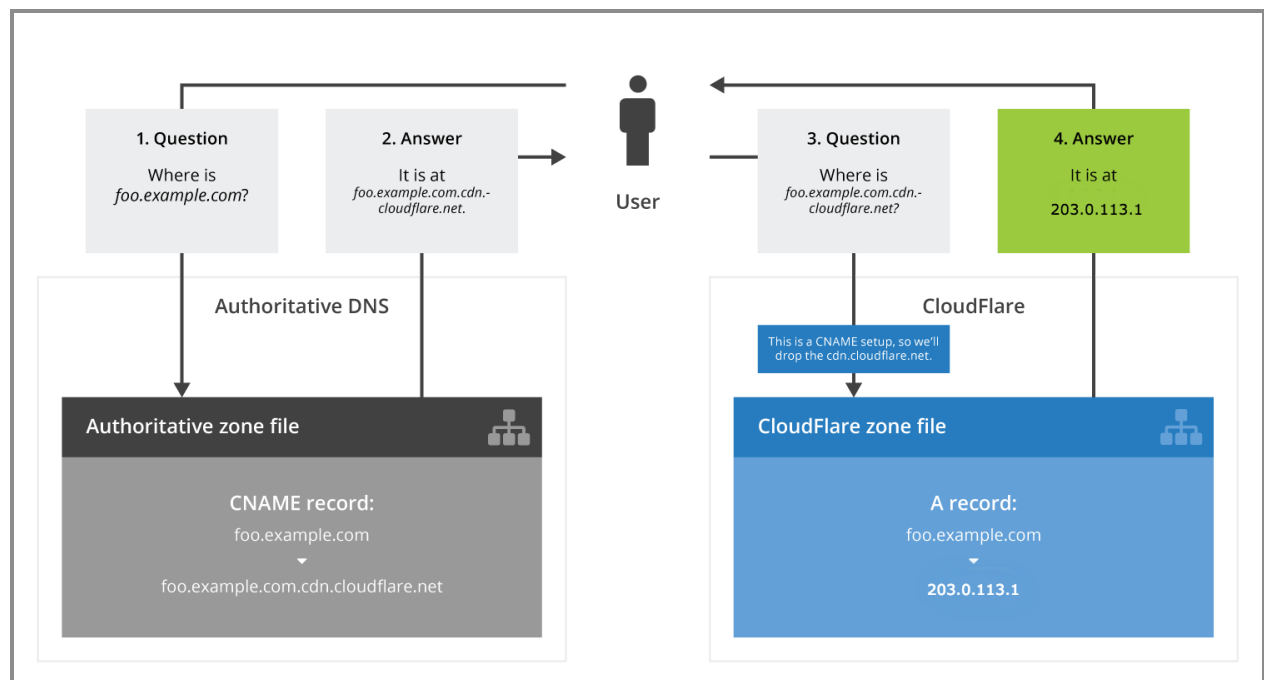
CNAME Setup

Overview

A CNAME setup allows a customer to maintain authoritative DNS outside of Cloudflare. It allows individual subdomains to benefit from Cloudflare's services without requiring updates for a domain's registration to point to Cloudflare's nameservers for DNS resolution.

Be careful not to confuse CNAME setup terminology with *CNAME records* which are available in the **DNS** app for all plan types.

The logical flow of a DNS lookup for a domain on a CNAME setup is shown in the diagram below:



Limitations

The CNAME setup has two limitations:

1. DDoS protection for attacks against DNS infrastructure is only available for the delegated subdomain records.
2. Only subdomains, not the root domain, can use Cloudflare's services. This limitation is imposed by Internet DNS specifications.

Add a redirect at your origin web server (such as in an `.htaccess` file) to forward traffic for the root domain to a subdomain proxied to Cloudflare.

CNAME Setup Configuration

Task 1 - Activating CNAME setup for a domain

1. Following the steps in the previous section
 2. A *TXT record* will appear in the Cloudflare **DNS** (or **Overview**) tab under the **Verification TXT Record** section. Add the *TXT record* to your authoritative DNS.
The TXT record must remain in authoritative DNS for the duration Cloudflare's services are utilized.
 3. It will take up to a few hours for Cloudflare to verify the *TXT record* and send a confirmation email.
-

Task 2 - Provision Cloudflare Universal SSL for CNAME setup

Cloudflare's Universal SSL certificate will be deployed once a domain is [activated on the CNAME setup](#) and proper Domain Control Validation (DCV) records have been added to authoritative DNS:

Option 1 - Upload your own SSL certificate

Navigate to the SSL/TLS tab. Under the "Edge Certificates" card press the "Upload Custom SSL Certificate" button. This will bring up a modal where you can enter the contents from your .cert and .key respectively.

Note: the .cert and .key must in the .pem format.

Option 2 - Use Cloudflare's Universal SSL

Cloudflare will provision a certificate for each record that exists within the DNS tab. By default, HTTP validation is used. Once the record is proxied, it will be deployed.

Alternatively, you can "pre-activate" the certificates by changing the validation method to TXT/CNAME.

- a. Call this [API](#) to get the cert_pack_uuid
- b. Call this [API](#) to change the certificate validation method using the cert_pack_uuid required for this API call.

Edge Certificates

Your plan allows you to upload 1 SSL certificate pack, which you must renew and re-upload prior to expiration.

You may also order an auto-renewing certificate.

[Order SSL Certificate](#)
[Upload Custom SSL Certificate](#)

Hosts	Type	Status	Expires on
erfi.ml	Universal	Initializing	(Managed)
www.erfi.ml	Universal	Pending Validation (TXT)	(Managed)

Review Universal Certificate for www.erfi.ml

Cloudflare will validate the certificate on your behalf only for zones that are proxying traffic.

Certificate validation TXT name

[Click to copy](#)

Certificate validation TXT value

[Click to copy](#)

Certificate Validity Period 1 year

Validation method TXT

[<](#)
[>](#)
1–2 of 2 certificates

[API](#)
[Help](#)

Option 3 - Dedicated Certificates

If provided in the contract, select Order SSL/TLS certificate, and follow the steps till you've reached the validation modal:

Order SSL Certificate

Select Type

Add Hostnames

Validate Domain

Finish

Validate Domain

Before we can order a certificate for your domain, we must verify that you control it. To do so you can either add a DNS CNAME record, or click on an email sent to one of the email addresses listed below.

Validate domain using email

Validate domain by adding DNS CNAME record

Add the following record to your DNS provider and then click the "I've added the CNAME to my DNS server" button below.

Type	Name	Value
CNAME	_ca3-471c76c5164f4565ab9bca4cb8619c54.erfi.ml	dcv.digicert.com

[Back](#)
[Cancel](#)
[I've added the CNAME to my DNS server](#)

Add the records to your current DNS provider and wait till the certificate is validated, and deployed.

Task 3 - Adding DNS records to a CNAME setup

Once a CNAME setup is enabled, DNS records must be updated in both Cloudflare's **DNS** tab and your authoritative DNS:

1. Add an *A* or *CNAME* record in the Cloudflare **DNS** tab for the subdomain.

An orange-cloud icon beside the DNS record will proxy traffic to Cloudflare.

2. Edit the corresponding *CNAME* record in your authoritative DNS to append **.cdn.cloudflare.net** to the hostname.

For example, when configuring **www.example.com** on a *CNAME* setup with Cloudflare, the *CNAME* record in authoritative DNS would need to point to **www.example.com.cdn.cloudflare.net**.

www.example.com CNAME www.example.com.cdn.cloudflare.net

If *www.example.com* is currently an *A* record in your authoritative DNS, it must be changed to a *CNAME*.

CNAME records can be added to your authoritative DNS for each subdomain to be proxied to Cloudflare.

Related resources

- [Managing DNS records in Cloudflare](#)
- [What is Domain Control Validation \(DCV\)](#)
- [Changing DCV method](#)

FULL Setup - SSL/TLS Certificates

Option 1 - Upload the Custom SSL for desired hostname(s)

On the SSL/TLS | Edge Certificates card, press the "Upload Custom SSL Certificate" button to set up your existing SSL certificate with us. You will need both the private key and the certificate to proceed.

Option 2 - Cloudflare Universal SSL certificates

You will be automatically provisioned Cloudflare Universal SSL certificates. By default, our certificates are issued with the root and wildcard, so we can secure the root domain and one level of subdomains. Check the SSL/TLS | SSL panel for the "Active Certificate" message that will be displayed when the certificate pack has been issued by our certificate issuing partner, and deployed globally on Cloudflare.

Option 2b - Pre-activating Universal SSL Certificate

If using CF certificates, setting up SSL/TLS before migration to ensure there are no SSL errors.

Click on the certificate modal, and retrieve the TXT record to add to your current DNS provider so that the certificate can be provisioned.

Alternatively, you can:

1. Call this [API](#) to get the cert_pack_uuid
2. Call this [API](#) to change certificate validation method using the cert_pack_uuid required for this API call:

You can choose either TXT or CNAME to add on your current DNS provider to validate the certificate and activate it before the nameserver migration.

Option 3 - Dedicated Certificates

As you would have already done either the automatic HTTP validation after the name-server change or the USSL pre-activation, ordering a dedicated certificate so that the common name matches your domain instead of a shared one in the USSL will be automatically activated and deployed upon completion of the order.

[← Back](#)

Change your nameservers

i Pointing to Cloudflare's nameservers is critical for activating your site successfully. Otherwise, Cloudflare is unable to manage your DNS and optimize your site.

Edge Certificates

Your plan allows you to upload 1 SSL certificate pack, which you must renew and re-upload prior to expiration.

You may also [order an auto-renewing certificate](#).

[Upload Custom SSL Certificate](#)

Hosts	Type	Status	Expires on
*.erfi.ml, erfi.ml	Universal	Pending Validation (TXT)	(Managed)
<div> 1–1 of 1 certificates</div>			
<div>API Help </div>			

1. Log in to your registrar account

Determine your registrar via [WHOIS](#).

Remove these nameservers:

```
ns03.freenom.com
ns04.freenom.com
ns02.freenom.com
ns01.freenom.com
```

2. Replace with Cloudflare's nameservers:

Nameserver 1

```
jeremy.ns.cloudflare.com
```

[Click to copy](#)

Nameserver 2

```
lola.ns.cloudflare.com
```

[Click to copy](#)

Check to make sure they're correct, then **Save your changes**.

Registrars typically process nameserver updates within 24 hours. Once this process completes, Cloudflare confirms your site activation via email.

[Learn how to change nameservers in Cloudflare.](#)

[Done, check nameservers](#)

FULL Setup - Changing your domain nameservers to Cloudflare

Overview


To route web traffic through the Cloudflare network, update the nameservers at your domain registrar to resolve your domain's DNS with Cloudflare's nameservers. Updating your nameservers does not change where your website is hosted. Also, you can still use OpenDNS, Google DNS, etc for recursive DNS although Cloudflare recommends the [1.1.1.1 resolver](#).

Changing nameservers is not required for Business and Enterprise domains on [CNAME setups](#).

Change your domain nameservers

To change your domain nameservers,

1. Enter your domain at [ICANN WHOIS](#) field:


**ICANN WHOIS**

[ABOUT WHOIS](#)[POLICIES](#)[GET INVOLVED](#)[WHOIS COMPLAINTS](#)[KNOWLEDGE CENTER](#)

[Lookup](#)

By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#).

Showing results for: example2.com
Original Query: example2.com



contact information redacted

Registrar

WHOIS Server: whois.godaddy.com
URL: <http://www.godaddy.com>
Registrar: GoDaddy.com, LLC
IANA ID: 146
Abuse Contact Email: abuse@godaddy.com
Abuse Contact Phone: +1.4806242505

Status

Domain Status:ok <http://www.icann.org/epp#ok>

Important Dates

Updated Date: 2018-10-20
Created Date: 2001-11-09
Registrar Expiration Date: 2019-11-09

Name Servers

NS67.DOMAINCONTROL.COM
NS68.DOMAINCONTROL.COM

Submit a Complaint for WHOIS
[WHOIS Inaccuracy Complaint Form](#)
[WHOIS Service Complaint Form](#)
[WHOIS Compliance FAQs](#)

2. Log into the administrator account for your domain registrar.

If you didn't copy the Cloudflare nameservers when initially adding your domain to Cloudflare, click on the Cloudflare **Overview** app to identify your Cloudflare nameservers as shown in this [video](#).

3. Replace the current nameserver records in your registrar account with your domain's Cloudflare nameservers. Allow **up to 72 hours** for nameserver changes to globally propagate.

Use the **Re-check now** button the Overview dashboard to finalize the nameserver update.

Contact your registrar's support center for the most accurate information. See below for instructions on changing nameservers at popular registrars:

Certain European registrars have a different nameserver registration process. [Contact Cloudflare support](#) if you experience issues.

Contact your registrar's support center for the most accurate information. See below for instructions on changing nameservers at popular registrars:

1and1	FlokiNET	Name.com
Blacknight	Gandi	NameCheap
BlueHost	GoDaddy	Network Solutions
DirectNIC	Google Domains	OVH
DNSMadeEasy	HostGator	Rackspace
Domain.com	HostMonster	Register
Dotster	Internetbs	Site5
DreamHost	iPage	Softlayer
EasyDNS	MediaTemple	Tucows
Enom	MelbourneIT	Yahoo!
Fast Domain	Moniker	Yola
101Domain		

4. Refresh the Cloudflare **Overview** app. If “**Complete your nameserver setup**” still appears, Perform the following steps:

- Ensure the **Name Server** output correctly spells the Cloudflare nameservers and confirm Cloudflare's nameservers are the only nameservers listed.
- If the **Name Server** output is correct, click the **Re-check now** button in the Cloudflare Overview app.

5. If “**Complete your nameserver setup**” no longer appears in the Cloudflare **Overview** app, you have successfully updated your nameservers and your domain is active at Cloudflare.

Once your domain is active on Cloudflare, review our [best practices for active Cloudflare domains](#).

If you run into issues, refer to our [Troubleshooting FAQ for new Cloudflare customers](#).

Confirm traffic is proxied to Cloudflare

Some online tools such as [GTmetrix](#) don't recognize Cloudflare as a Content Delivery Network ([CDN](#)) because we don't operate like a traditional [CDN](#). Instead, confirm your domain traffic actively proxies through Cloudflare by browsing to **<https://www.example.com/cdn-cgi/trace>**.

Replace **www.example.com** with the domain and hostname proxied to Cloudflare. If proxied to Cloudflare, output similar to the following appears in the browser:

```
fl=4f177
h=www.example.com
ip=2001:1900:2200:7525:749f:9ed1:444c:80b4
ts=1562191016.292
visit_scheme=https
uag=Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/74.0.3729.157 Safari/537.36
colo=SJC
http=http/2
```

```
loc=US
```

```
tls=TLSv1.3
```

```
sni=plaintext
```

```
warp=off
```

If you don't observe similar output:

1. Confirm your DNS record is [orange-clouded](#) in the Cloudflare **DNS** app,
2. Enter your domain at [ICANN WHOIS](#) to confirm the **Name Servers** only list Cloudflare nameservers for your domain, or
3. [Contact Cloudflare Support](#).

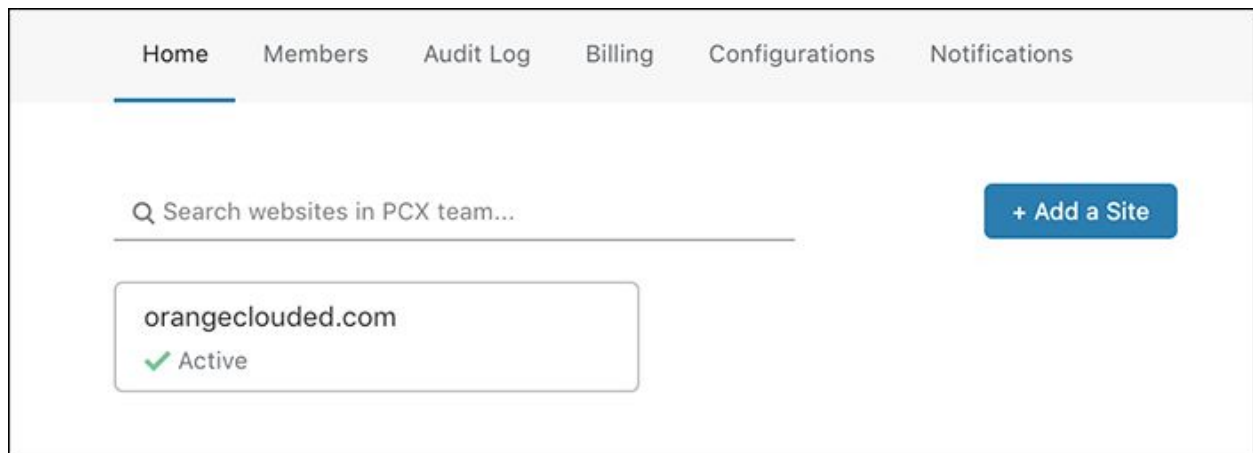
Related resources

- [Creating a Cloudflare account and adding a website](#)
- [Best practices for active Cloudflare domains](#)
- [Troubleshooting FAQ for new Cloudflare customers](#)
- [Understanding the Cloudflare dashboard](#)
- [Contacting Cloudflare support](#)

Understanding Domain Status

Overview

When a domain is successfully [added to Cloudflare](#), it appears as *Active* in the dashboard.



A Cloudflare domain's nameservers are periodically checked to confirm that the nameservers point to Cloudflare. However, if a check fails or if you do not [complete the sign-up process](#) you may see a different status based on where you left off in the process. You will receive an email to the email address on file when your domain's status changes.

Possible domain statuses include:

- *Setup*: the sign-up process was initiated but the domain has not been authenticated
- *Pending Nameserver Update*:
 - if using Cloudflare as your [authoritative DNS](#): a Cloudflare plan type was selected and domain nameservers may have been changed, but are not yet authenticated
 - if using a [CNAME set up](#), the verification .txt record to validate ownership of your domain was not added or authenticated at your authoritative DNS
- *Active*: Cloudflare has authenticated the nameserver changes and traffic can be proxied to Cloudflare.

- *Moved*: your domain has failed multiple DNS checks, indicating that your authoritative DNS no longer points to Cloudflare nameservers.

Domains remaining in the Pending Nameserver Update or Moved status are eventually removed from the dashboard and the Cloudflare network. Review our documentation on [recovering a deleted domain](#) for troubleshooting tips.

To ensure that your domain remains Active, complete the sign-up process as described in [Getting Started with Cloudflare](#) and ensure that your DNS settings are properly configured.

Related resources

- [Getting Started with Cloudflare](#)
- [Configuring a CNAME setup](#)
- [Why was my domain deleted from Cloudflare?](#)

Identifying network ports compatible with Cloudflare's proxy

Overview

By default, Cloudflare proxies traffic destined for the HTTP/HTTPS ports listed below.

HTTP ports supported by Cloudflare:

- 80
- 8080
- 8880
- 2052
- 2082
- 2086
- 2095

HTTPS ports supported by Cloudflare:

- 443
- 2053
- 2083
- 2087
- 2096
- 8443

If traffic for your domain is destined for a different port than listed above, either:

- Add the subdomain as a [gray-clouded record](#) via your Cloudflare **DNS** app, or
- Enable [Cloudflare Spectrum](#).

Block traffic on ports other than 80 and 443 for Pro, Business, and Enterprise domains via [WAF](#) rule id 100015: "Anomaly:Port - Non Standard Port (not 80 or 443)".

Ports 80 and 443 are the only ports compatible with:

- HTTP/HTTPS traffic within China data centers for domains that have the **China Network** enabled,
- Proxying of [Cloudflare Apps](#), and
- [Cloudflare Caching](#).

[Cloudflare Access](#) does not support port numbers in URLs. Port numbers are stripped from requests for URLs protected through Cloudflare Access.

Related resources

- [Identifying subdomains compatible with Cloudflare's proxy](#)
- [Cloudflare Spectrum](#)
- [Managing DNS records at Cloudflare](#)

Allowing Cloudflare IP addresses

Overview

Changing your name servers to Cloudflare routes traffic through Cloudflare for any orange-clouded DNS records in the Cloudflare DNS app. Your origin web server receives traffic from Cloudflare IP addresses due to Cloudflare's reverse proxy.

Blocking or rate limiting Cloudflare connections prevents visitor traffic from reaching your website.

To avoid blocking Cloudflare IPs unintentionally, check that:

- Your origin web server iptables are set to trust Cloudflare IPs.
- Bad Behavior or mod_security plugins are up to date.
- Your htaccess file allows Cloudflare IPs.
- Any security plugins, such as WordPress security plugins, allow Cloudflare IPs.

Allow Cloudflare IP addresses

For Cloudflare to send visitor requests to your origin web server, allow Cloudflare IP addresses at your origin web server. Contact your hosting provider or website administrator for guidance.

Also, consult documentation for walkthroughs on using .htaccess or iptables to allow IP addresses. The following examples demonstrate the format of an iptables rule to allow a Cloudflare IP address range. Replace \$ip below with one of the Cloudflare IP address ranges.

For IPv4 address ranges:

```
iptables -I INPUT -p tcp -m multiport --dports http,https -s $ip -j ACCEPT
```

For IPv6 address ranges:

```
ip6tables -I INPUT -p tcp -m multiport --dports http,https -s $ip -j ACCEPT
```

You may also consult the following resources for help in allowing Cloudflare IPs for these Wordpress plugins:

- [iThemes Security](#)
- [Wordfence](#)

Related resources

- [Is Cloudflare compatible with Bad Behavior?](#)
- [What are Cloudflare's IPs?](#)

Configuring IP Access Rules

Overview

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 (APIs, crawlers, payment providers, etc). **IP Access Rules** allow *allowlist*, *block*, and *challenge* actions for traffic based on the visitor's IP address, country, or AS number.

There are four configurable actions for an **IP Access Rule**:

- *Allowlist*: Excludes visitors from all security checks (Browser Integrity Check, I'm Under Attack Mode, the WAF, etc). This is useful if a trusted visitor is blocked by Cloudflare's default security features. *Allowlist* takes precedence over *block*.

Allowing a country code does not bypass Cloudflare's WAF.

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. Firewall events downloaded from the API show **rule_id** as *security_level* and **action** as *drop* when this behavior occurs.

- *JavaScript Challenge*: Presents the [I'm Under Attack Mode](#) interstitial page to visitors. Requires a visitor's browser or client to support JavaScript. Useful for blocking DDoS attacks with minimal impact to legitimate visitors.
- *Challenge*: Requires the visitor to complete a [CAPTCHA](#) before visiting your site. Prevents bots from accessing the site.
- *Block*: Prevents a visitor from visiting your site.

Add an IP Access Rule

To create an **IP Access Rule**, follow these steps:

1. Log in to your Cloudflare account.
2. Select your domain.
3. Click the **Firewall** app.
4. Click on the **Tools** tab.
5. Under **IP Access Rules**, enter the following details:
6. Enter the **Value** as an IP, IP range, or two-letter country code.
7. Select an **Action**.
8. Select whether the rule **applies to** *This website* or *All websites in the account*.
9. (Optional) add a **Note** (i.e. *Payment Gateway*).
10. Click **Add**.

Also, you can programmatically block or trust IPs via the [Cloudflare API](#). Cloudflare supports the 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.

Types of Access Rules

There are several types of Access Rules:

Type	Example Value
IPv4 address	192.0.2.3
IPv4 /24 range	192.0.2.0/24
IPv4 /16 range	192.0.0.0/16
IPv6 address	2001:db8::
IPv6 address range	2001:db8::/48, 2001:db8::/64
Country (by name or code)	US, germany, tor, CN
Autonomous System Number (ASN)	AS13335

IPs globally allowed by Cloudflare override a *Country* block via IP Access Rules but not a *Country* block via [Firewall Rules](#).

Address range examples

CIDR	Start of range (example)	End of range (example)	Number of addresses
/64	2001:db8::	2001:db8:0000:0000:ffff:ffff:ffff:ffff	18,446,744,073,709,551,616
/48	2001:db8::	2001:db8:0000:ffff:ffff:ffff:ffff:ffff	1,208,925,819,614,629,174,706,176
/32	2001:db8::	2001:db8:ffff:ffff:ffff:ffff:ffff:ffff	79,228,162,514,264,337,593,543,950,336
/24	192.1.2.0	192.1.2.255	256
/16	192.1.0.0	192.1.255.255	65,536

IP Access Rule limits

Accounts are limited to a maximum of 50,000 rules. Enterprise customers can request increased rule limits via their Account Team.

Two-letter country codes

The full list of the two letter country codes is in the [ISO 3166-1 Alpha 2 format](#) needed to create Access Rules for the IP Firewall.

Related resources

- [Understanding your site protection options](#)
- [Firewall Analytics](#)

Understanding the Cloudflare Dashboard

Overview

The Cloudflare Dashboard manages account and domain settings. Key dashboard features include:

- Control Cloudflare features,
- Gain insights into domain security and caching analytics,
- [Share account access](#)
- Configure settings from any device via our flexible dashboard design.

Changes update globally on Cloudflare's network **within 30 seconds**. This applies to configuration changes for all of Cloudflare's products and features except [cache purge](#), which can take **up to a minute**. Changes committed via the Cloudflare API and dashboard, as well as via [Terraform](#), all utilize the same API and underlying technology.

All Cloudflare plans allow [sharing account access with additional users](#). Additionally, Enterprise plans allow Administrators to create [Multi-User accounts](#) that allow each user to edit only those Cloudflare settings applicable to their role.

The Cloudflare dashboard requires a web browser that supports [TLS 1.2](#) or newer. The Cloudflare dashboard isn't supported on pre IE 10 browser versions. Visit [Browse Happy](#) for upgrade links to the most popular browsers.

Cloudflare uses tokens to authenticate a session when a user is logged in to their Cloudflare account. An invalid token or email error message appears if your ISP changes your IP address during your session as it invalidates the token. Log out, then log back in to correct the issue or clear your browser cache and cookies.

Summary of Cloudflare Dashboard apps

The Cloudflare dashboard contains several apps focused on providing [data insights](#), [optimizing security](#), providing [configuration flexibility](#), [improving performance](#), and enhancing site reliability.



The information below summarizes the utility of each dashboard app.

Insights

Overview

Provides the following functionalities:

- Summarizes site analytics
- Displays notifications
- Links to common quick actions
- Summarizes plan extensions and add-on features
- Provides API authentication details, including **Zone ID** and **Account ID**
- Allows changing domain plans
- Allows removing a site from Cloudflare

Analytics

Monitor statistics and trends on:

- Visitor traffic
- DNS request handling
- Threat detection
- Performance

Security

Spectrum

- [Protect all TCP/UDP ports](#) from layer 3 and 4 [Denial-of-Service attacks](#)
- Stop traffic snooping by enabling TLS encryption for TCP services

SSL/TLS

- Manage [Cloudflare's SSL certificate products](#)
- Adjust [browser supportability](#) by modifying TLS and encryption settings
- [Redirect all HTTP requests to secure HTTPS](#)

Firewall

- [Block or allow traffic](#) based on IP address, IP range, country, or user agent
- [Set rate limits](#) and restrict specific URL access to specific IPs
- Adjust [OWASP](#) and [WAF Rule](#) settings
- [Evaluate visitor's HTTP headers for threats](#)

Access

- [Eliminate VPNs without requiring changes at your origin](#)
- Protect internal resources by requiring authentication
- Control which users and groups have access to sensitive resources
- Review access logs

ScrapeShield

- [Protect sensitive information](#) from spammers and bots
- [Obfuscate email addresses](#) to prevent bot scraping
- [Prevent image hotlink abuse](#) from unapproved sites

Flexibility

Workers

- [Run JavaScript applications in a serverless execution environment](#)
- Scale applications without spending effort on infrastructure or operations
- Build granular control into requests and responses

Page Rules

- [Provides granular control](#) for many Cloudflare settings based on a matching URL
- [Cache static HTML](#)

Custom Pages

- [Create custom error pages](#) for IP blocks, WAF blocks, HTTP 5XX errors, Cloudflare HTTP 1XXX errors, and more

Apps

- [Preview and install](#) a wide range of apps that enhance your site's security, performance, analytics, design, etc.

Performance

DNS

- [Manage a domain's DNS records](#)
- [Select which A or CNAME records to proxy](#)
- Find the Cloudflare nameservers assigned to your domain

Speed

- [Improve load time on mobile devices](#)
- [Compress images to accelerate page load](#)
- Accelerate site speed by [minifying the size of your origin source code](#)

- [Defer loading JavaScript](#) until after your site is rendered

Caching

- [Adjust caching level](#)
- [Purge cached files](#) from all Cloudflare data centers
- [Tell Cloudflare what to cache](#) and [set Browser Cache TTL](#)

Network

- Toggle features that enhance network performance such as [HTTP/2](#) and [QUIC](#)

Traffic

- [Reduce latency and connection errors](#)
- [Protect origin web servers from IP address exposure](#) and attack
- [Balance traffic](#) and prevent disruptions

Stream

- [Encode, store, and deliver your videos](#)
- Automatically optimize format and bitrate for every device and network

Related resources

- [Getting started with Cloudflare](#)
- [Shared account access](#)
- [Multi-user domains \(Enterprise only\)](#)

Setting up Multi-User accounts on Cloudflare

Overview

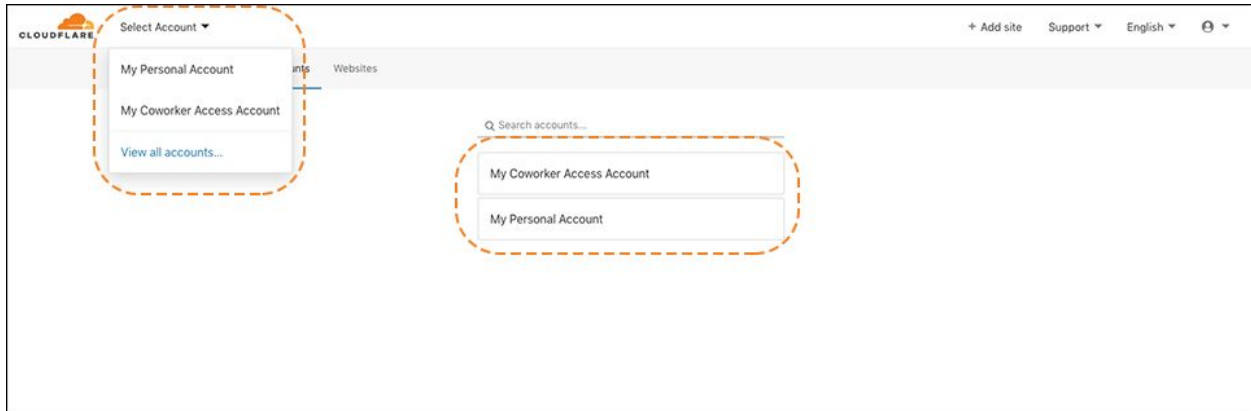
With a multi-user account, you can control multiple websites and invite users to manage Cloudflare settings on those websites. A user can access multiple accounts and have different permissions for each account that they can access.

There are two user roles: Super Administrator and Administrator. Super Administrators can edit all Cloudflare settings, make purchases, update billing, manage memberships and revoke access of other Super Administrators. As the account owner, you are automatically assigned the Super Administrator role.

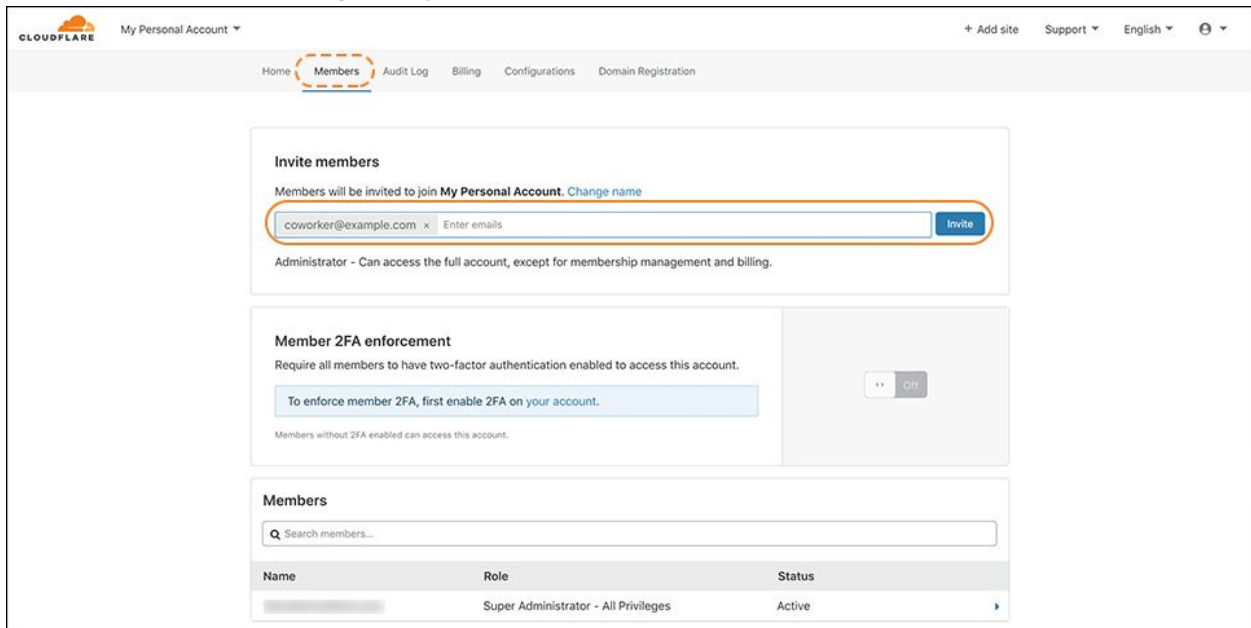
Administrators can edit all Cloudflare settings except for membership management and billing. When setting up your Cloudflare account, you are automatically assigned the Super Administrator role.

Set up a Multi-User account

1. Log in to the Cloudflare dashboard.
2. Choose the account that you would like to update.



3. Click the Members tab.
4. Enter the email address of the member you want to invite to your account. Click Invite. That member will receive an email invitation from Cloudflare to join your account.



User roles and permissions

All roles and permissions have access to the Overview app. For a detailed breakdown of available user roles and permissions, see below. Only Enterprise users can assign multiple roles to additional members.

Super Administrator - All Privileges

Can edit any Cloudflare setting, make purchases, update billing, and manage memberships. Super Administrators can revoke the access of other Super Administrators.

Administrator

Can access the full account, except for membership management and billing.

Administrator Read Only

Can access the full account in read only mode

Analytics

Can read Analytics.

Audit Logs Viewer

Can view Audit Logs.

Billing

Can edit the account's billing profile and subscriptions.

Cache Purge

Can purge the edge cache.

Cloudflare Access

Can edit Cloudflare Access policies.

Cloudflare for Teams

Can edit Cloudflare for Teams.

Cloudflare for Teams Read Only

Can access Cloudflare for Teams in read only mode.

Cloudflare for Teams Reporting

Can access Cloudflare for Teams reporting data.

Cloudflare Stream

Can edit Cloudflare Stream media.

Cloudflare Workers

Can edit Cloudflare Workers.

DNS

Can edit DNS records.

Firewall

Can edit WAF, IP Firewall, and Zone Lockdown settings.

Load Balancer

Can edit Load Balancers, Pools, Origins, and Health Checks.

Log Share

Can edit Log Share configuration.

Log Share Reader

Can read Enterprise Log Share.

SSL/TLS, Caching, Performance, Page Rules, and Customization

Can edit most Cloudflare settings except for DNS and Firewall.

Change Super Administrator

If you or someone in your organization leaves or loses access to email, you must change who is assigned the Super Administrator role. However, the process differs based on your plan type.

Enterprise users can have multiple Super Administrators associated with their accounts. To edit your Super Administrator, add an additional Member to your account and assign the role. Only remove the original Super Administrator from the account after adding the additional member.

Related resources

- [Securing user access with two-factor authentication](#)
- [Managing API Tokens and Keys](#)
- [Updating your Cloudflare email and password](#)

Managing API Tokens and Keys

Overview

The Cloudflare API exposes the entire Cloudflare functionality via a programmatic interface. You can manage your account settings, configure products, and develop applications using the Cloudflare API.

Using the Cloudflare API requires either an API token or API key to authenticate the source of the API request. To learn more about the authentication process, review the [Cloudflare API documentation](#).

An API key is unique to each Cloudflare user and used only for authentication. The API key does not authorize access to accounts or zones.

API tokens allow you to authorize access to specific Cloudflare apps, accounts, and zones with limited permissions. Each Cloudflare user can have up to 50 API tokens associated with their Cloudflare account.

API tokens are associated with the user that created them. If your Cloudflare account is invalidated or your permissions change, you will lose access to your API token.

If you manage a multi-user account, Cloudflare recommends creating a service account to issue tokens for automated production processes.

Generate API token

To generate an API token:

1. Log in to the Cloudflare dashboard.
2. Under the **My Profile** dropdown, click **My Profile**.
3. Click the **API tokens** tab.
4. Click the **Create Token** button. You will see the **Create Token** screen.

Communication **API Tokens**

API Tokens
Manage access and permissions for your accounts, sites, and products

Create Token

Token name	Permissions	Resources	Last used
No API tokens			

Help ▶

5. You have two configuration options to select from:

- Select *Custom* to manually set your desired token configuration. Then, proceed to Step 6.

← Back to view all tokens

Create

Token name

☒ Custom ☐ Start with a template

Permissions

Select edit or read permissions to apply to your accounts or websites for this token

Account ▼

Select... ▼

Select... ▼

Add more

Account Resources

Include ▼

All accounts ▼

Add more

Cancel Continue to summary

- Select *Start with a template* to choose from a list of common configurations. Choose a template, then click **Use template**. Then, proceed to Step 6.

[← Back to view all tokens](#)

Create

Token name

☐ Custom ☒ Start with a template

API tokens templates

Start with a template with common configurations to save time.

Template name	
Edit zone DNS	Use template
Read billing info	Use template
Read analytics and logs	Use template
Edit Cloudflare Workers	Use template
Edit load balancing configuration	Use template
Wordpress	Use template
Read all resources	Use template

6. Select the following edit or read **Permissions**:


- *Account or Zone Resources*: API token will include or exclude your account(s) or the domains and subdomains associated with your account(s).

7. Select the following edit or read **Resources**:

- *Account or Zone*: API token will apply to your account(s) or the domains and subdomains associated with your account(s).

[← Back to view all tokens](#)

Create a new API token from this template

Token name: Edit zone DNS 

Permissions

Select edit or read permissions to apply to your accounts or websites for this token

Zone Edit

Zone Resources

Include

8. Click **Continue to summary**.

9. Review the API token details, then click **Create Token** to finish. You will see a confirmation message with your API token.

10. Click **Copy** to save your API token on your computer. This token contains your secret key, so be sure to save it in a secure location.

Communication **API Tokens**

Edit zone DNS API token was successfully updated

Copy this token to access the Cloudflare API. For security this will not be shown again.

Test this token

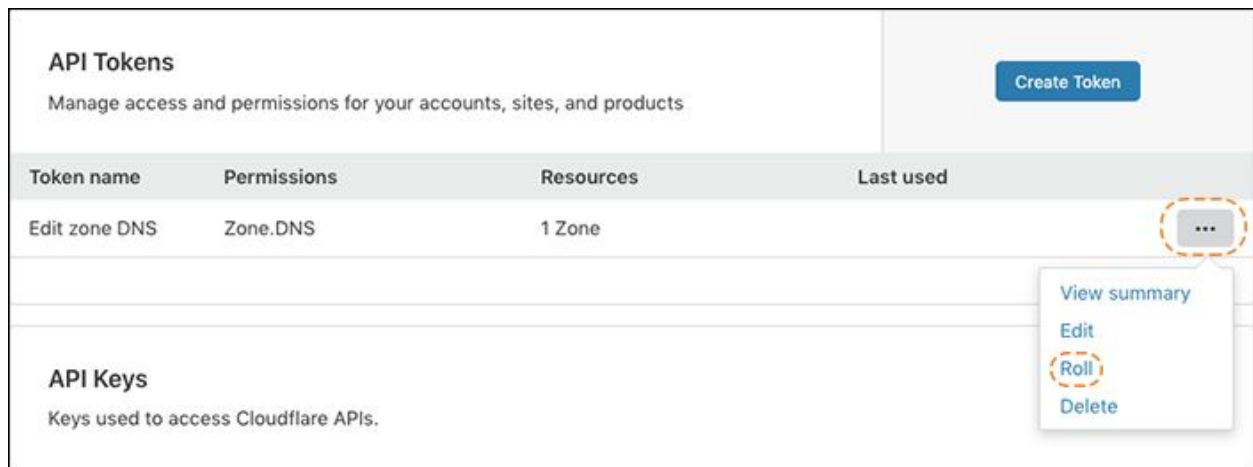
To confirm your token is working correctly, copy and past the below CURL command in a terminal shell to test.

```
curl -X GET "https://api.cloudflare.com/client/v4/user/tokens/verify" \
-H "Authorization: Bearer " \
-H "Content-Type:application/json"
```

Roll API token

If your **API token** is compromised or lost, you can either create a new token or *Roll* your secret key into a new one. Rolling your secret key will authorize the same access and permissions as the previous key.

To roll your API token, click *Roll* in the **API Tokens** section of the Cloudflare dashboard.



Then, click **Confirm** to continue and you will see a new API token secret key.

View API Key

To retrieve your API key:

1. Log in to the Cloudflare dashboard.
2. Under the **My Profile** dropdown, click **My Profile**.
3. Click the **API tokens** tab.
4. In the **API keys** section, choose one of two options: Global API Key or Origin CA Key. Choose the API Key that you would like to view.

The Global API Key is your main API key. The Origin CA Key is only used when creating origin certificates using the API.

5. To change your API Key, click **Change**. You will need to complete a Captcha before the change is applied.

API Keys

Keys used to access Cloudflare APIs.

Global API Key	Change View
Origin CA Key	Change View

[Help ▶](#)

The Global API key does not work for the Hosting Partner API. To retrieve your Hosting Partner key (also known as "Host API key"), review [these instructions](#). If you would like to become a Hosting partner, please [contact our hosting partner team](#).

Related resources

- [Cloudflare API documentation](#)
- [Where can I find the Partner API key?](#)

Using Cloudflare API with Postman Collections

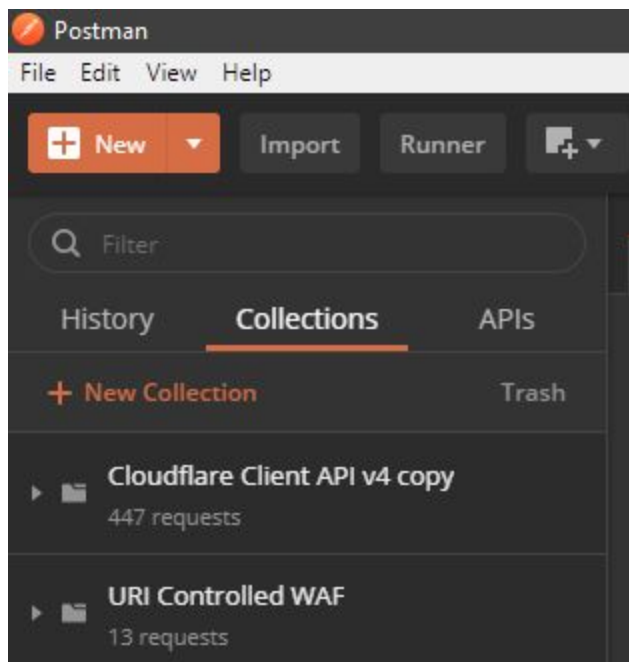
Cloudflare's client API gives users great customization power and potential for automation. It can be intimidating for users that aren't familiar with APIs or Command Line Interfaces.

Postman is an API client that makes API calls easier to make by giving the user a full Graphical User Interface. With Collections you can upload all of the formatting for all of our API calls so that it's plug and play. Find the full documentation on their site, <https://www.getpostman.com/collection>

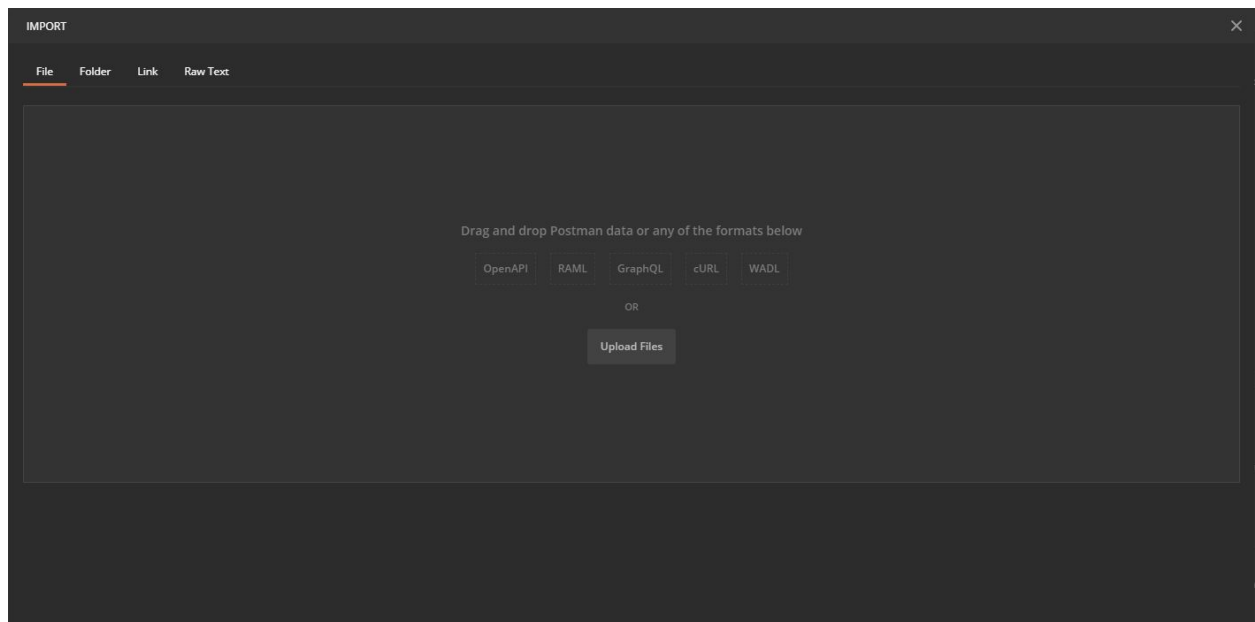
First you'll download the appropriate Postman client for your operating system.

They can be found at: <https://www.getpostman.com/>

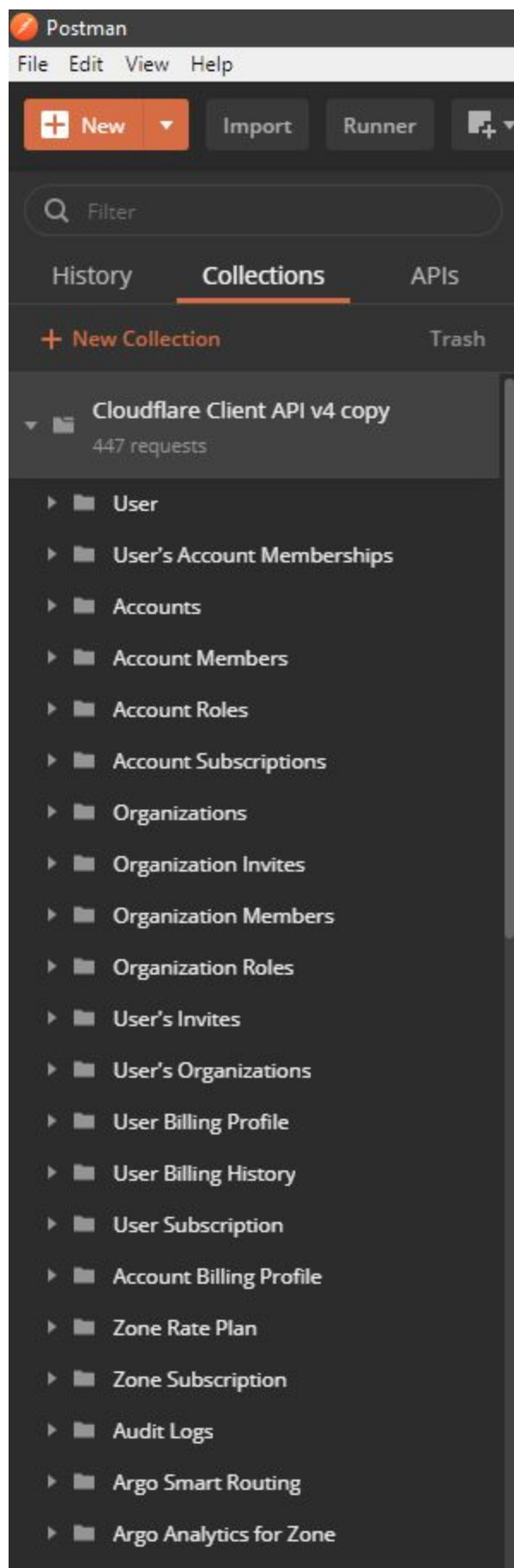
After downloading you'll select "Import" to upload the Cloudflare API collection (found at the bottom of this article):



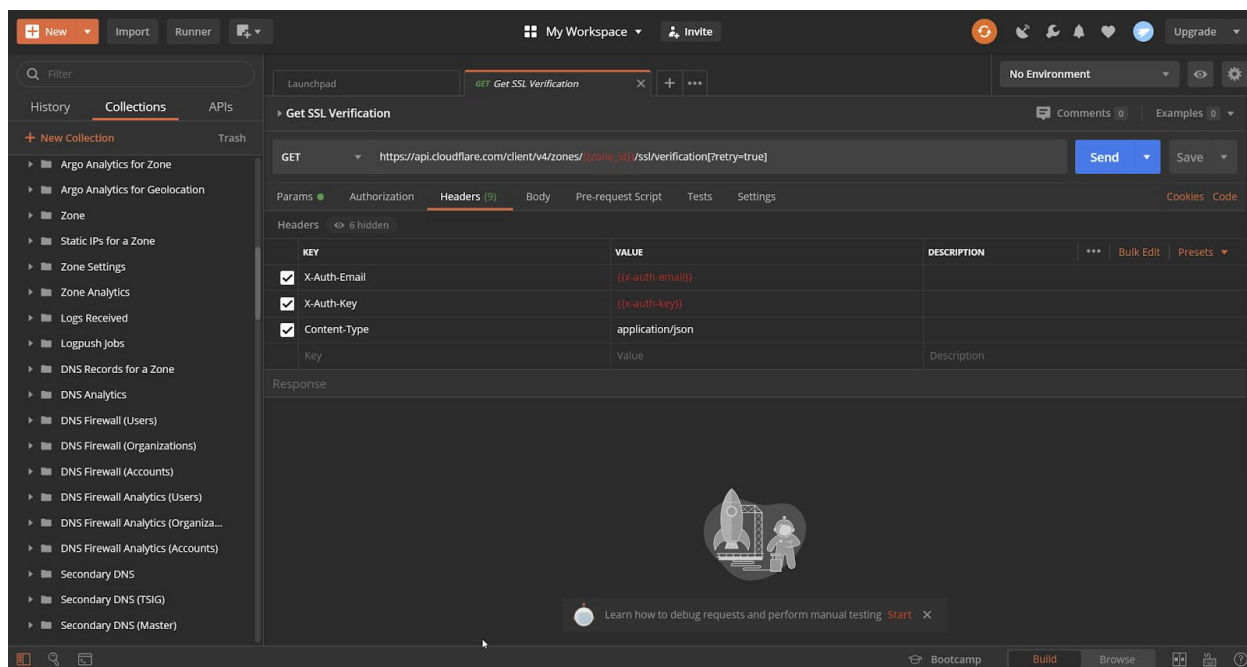
Then you can upload the .json collection file obtained here:



Then you can click on the "Cloudflare Client API v4 to the left to open all the individual API calls included in the collection:





After selecting an API call it's simple plug in play to send the request (don't forget to set your email and API key outlined below).




You'll find the Zone ID in the [overview](#) for each website in your account.


Domain Summary

 **Security Level:** [Medium](#)

 **SSL:** [Flexible](#)

 **Caching Level:** [Standard](#)

Development Mode: [Disabled](#)

 **Zone ID:**

207d323a739f25dd6ffc34fa6bbcc59b

Click to copy

[Get your API key](#) [API documentation](#)

Then the API "Auth-key" is found in your [profile](#). For everything except Origin CA you'll use the "Global API key"

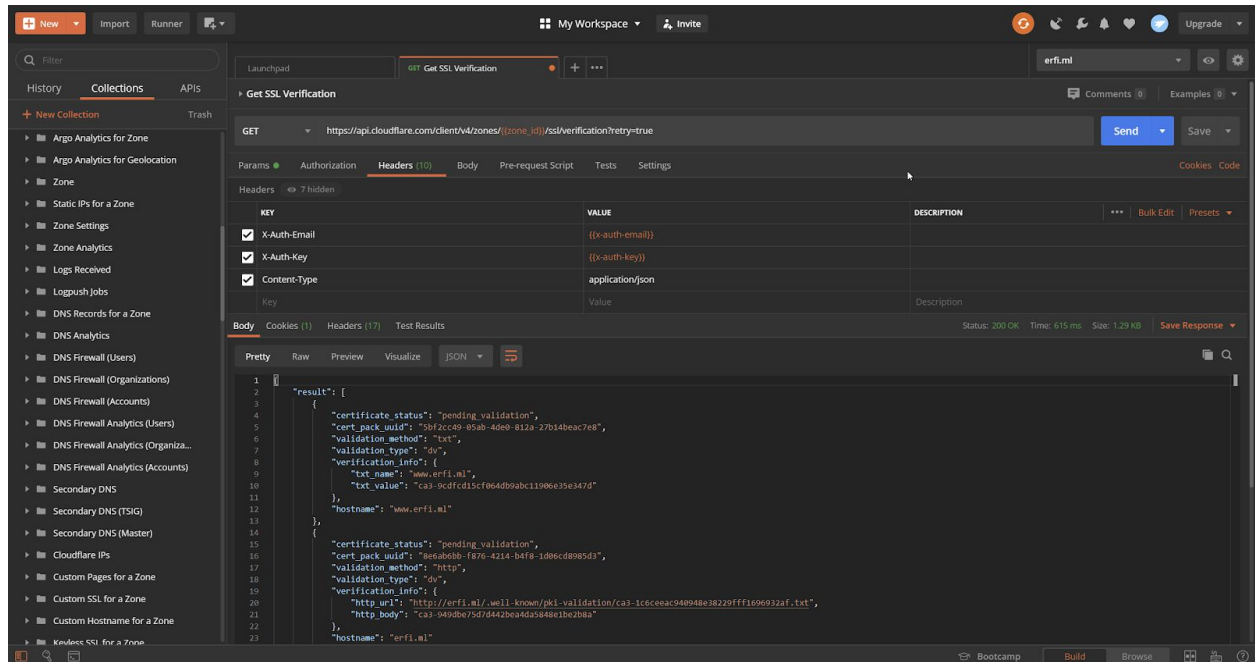
API Key

Your API key is used to access Cloudflare APIs.

Global API Key	View API Key	Change API Key
Origin CA Key	View API Key	Change API Key

[Help](#)

Then you just fill in your info and press send. The results will print below.



Related resources

- [Cloudflare API documentation](#)
- [Cloudflare Postman Collection](#)

Troubleshooting FAQ

Overview

Below are the most common customer questions and issues experienced when adding new domains to Cloudflare. If you are experiencing issues not mentioned below, the [Cloudflare Community](#) and [Cloudflare Help Center](#) are great ways to find quick answers.

Questions

- [Why do I see Cloudflare's IPs in my origin web server logs?](#)
- [Why doesn't my CNAME record resolve?](#)
- [Why is my site served over HTTP instead of HTTPS?](#)
- [Why is my Cloudflare Universal SSL certificate not active?](#)

Issues

- [SSL errors in appear in my browser](#)
- [I see 525 or 526 errors or redirect loops](#)
- [SSL isn't working for my second-level subdomain \(i.e. `dev.www.example.com`\)](#)
- [Why is my site content not properly rendering? Why do I see mixed content errors?](#)
- [My domain's email stopped working](#)
- [Why was my domain deleted from Cloudflare?](#)

Related resources

- [SSL FAQ](#)
- [DNS FAQ](#)
- [Understanding the Cloudflare dashboard](#)
- [Gathering information to troubleshoot site issues](#)
- [Contacting Cloudflare support](#)