

Using Cloudflare

Cloudflare DNS:

If you wish to use Cloudflare for DNS ONLY, you can configure it just like any other DNS provider, and simply [follow the steps for adding a custom domain as usual](#).

WARNING: Your domain DNS entry must have a GRAY cloud, not an ORANGE (proxied) cloud next to the entry.



Using Cloudflare's proxy for your domain without additional configuration will cause all incoming connections to fail!



This is the correct image shown for DNS-only entries.

Cloudflare Proxy

Even though Elest.io automatically provides SSL and has a firewall, there can be advantages to using Cloudflare for Proxying traffic, notably DDoS attacks and automatic filtering of scripted attacks.

Note: [Cloudflare only proxies traffic on certain ports](#). If you want to use this hostname for SSH, FTP, or other services whose ports are not listed in the above link, you must configure Cloudflare to provide DNS only or use [Cloudflare's Spectrum offer](#).

Because Elest.io already creates an SSL certificate for your website trusted by a root CA, the recommended configuration is to set Cloudflare to use Strict SSL verification when connecting to your server.

Before continuing, ensure you have already configured the domains [as per the instructions on the previous page](#).

Option 1: To set up strict SSL verification for your **whole domain**:

1. Navigate to the `SSL/TLS` section of your domain's dashboard.

2. Select the "Full (strict)" option.
3. Your changes will be saved automatically. You're done!

SSL/TLS

Overview

Edge Certificates

Client Certificates

Origin Server

Custom Hostnames

Security

Access

Speed

Caching

Workers Routes

Rules

Network

Traffic

Custom Pages

Apps

✔ Your SSL/TLS encryption mode is Full (strict)

This setting was last changed 2 hours ago

Browser

Cloudflare

Origin Server

Off (not secure) ⓘ

No encryption applied

Flexible

Encrypts traffic between the browser and Cloudflare

Full

Encrypts end-to-end, using a self signed certificate on the server

Full (strict)

Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server

[Learn more about End-to-end encryption with Cloudflare.](#)

Create a Configuration Rule to customize these settings by hostname.

API Help

Option 2: To set up strict SSL verification for a **specific subdomain**:

1. In your domain's dashboard, navigate to Rules > Configuration Rules and click Create Rule
2. Name your rule, and configure the incoming request filters.

Edit Configuration Rule

Rule name (required)

Cloudflare SSL for Subdomain

Give your rule a descriptive name.

If...

When incoming requests match...

☐ All incoming requests
The rule will apply to all traffic

☒ Custom filter expression
The rule will only apply to traffic matching the custom expression

When incoming requests match...

Field	Operator	Value	
Hostname	equals	subdomain.example.com	And Or
e.g. example.com			

Expression Preview

[Edit expression](#)

```
(http.host eq "subdomain.example.com")
```

3. Configure the SSL to Strict

SSL (optional)

Configure SSL settings available in SSL/TLS > Overview tab.

Select SSL/TLS encryption mode

Strict

Cancel

Save

4. Click Save

Option 3: Manual configuration (Advanced)

If you need a custom implementation, you can disable the creation of an SSL certificate with the following steps.

Create a CNAME record for your Cloudflare entry and point to the CNAME provided for that service in the Elestio dashboard.

These changes can be overwritten in the future if you modify the list of domains via the Elest.io dashboard.

1) Connect to the VM with SSH and type this:

nano /opt/elestio/nginx/.env

there remove your domain from the first line and save with CTRL+X

then type this command:

cd /opt/elestio/nginx;
docker-compose down;
docker-compose up -d;

After that, nginx won't try again to obtain an SSL certificate for your domain.

Revision #4

Created 17 July 2023 15:44:13 by Daniel

Updated 17 July 2023 16:35:17 by Daniel