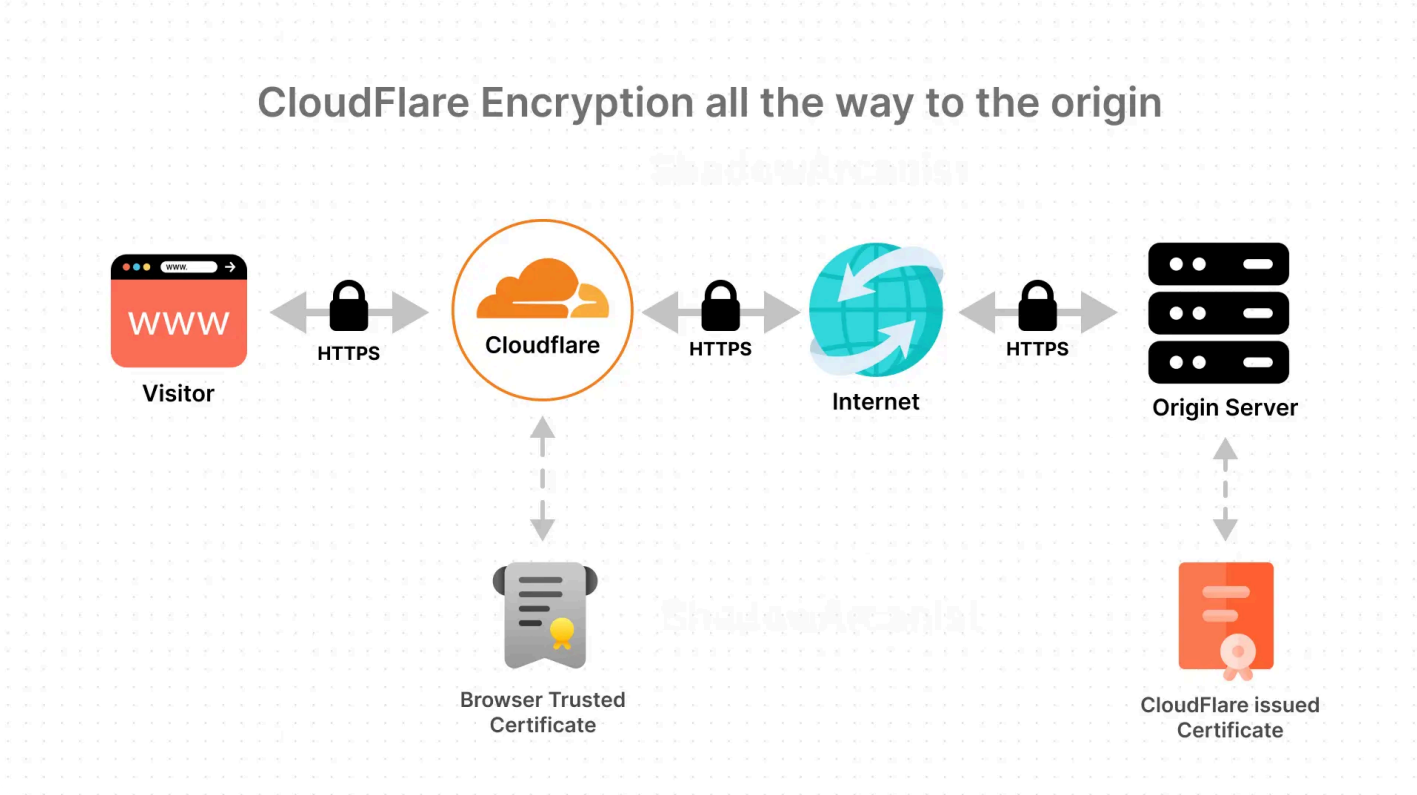
Cloudflare Origin Certificate



The Cloudflare Origin Certificate ensures secure communication between your server and Cloudflare when using Cloudflare's Proxy, CDN, and security features.

It encrypts the data exchanged between your server and Cloudflare, keeping it safe.

Why Use Cloudflare Origin Certificate with Coolify?

1. No need for HTTP or DNS challenges to create certificates.
2. Keep port 80 closed — everything happens securely over TLS.
3. Longer certificate validity (15 years) — once set up, you don't need to worry about renewing every few months.

When to Avoid Using Cloudflare Origin Certificate

Envix

access your server or apps.

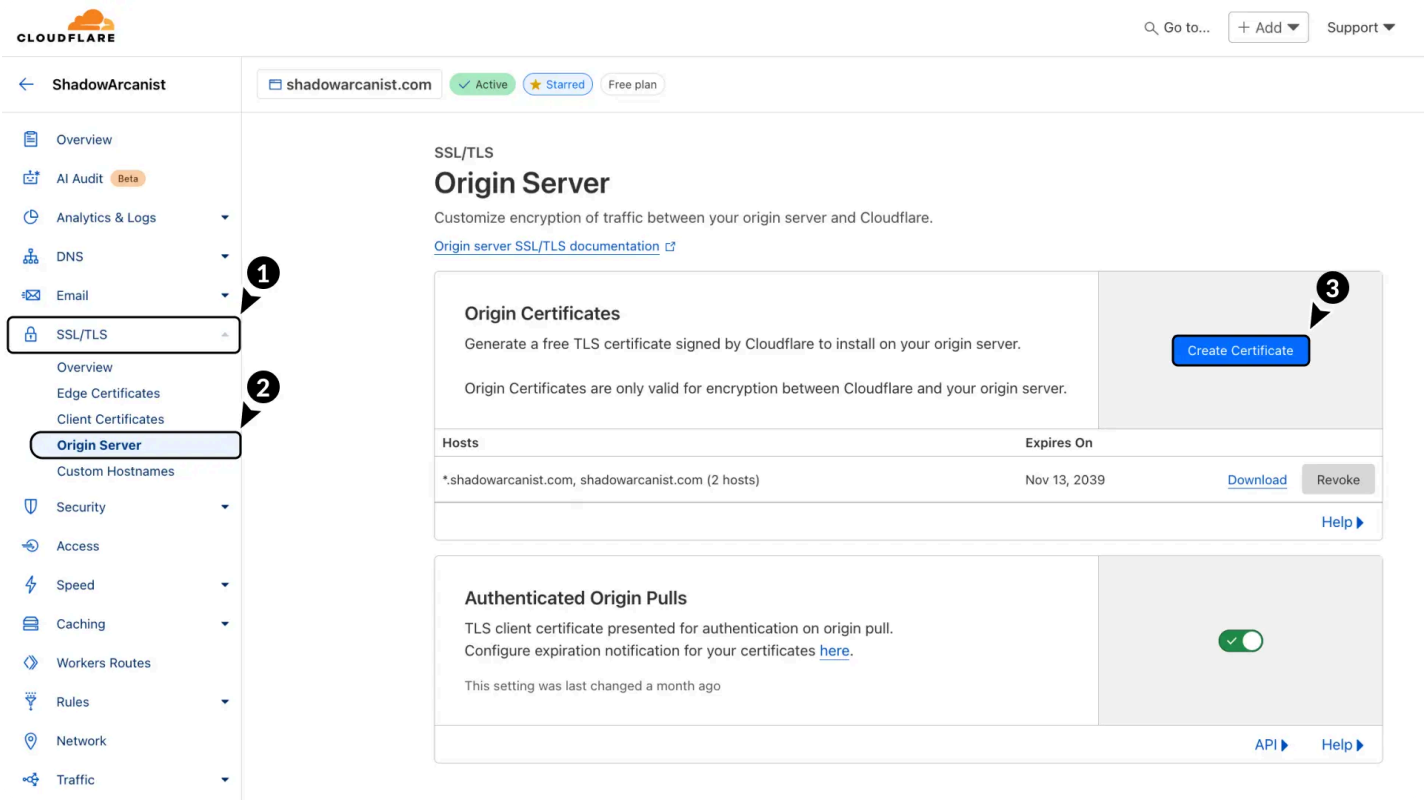
Example Data

The following data is used as an example in this guide. Please replace it with your actual data when following the steps:

- **IPv4 Address of Origin Server:** 203.0.113.1
- **Domain Name:** shadowarcanist.com
- **Username:** shadowarcanist

1. Create the Origin Certificate

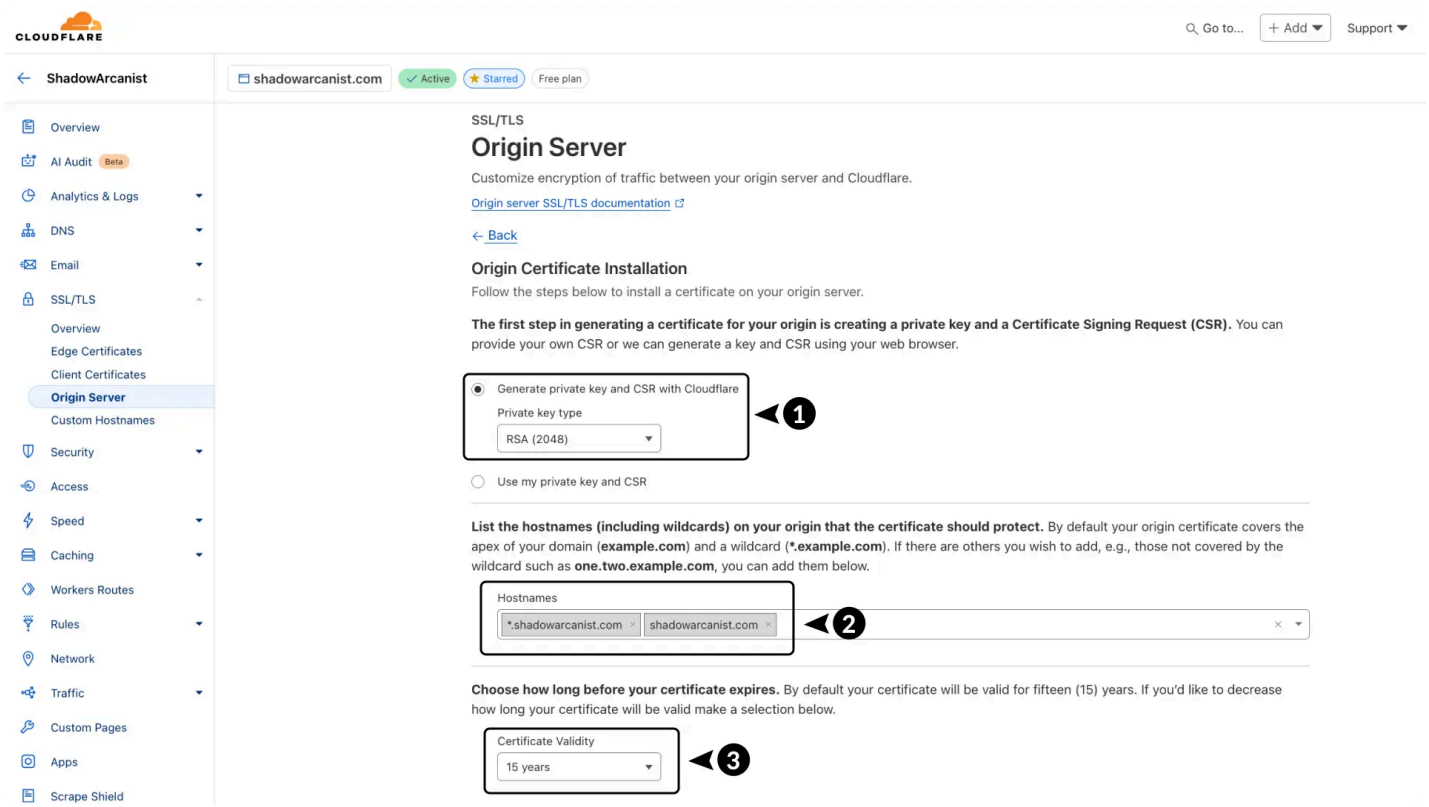
To create your Cloudflare Origin Certificate, follow these steps:



Envix

2. Select **Origin Server**.
3. Click the **Create Certificate** button.

You'll be asked to choose a private key type, hostnames, and certificate validity.

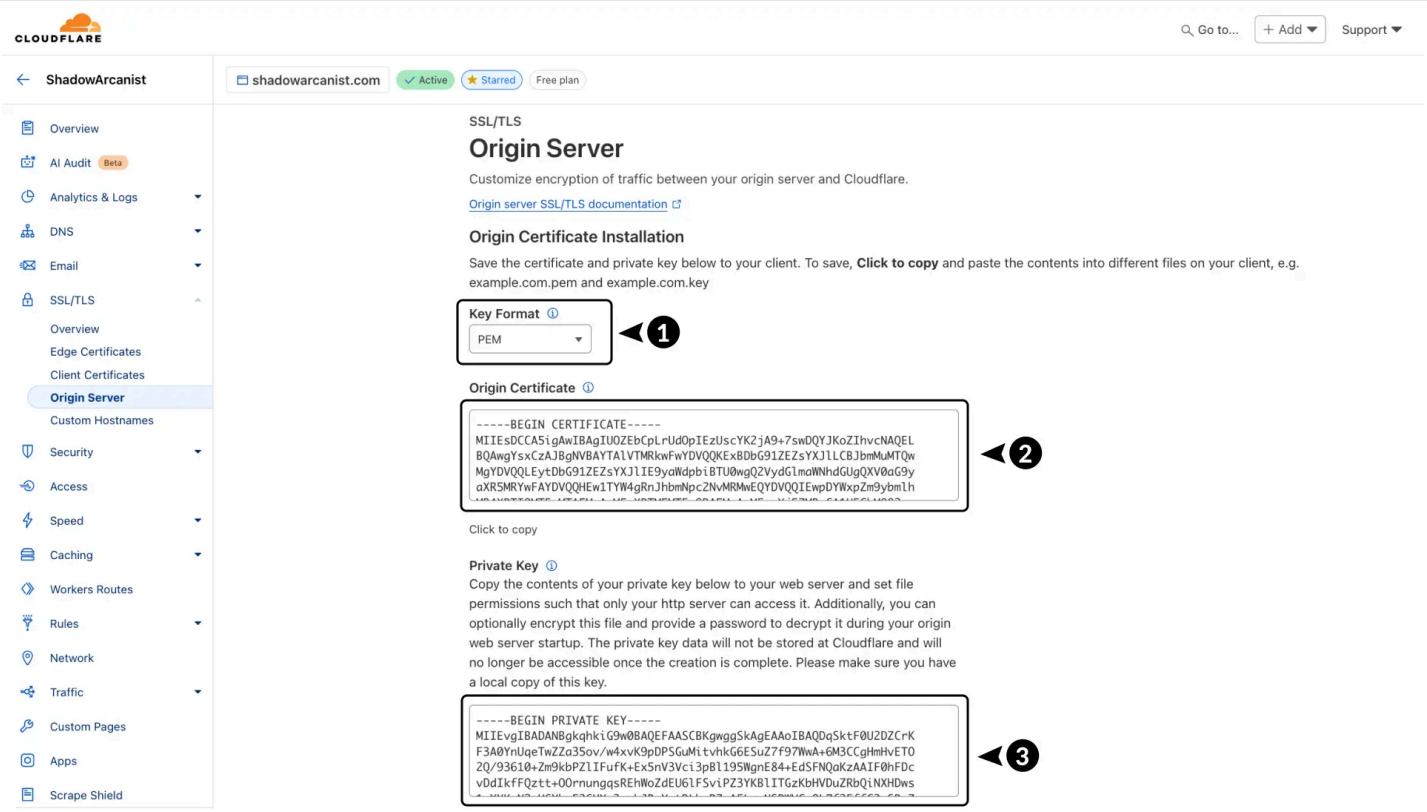


1. Choose **RSA (2048)** for the key type.
2. Add the hostnames you want the certificate to cover.

> **Note**
>
> - `shadowarcanist.com` will cover only the main domain.
> - `*.shadowarcanist.com` will cover all subdomains.
>
> On Cloudflare's free plan, wildcard certificates cover just one level of subdomains
>
> For example, it works for `coolify.shadowarcanist.com` but not `www.coolify.shadowarcanist.com`.
>
> To cover multiple levels, you'll need to purchase the Advanced Certificate Manager

3. Set the certificate validity to **15 years**.

Envix



Next, you'll add these to your server running Coolify and configure Coolify to use this certificate.

2. Add Certificate to Your Server

SSH into your server or use Coolify's terminal feature. For this guide, I'm using SSH:

```
ssh shadowarcanist@203.0.113.1
```

Once logged in, navigate to the Coolify proxy directory:

```
$ cd /data/coolify/proxy
```

Envix

```
$ ls
acme.json  docker-compose.yml  dynamic
```

If there's no **certs** folder, create it:

```
$ mkdir certs
```

Verify it was created:

```
$ ls
acme.json  certs docker-compose.yml  dynamic
```

Now, navigate into the **certs** directory:

```
$ cd certs
```

Create two new files for the certificate and private key:

```
$ touch shadowarcanist.cert shadowarcanist.key
```

Verify the files were created:

```
$ ls
shadowarcanist.cert shadowarcanist.key
```

Open the **shadowarcanist.cert** file and paste the certificate from the Cloudflare dashboard:

```
$ nano shadowarcanist.cert
```

Save and exit after pasting the certificate.

Do the same for the **shadowarcanist.key** file and paste the private key:

Envix

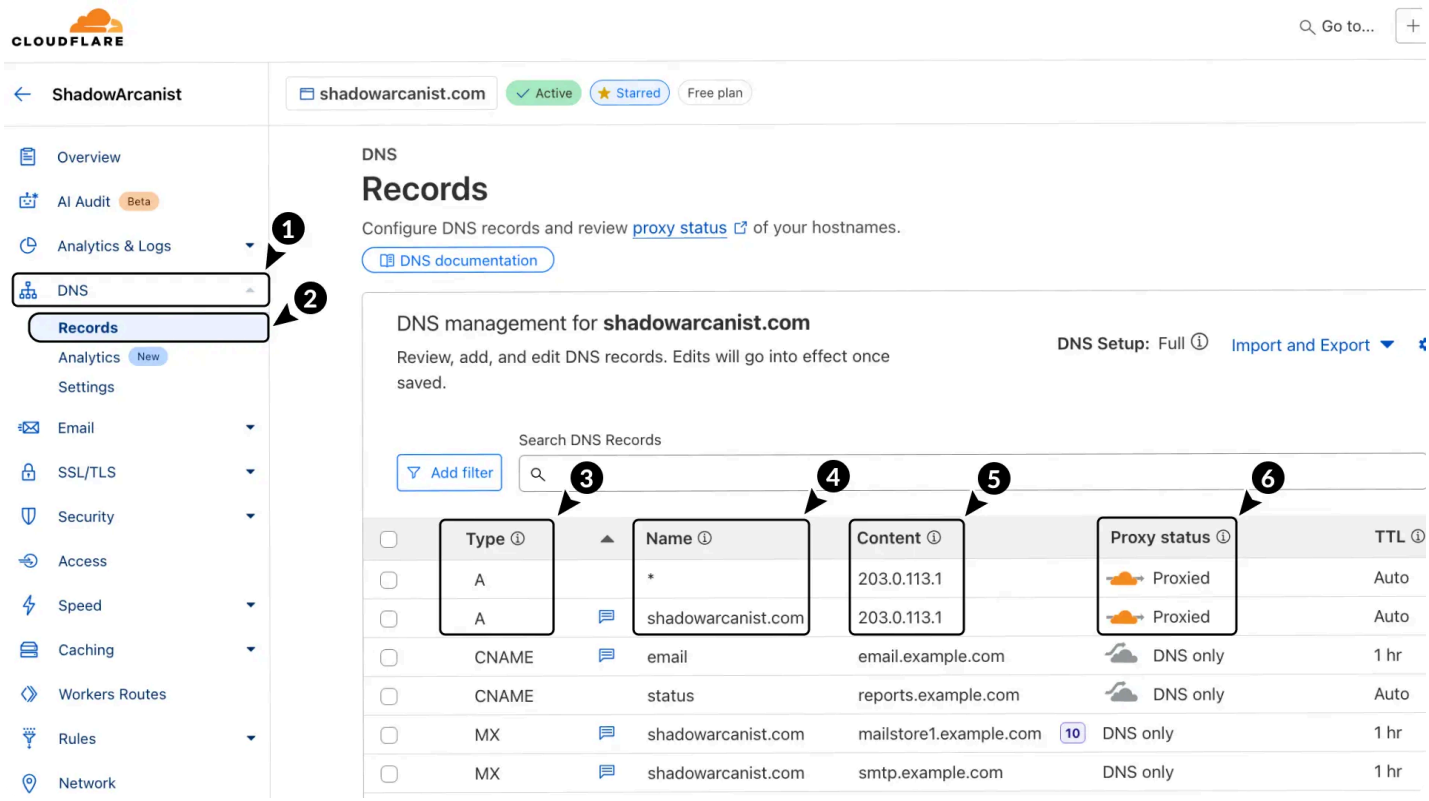
Save and exit.

Now the origin certificate is installed on your server.

> Commands Used on Server (click to view)

3. Set Up DNS Records and TLS Encryption

To make the origin certificate work, configure your DNS records, enable TLS, and set up HTTP to HTTPS redirects in Cloudflare:

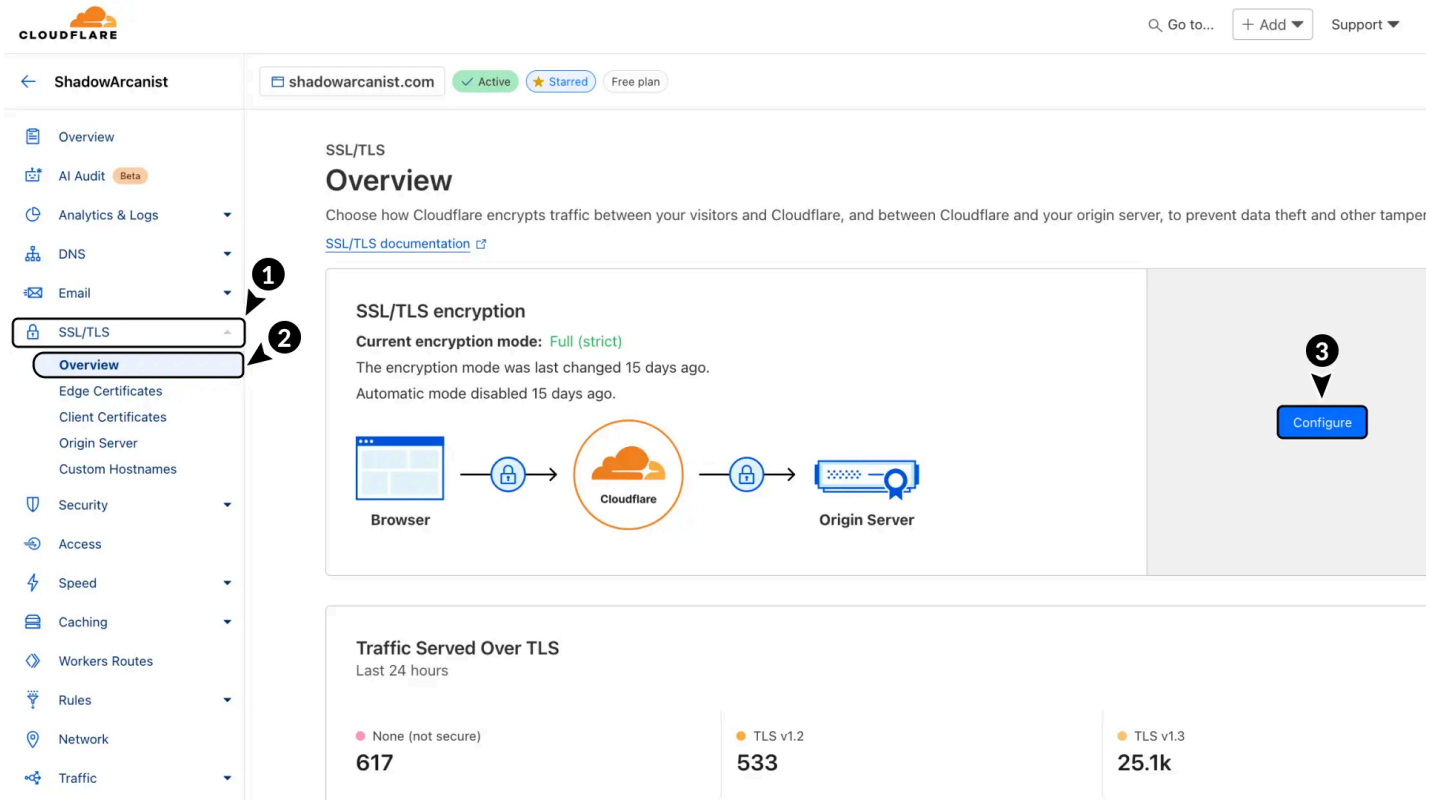


1. In Cloudflare, go to **DNS**.
2. Select **Records**.
3. Add 2 A records:

Envix

6. Set the proxy status to **Proxied** for better security.

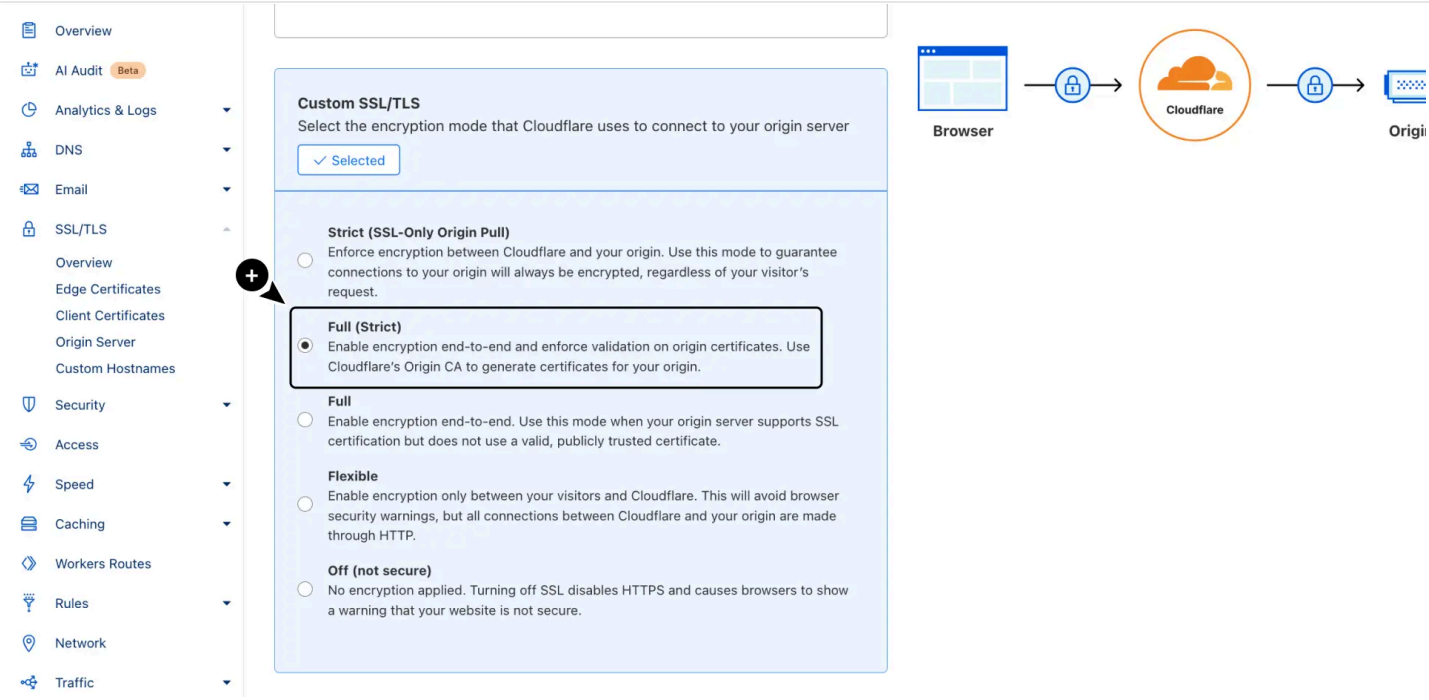
Next, set up TLS encryption:



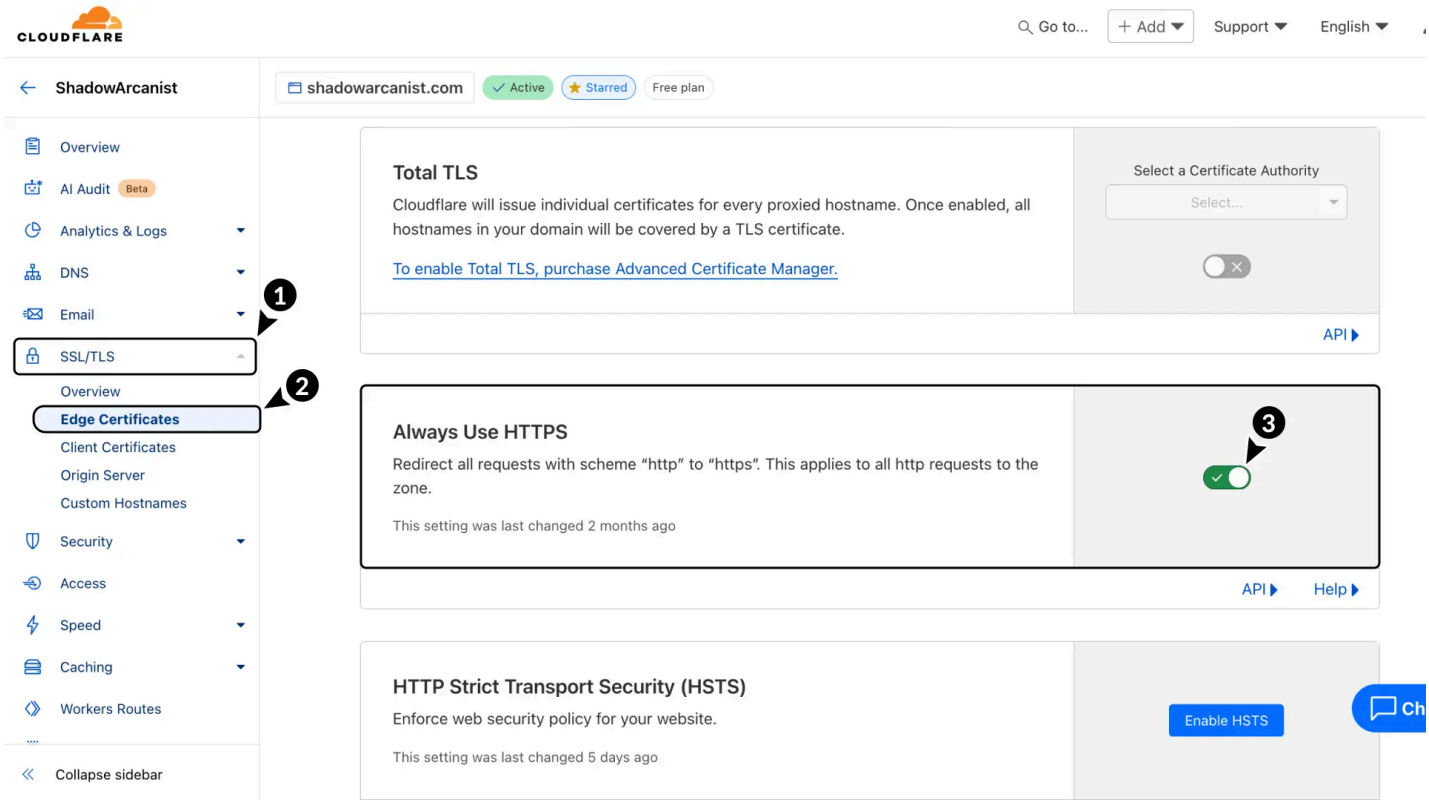
1. Go to **SSL/TLS** in Cloudflare.
2. Select **Overview**.
3. Click **Configure** button

Choose **Full (Strict)** as the encryption mode.

Envix



Finally, enable HTTP to HTTPS redirects:

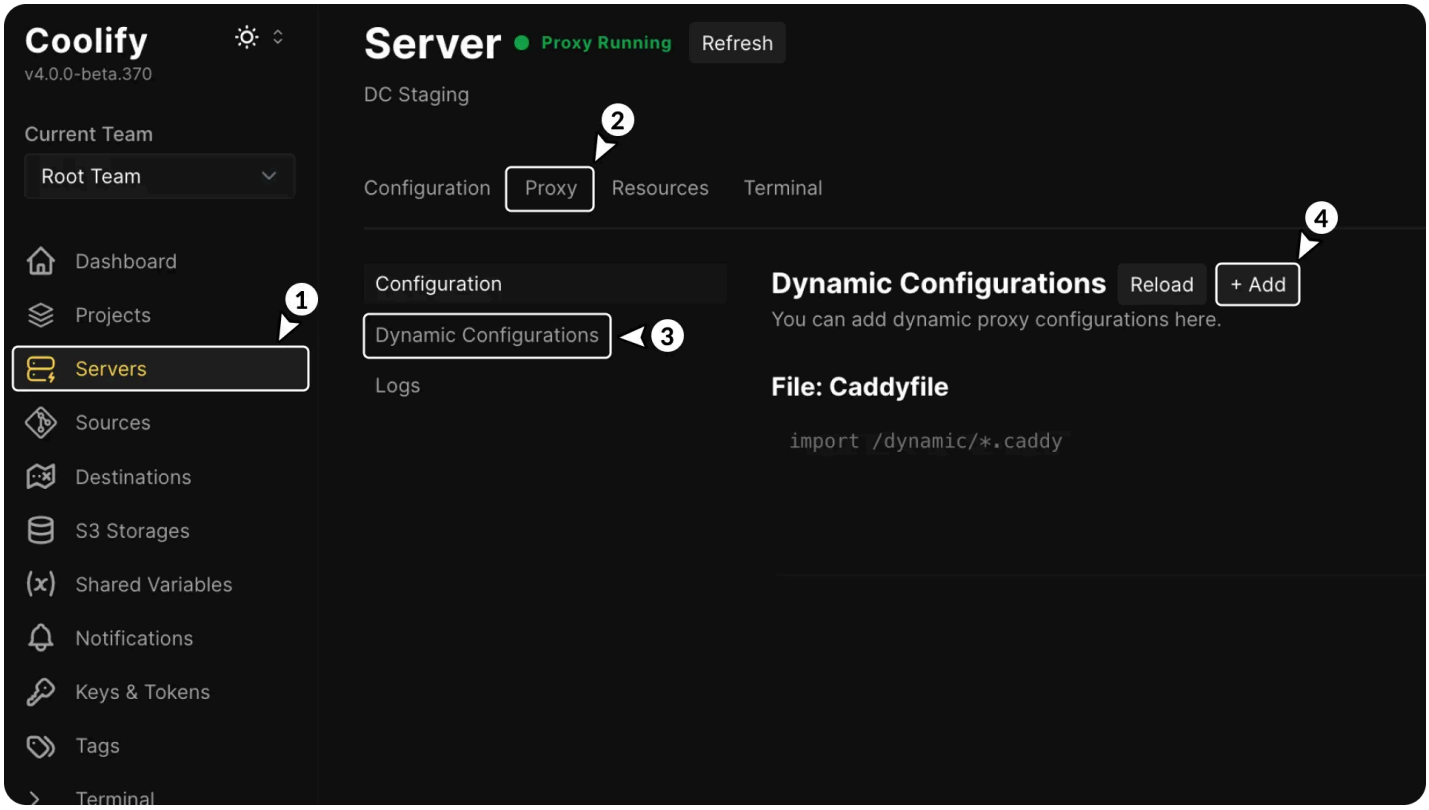


1. In Cloudflare, go to **SSL/TLS**
2. Select **Edge Certificates**.

Envix

4. Configure Coolify to Use the Origin Certificate

Now, in your Coolify dashboard:



1. Go to the **Server** section in the sidebar.
2. Select **Proxy**.
3. Open the **Dynamic Configuration** page
4. Click **Add** button

You will now be prompted to enter the Dynamic Configuration.

Envix

1. Choose a name for your configuration.
2. Enter the following details in the configuration field:

```
tls:
  certificates:
    -
      certFile: /traefik/certs/shadowarcanist.cert
      keyFile: /traefik/certs/shadowarcanist.key
```

> Adding Multiple Certificates (click to view))

3. Save the configuration

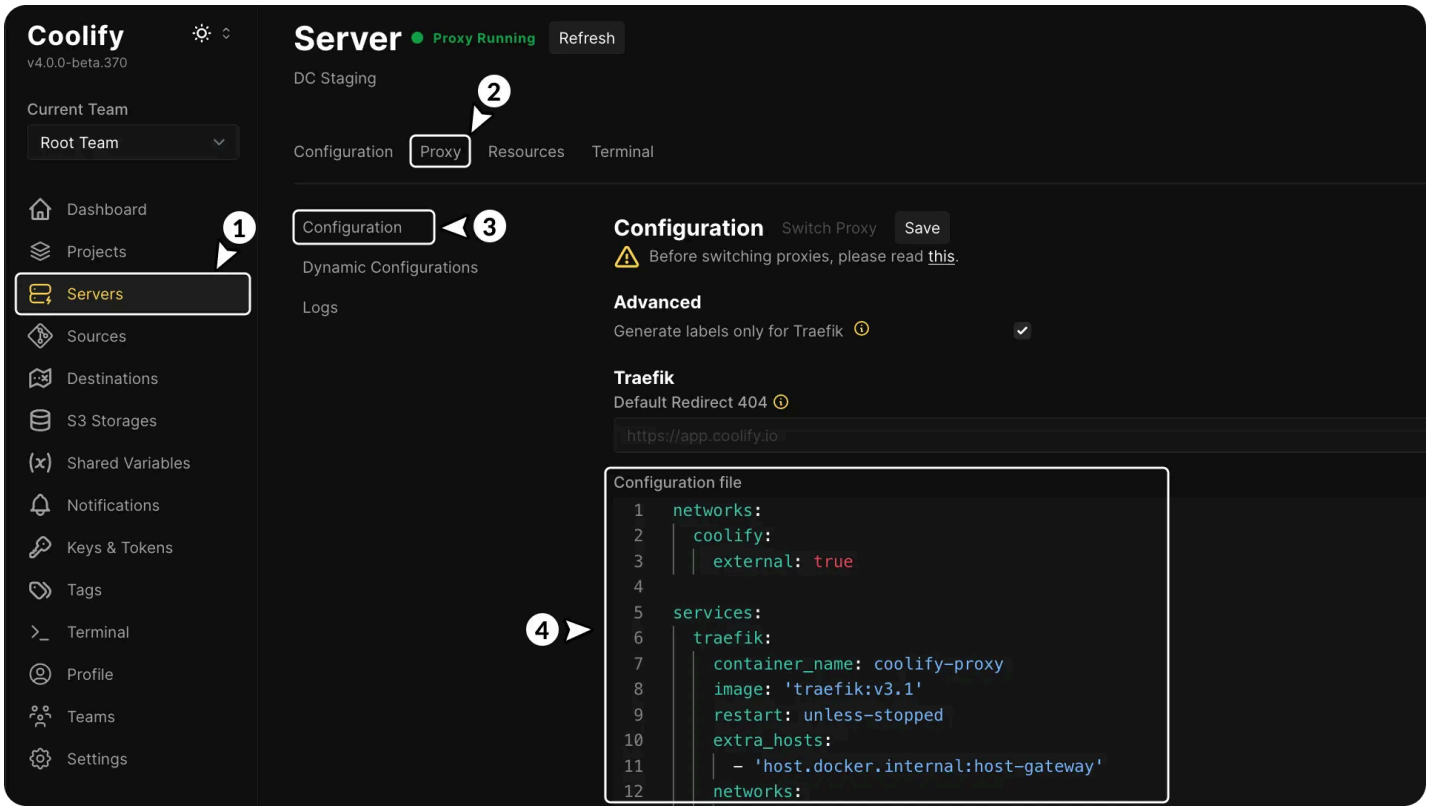
From now on, Coolify will use the origin certificate for requests matching the hostname.

> All the steps below are completely optional

5. Optional: Configure Traefik

Envix

Since you're using an Origin Certificate, you no longer need HTTP challenges or port 80 open.



1. Go **Server** in the Coolify dashboard.
2. Select **Proxy**.
3. Open **Configuration**.
4. Replace the configuration with this:

```
# Define external networks
networks:
  coolify:
    external: true  # External network.

services:
  # Traefik reverse proxy
  traefik:
    container_name: coolify-proxy  # Container name.
    image: 'traefik:v3.1'  # Traefik image version.
    restart: unless-stopped  # Auto-restart policy.
    extra_hosts:
      - 'host.docker.internal:host-gateway'  # Host communication.
    networks:
      - coolify  # Network connection.
```

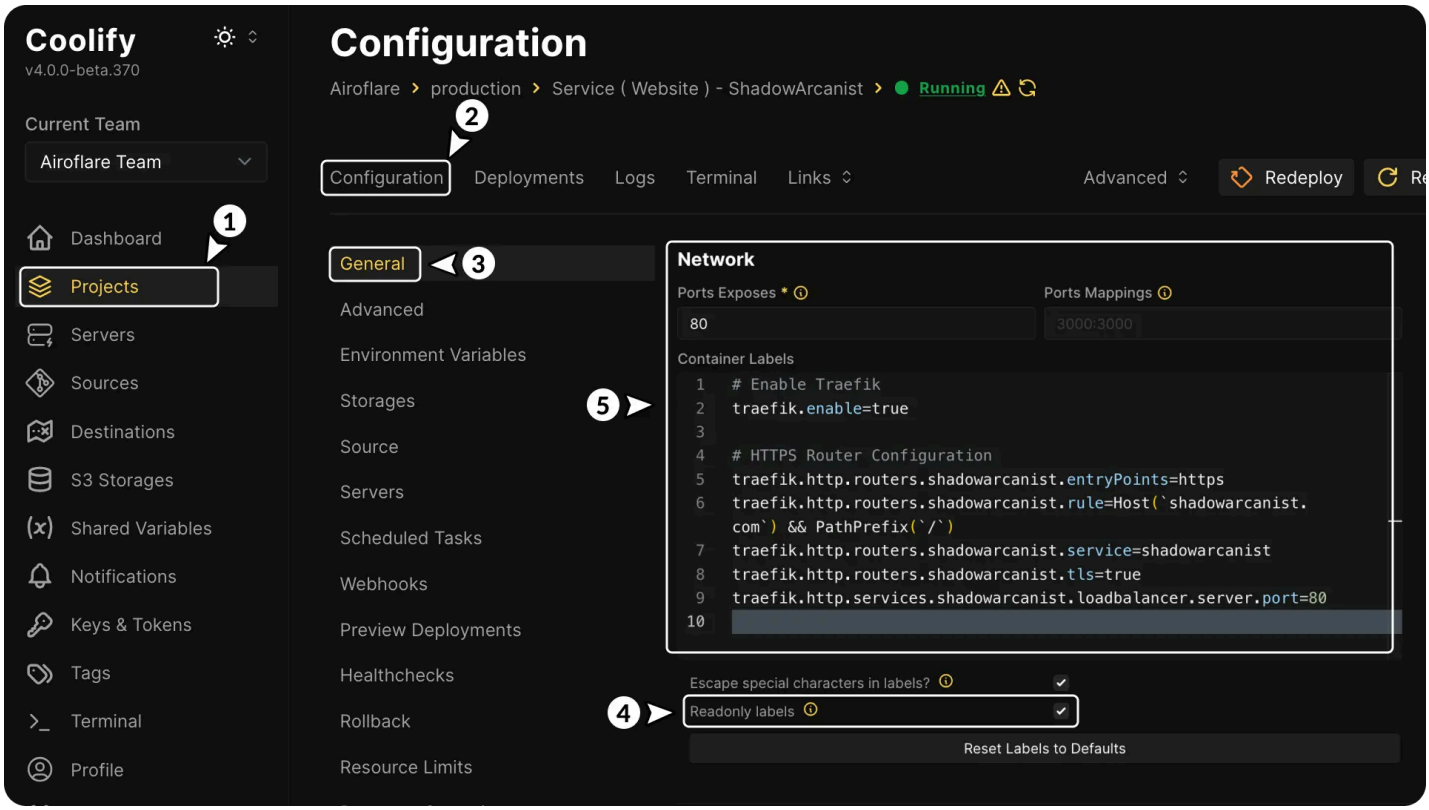
Envix

```
    test: 'wget -qO- http://localhost:80/ping || exit 1'  # Ping endpoint for health check.
    interval: 4s  # Health check interval.
    timeout: 2s  # Health check timeout.
    retries: 5  # Retry attempts.
  volumes:
    - '/var/run/docker.sock:/var/run/docker.sock:ro'  # Docker socket access.
    - '/data/coolify/proxy:/traefik'  # Traefik config volume.
  command:
    # Traefik configuration options
    - '--ping=true'  # Enable ping for health check.
    - '--ping.entrypoint=http'  # Use HTTP entrypoint for ping.
    - '--entrypoints.http.address=:80'  # HTTP entry point for health checks.
    - '--entrypoints.https.address=:443'  # HTTPS entry point.
```

Note

The comments in this configuration explain each line. You can remove the comments when copying it into your configuration.

Next, you'll need to remove a few labels from your Dockerfile-based deployments. Below is an example of how I set this up for my website.



1. Go to **Projects** and select your project.

Envix

4. Check **Readonly labels** option
5. Replace the labels with the following:

```
# Enable Traefik for this configuration
traefik.enable=true

# Define the entry point for the router (HTTPS)
traefik.http.routers.shadowarcanist.entryPoints=https

# Set the routing rule for this router to match the domain "shadowarcanist.com" and any path s
traefik.http.routers.shadowarcanist.rule=Host(`shadowarcanist.com`) && PathPrefix(`/`)

# Assign the service 'shadowarcanist' to this router
traefik.http.routers.shadowarcanist.service=shadowarcanist

# Enable TLS (HTTPS) for this router
traefik.http.routers.shadowarcanist.tls=true

# Specify the backend service and its port (port 80)
traefik.http.services.shadowarcanist.loadbalancer.server.port=80
```

Now you're done! Your server is set up to use the Cloudflare Origin Certificate, and all traffic is secured via TLS.

Note

If this guide doesn't resolve your issue, please join the Coolify Discord server and seek assistance there.

Links

Coolify Support Server

Author's Website

Envix

The header image is designed using icons from Flaticon. Links to each icon can be found below:

- Medal icon by Vlad Szirka
- Award icon by explanaicon
- Worldwide icon by Freepik
- Lock icon by Those Icons
- Browser icon by Alfredo Hernandez
- Database icon by Tanah Basah