

Cloudflare Tunnels Securing Them

how can i 'secure' the clips.ldmathes.cc

Great question! Here are your options to secure your ComfyUI tunnel:

Option 1: Cloudflare Access (Built-in, Recommended)

Add authentication directly in your Cloudflare Zero Trust dashboard:

Go to <https://one.dash.cloudflare.com/>

Access → Applications → Add an application

Choose Self-hosted

Settings:

Application domain: clips.ldmathes.cc

Policy: Create a rule like:

Emails ending in: @yourdomain.com (your email)

Or Emails: your@email.com (specific email)

Or use a One-time PIN sent to your email

Now anyone visiting clips.ldmathes.cc will hit a Cloudflare login page first.

Option 2: Basic Auth in the Tunnel Config

Edit your config.yml:

yaml

tunnel: <your-tunnel-id>

```
credentials-file: C:\Users\<YourUsername>\.cloudflared\<tunnel-id>.json
```

ingress:

```
- hostname: clips.ldmathes.cc  
  service: http://localhost:8188  
  
  originRequest:  
    noTLSVerify: true  
  
    # Add basic auth here - but this is less secure than Access  
  
- service: http_status:404
```

Actually, skip this - Option 1 is way better.

Option 3: ComfyUI's Built-in Auth

ComfyUI has some basic auth options, but they're not as robust.

My recommendation:

Use Cloudflare Access (Option 1) - it's free for up to 50 users, super easy to set up, and way more secure than basic auth. Takes 2 minutes.

Want me to walk you through setting up Cloudflare Access?

yes

Perfect! Here's the step-by-step:

Setting up Cloudflare Access for clips.ldmathes.cc

Step 1: Go to Zero Trust Dashboard

Navigate to: <https://one.dash.cloudflare.com/>

If prompted, select your account

You might need to set up a "team name" if this is your first time - just pick something like "ldmathes-team"

Step 2: Create an Application

In the left sidebar: Access → Applications

Click Add an application

Select Self-hosted

Step 3: Configure Application

Application Configuration:

Application name: ComfyUI (or whatever you want)

Session Duration: 24 hours (how long before re-login)

Application domain:

Subdomain: clips

Domain: ldmathes.cc

Click Next

Step 4: Create Access Policy

Add a policy:

Policy name: Allow My Email

Action: Allow

Configure rules:

Selector: Emails

Value: your@email.com (your actual email)

Click Next, then Add application

Step 5: Test It

Open a new incognito/private browser window

Go to <https://clips.ldmathes.cc>

You should see a Cloudflare Access login page

Enter your email → Check your email for code → Enter code

You're in!

Done! Now only you (or whoever you add to the policy) can access your ComfyUI.

Bonus: Add More Users Later

Go back to Access → Applications → Click your app → Policies → Edit to add more emails

Try it and let me know if you hit any snags!

create an access group rule --- so i can use it for some of my other tunnel apps?

Great idea! Access Groups are reusable and way cleaner than recreating rules for each app.

Create an Access Group

Step 1: Create the Group

Go to <https://one.dash.cloudflare.com/>

Access → Access Groups (in the left sidebar)

Click Add a Group

Step 2: Configure the Group

Group Configuration:

Group name: My Personal Access (or whatever you want)

Define group criteria: Choose one or more: Option A - Single Email:

Selector: Emails

Value: your@email.com

Option B - Multiple Emails:

Selector: Emails

Value: your@email.com

Click Add require and add more emails

Option C - Email Domain (if you have your own domain):

Selector: Emails ending in

Value: @yourdomain.com

Click Save

Step 3: Use the Group in Applications

Now when you create or edit applications:

Access → Applications → Your app → Policies

When creating a policy, instead of selecting "Emails":

Selector: Access groups

Value: Select My Personal Access (your group name)

Step 4: Apply to Existing Apps

For your ComfyUI app (clips.ldmathes.cc):

Access → Applications → Find ComfyUI

Click on it → Policies tab

Edit the existing policy

Change the rule from specific email to:

Include: Access groups → My Personal Access

Save

Now you can:

Add more emails to the group in one place

Reuse this group for all your tunnels

Manage access centrally

Pro tip: You can create multiple groups like:

"Family Access" - for family members

"Friends Access" - for trusted friends

"Admin Access" - just you

Want to set up your RDP tunnel with the same group next?

I have two policies, one 'resuable' policies and the other 'rule groups'

i defined an application

how do i connect them?

Ah, I see the confusion! Here's how they connect:

Connecting Access Groups to Applications

In Your Application:

Go to Access → Applications

Click on your application (e.g., ComfyUI)

Go to the Policies tab

Either edit existing policy or add new policy

In the Policy Configuration:

When you're editing/creating a policy, you'll see:

Configure rules:

Click Add include (or it might already have a rule)

In the Selector dropdown, choose: Access groups

In the Value dropdown, select your group from "Rule Groups"

Example:

Policy name: Allow My Access Group

Action: Allow

Include:

Selector: Access groups

Value: My Personal Access <-- Your group from "Rule Groups"

Reusable Policies vs Rule Groups:

Rule Groups: These are the groups you define (like "My Personal Access")

Reusable Policies: These are complete policies you can apply to multiple apps

You probably want to use Rule Groups (Access Groups) within your application policies.

So the flow is:

Create Access Group (Rule Groups) ✓ You did this

Create Application ✓ You did this

Edit Application Policy → Use Access Group in the Include rule ← Do this

Does that make sense? Which step are you stuck on?

I got it to work for `clips.ldmathes.cc` but not: <https://ldmathes.cc/movies-shows-editor/>

Ah! The issue is that <https://ldmathes.cc/movies-shows-editor/> is a path on your root domain, not a separate subdomain like `clips.ldmathes.cc`.

Cloudflare Access policies work on hostnames, not paths by default.

You have two options:

Option 1: Protect the Entire Root Domain

Create an Access application for the entire `ldmathes.cc` domain:

Access → Applications → Add an application

Self-hosted

Application domain:

Leave subdomain blank

Domain: `ldmathes.cc`

Use your Access Group in the policy

Downside: This protects ALL of `ldmathes.cc`, not just `/movies-shows-editor/`

Option 2: Use Path-based Rules (Better)

You can add path specifications:

Access → Applications → Add an application

Self-hosted

Application domain:

Leave subdomain blank

Domain: ldmathes.cc

Path: /movies-shows-editor (or /movies-shows-editor/* to include subpaths)

Use your Access Group in the policy

This way only that specific path requires authentication.

Option 3: Move to a Subdomain (Cleanest)

If you control the tunnel config, you could set it up as:

movies.ldmathes.cc instead of ldmathes.cc/movies-shows-editor/

This gives you the cleanest separation.

Which setup do you have? Is /movies-shows-editor/ served by the same tunnel as your root domain, or a different service?

Perfect! You've already set it up correctly with the Path option. I can see:

Domain: ldmathes.cc

Path: movies-shows-editor/

This looks right! Now you just need to:

Complete the Setup

Click on the "Policies" tab at the top (next to "Basic information")

Add or edit a policy to include your Access Group:

If there's already a policy, click Edit

If not, click Add a policy

Configure the policy:

Policy name: Allow My Access Group (or whatever)

Action: Allow

Include:

Selector: Access groups

Value: Select your group (the one you created earlier)

Save the policy

Save the application

Test It

Open an incognito window

Go to <https://ldmathes.cc/movies-shows-editor/>

You should see the Cloudflare Access login page

If it's not prompting for login, double-check:

The policy is set to Allow (not Block)

The Access Group is selected in the Include section

You saved everything

Does it show you the Policies tab? What do you see there?

i set the policy in the tab ... still free access from the wild

Hmm, if the policy is set but you still have free access, let's troubleshoot:

Quick Checks:

Did you click the final "Save" or "Add application" button?

Sometimes there's a save at the policy level AND at the application level

Look for a button at the bottom of the page

Check the application status:

Go back to Access → Applications

Does your "MoviesShows" application show up in the list?

Is there any warning icon or status indicator?

Verify the policy action:

Go to Access → Applications → MoviesShows → Policies tab

Make sure the policy Action is set to Allow (not Service Auth or something else)

Make sure there's no other policy that might be bypassing it

Clear browser cache or try a different browser:

Sometimes cached sessions bypass the auth

Try in a completely fresh incognito window

Check if there's a "Bypass" rule:

In the Policies tab, scroll down

Make sure there's no policy with Action = "Bypass" that's above your Allow policy

Nuclear Option - Delete and Recreate:

If nothing works:

Delete the application entirely

Create it fresh from scratch

Make sure you hit all the "Save" buttons

Can you screenshot what you see in the Policies tab? That will help me see what might be wrong.