Basic Coolify Security

Coolify runs as the **root user** by default. This means it has **full control** over your server. You can deploy many different applications with it, and that often means **opening ports** on your server to the internet.

If you're new to **self-hosting** or **Linux**, it can be hard to know how to **secure your server** or understand the **risks**. A small mistake like keeping port open that shouldn't be — can give hackers full access.

There are many things you can do to improve security, but in this guide, we will focus on the **basic steps**. These steps will already make your server **much safer** than most first-time self-hosters.

First, you need to have a security mindset. Just changing the way you think about security can make a big difference. Below are the key mindsets every self-hosting user should follow.

The Security Mindset

★ Zero Trust

Never trust anyone by default - not users, not apps, not even yourself. Always ask: "**Is this safe? Is this necessary?**"

★ Least Privilege

Only give the **minimum access or permissions** needed. If someone only needs to read files, don’t give them permission to write or delete.

exposed to internet, can be all it takes for an attack.

Keep It Secret

Never share details about your server, setup, or security tools with anyone. The more others know, the easier it is to attack you.

Disable What You Don’t Use

If you're not using something (like FTP, extra ports, or old apps), turn it off or remove it. Less things running = less ways to get hacked.

Backups Are Security Too

Always set up **automatic backups**. A single error, exploit, or failure can take everything down — backups are your safety net when things go wrong.

Don’t Blindly Trust AI

AI can be helpful, but it’s not always correct or safe. **Always double-check** any commands or advice before running them — especially if it involves your server or security.

Don’t Trust the UI Alone

Web dashboards like Coolify are useful, but don’t rely only on them. **Learn some basic command line tools** so you can check logs, ports, and users yourself.

Security is boring until it’s too Late

No one cares about firewall rules, updates, or SSH keys... until they wake up to a wiped server or a crypto miner eating their CPU. **Don’t wait for regret**. Secure it before something happens.

If You Don’t Understand It, Don’t Run It

Copy-pasting commands or scripts from forums or AI without understanding them is like eating pills without knowing what they are. **Read**. **Learn**. Then **run**. Or you might open a hole you didn’t even know was there.

Don’t Panic!

You’ll see lots of bots trying to brute-force SSH into your server. **It’s normal — don’t panic!**. If you panic, you might make dumb decisions that put your server at risk. Stay patient, stay calm, and

Now that you have the security mindset, it’s time to take action. Here are the essential steps to lock down your server and Coolify instance.

Securing Your Server

1. Use Your Hosting Provider's Firewall

Your server's first line of defense is a **firewall.**

Don't use UFW on your server because Docker bypasses it.

Docker modifies iptables directly, which can allow containers to expose ports even if UFW says they're blocked.

Instead, **use the firewall provided by your hosting company** (like DigitalOcean, Vultr, or Hetzner). It's simpler, safer, and controls traffic before it even reaches your server.

2. Lock Down Your Ports

Only open the ports you absolutely need.

For a basic Coolify setup, you only need to allow inbound traffic for:

- **Port 22 (SSH)**: Only from your IP address.
- **Port 80 (HTTP)**: From anywhere.
- **Port 443 (HTTPS)**: From anywhere.

Block everything else. The fewer open doors, the safer you are.

3. Use SSH Keys, Not Passwords

Passwords can be guessed or brute-forced. **SSH keys are nearly impossible to crack.**

Disable password authentication on your server immediately. It’s the single most important step to prevent unauthorized access.

★ How to Disable SSH Passwords

1. Log in to your server.

```
PasswordAuthentication no
PermitEmptyPasswords no
```

4. Save the file and restart the SSH service: `sudo systemctl restart sshd`.

Warning: Make sure your SSH key is working before you do this, or you will lock yourself out.

4. Stick with the Root User (For Now)

Coolify runs as the **root user** by default. While running as a non-root user is possible, it's an experimental feature that can cause many permission issues.

If you're a beginner, **stick with the default root setup**.

Just be aware that this makes securing your Coolify dashboard extremely important.

Securing Coolify

1. Your Dashboard have Root Access

The terminal inside the Coolify dashboard gives you **full root access** to your server.

Anyone who gets into your Coolify admin account owns your server.

Treat your Coolify password like your root password.

2. Enable Two-Factor Authentication (2FA)

2FA adds a critical layer of security.

Even if someone steals your password, they won't be able to log in without your phone (or 2FA application).

Enable it now. Go to `Settings` → `Advanced` and set it up.

Store your backup codes somewhere safe.

This is the correct and secure setting.

Double-check that `Settings` → `Advanced` → `Registration Allowed` is turned **off**.

Links

Join our community on Discord

Need help? Join our community for assistance.

Visit the Author's Website

Learn more about the person behind this guide.