Securing HestiaCP — The Key Hardening Steps, Step by Step 2026

HestiaCP · https://www.hyyat.com/en/knowledgebase/secure-hestiacp/

In short To secure HestiaCP: enable two-factor auth for the admin account, use a strong password, issue an SSL certificate for the panel, restrict port 8083 with the firewall, make sure fail2ban is running, and keep the panel and system updated.

Embedded media: https://www.hyyat.com/wp-content/uploads/2026/11/hyyat-cp-hest-sec-en.mp4?_=1

HestiaCP manages your entire server, so its security is a top priority — compromising it means compromising all your sites. In this guide from the Hyyat Host team we walk through the key practical steps to secure the panel after installation.

Hyyat Host virtual servers come with a firewall and basic security settings, plus Arabic support to help you harden step by step.

Explore Hyyat Host VPS plans ←

This guide follows on from the HestiaCP install guide; apply these steps right after installation.

1) Enable two-factor authentication (2FA)

HestiaCP supports two-step verification for the admin account. Enable it from the user settings with an app like Google Authenticator, so even if the password leaks, no one gets in without your phone's code.

1. **Open the user settings** Click the username at the top then `Edit`.

2. **Enable Two-Factor Authentication** Scan the QR code with an authenticator app, enter the code to confirm, then save.

2) Use a strong password and change it after install

Change the default admin password immediately to a long, unique one. You can do this from the user settings, or with the command:

```
v-change-user-password admin your-strong-password
```

3) Issue an SSL certificate for the panel itself

Make access on port 8083 encrypted with a trusted certificate instead of a self-signed one, so your password isn't sent in clear text. You can issue a Let's Encrypt certificate for the panel hostname from the server settings.

4) Restrict port 8083 with the firewall

HestiaCP includes a built-in firewall under the `Firewall` section. Allow access to the panel port **8083** from your own IP only where possible, and close unused ports.

1. **Open the firewall** From the top menu open the `Firewall` section.
2. **Restrict the panel port** Edit the rule for port 8083 to allow only your IP address if it is static.

5) Make sure fail2ban is running

fail2ban ships enabled by default in HestiaCP and bans IPs after repeated failed login attempts. Confirm it is on under `Firewall → Fail2Ban` — it is strong protection against brute-force attacks.

6) Keep the panel and system updated

Updates close security holes as they are found. Update system packages regularly, and update HestiaCP from the server settings or with the command:

```
apt update && apt upgrade -y
```

Quick security checklist

- Strong, unique admin password ✔
- Two-factor authentication enabled ✔
- SSL certificate for the panel issued ✔
- Port 8083 restricted by the firewall ✔
- fail2ban running ✔
- Panel and system updated ✔

Next step

- Enable 2FA and issue a certificate for the panel.
- Review your firewall and close unused ports.
- See the VPS control panel comparison to learn each panel's strengths.

And if you'd like us to secure your server and panel for you, open a support ticket — we reply within 24 hours at most.

Frequently asked questions

What is the most important step to secure HestiaCP?

Enabling two-factor authentication for the admin account and using a strong, unique password.

Is fail2ban enabled by default?

Yes, fail2ban ships enabled in HestiaCP and bans IPs after failed login attempts.

How do I restrict access to the panel?

From the Firewall section restrict port 8083 to your IP, and close unused ports.

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Web HostingSaudi Hosting