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

Plesk · https://www.hyyat.com/en/knowledgebase/secure-plesk/

In short To secure Plesk: enable two-factor auth, use a strong password, enable fail2ban and the firewall from the panel, restrict access to port 8443 to your IP, and enable automatic updates for the panel and components.

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

Plesk manages your entire server, so its security is a top priority. Plesk provides strong built-in security tools. In this guide from the Hyyat Host team we walk through the key hardening steps 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 Plesk install guide; apply these steps right after installation.

1) Enable two-factor authentication (2FA)

From your profile settings enable **Two-Factor Authentication** with an authenticator app, so even if the password leaks, no one gets in without your phone's code.

2) Use a strong password

Make the admin password long and unique, and change it immediately if default. Plesk shows a password strength indicator.

3) Enable fail2ban and the firewall

From `Tools & Settings → IP Address Banning (Fail2Ban)` enable protection against brute-force attacks, and from `Firewall` close unused ports.

4) Restrict access to the panel

Allow access to the panel port **8443** from your own IP only where possible, and you can restrict the admin area to a trusted IP list.

5) Enable automatic updates

From `Tools & Settings → Update and Upgrade Settings` enable automatic updates for the panel and components, and update the system regularly:

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

Quick security checklist

- Two-factor authentication enabled ✔
- Strong, unique password ✔
- fail2ban and firewall enabled ✔
- Port 8443 restricted ✔
- Automatic updates enabled ✔

Next step

- Enable 2FA and fail2ban.
- Review your firewall and restrict 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 Plesk?

Enabling two-factor authentication and using a strong password with fail2ban.

Does Plesk support fail2ban?

Yes, from Tools & Settings enable IP Address Banning (Fail2Ban) to block brute-force attacks.

How do I restrict access to the panel?

Allow port 8443 from your IP, and enable the firewall from the panel.

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

windows hosting