Security

SSL/TLS, IP blocking, hotlink protection, ModSecurity, 2FA, and SSH access in cPanel.

Contents

- SSL/TLS Management
- IP Blocker
- Hotlink Protection
- Leech Protection
- ModSecurity
- Two-Factor Authentication
- SSH Access

DANUMHOST

SSL/TLS Management

Manage SSL certificates, private keys, and TLS settings for your domains in cPanel.

The **SSL/TLS** section in cPanel centralizes certificate management, key storage, and HTTPS configuration for all domains on your account.

Key SSL/TLS tools

- **SSL/TLS Status** — view certificate status and run AutoSSL for all domains.
- **Manage SSL Sites** — install custom certificates or update existing ones.
- **Private Keys** — generate or upload private keys for certificates.
- **Certificate Signing Requests (CSR)** — generate CSRs for commercial SSL orders.

Install or renew a certificate

1. Go to **Security → SSL/TLS Status** and run AutoSSL for automatic free certificates.
2. For custom SSL, generate a CSR, order the certificate, then install it under **Manage SSL Sites**.
3. Enable HTTPS redirect on each domain after the certificate is active.

DanumHost servers support modern TLS versions. Keep certificates current to maintain browser trust and search ranking benefits.

DANUMHOST

IP Blocker

Block specific IP addresses or ranges from accessing your website through cPanel.

The **IP Blocker** tool denies HTTP access from specified IP addresses — useful when you identify malicious traffic, brute-force attempts, or unwanted visitors.

Block an IP address

1. Go to **Security → IP Blocker**.
2. Enter a single IP (for example `203.0.113.50`) or a range using CIDR notation (for example `203.0.113.0/24`).
3. Click **Add**.

Find IPs to block

Review **Metrics → Visitors** or raw access logs to identify repeat offenders. Look for excessive 404 requests, login attempts, or scanner patterns.

Remove a block

Return to IP Blocker, select the entry, and click Remove. Be careful not to block your own IP or shared CDN ranges used by legitimate services.

DANUMHOST

Hotlink Protection

Prevent other websites from embedding your images and wasting your bandwidth.

Hotlink protection stops external sites from linking directly to your images and files, which can consume your DanumHost bandwidth without benefiting your site.

Enable hotlink protection

1. Go to **Security → Hotlink Protection**.
2. Click **Enable**.
3. Add your own domains to the **URLs to allow access** list so your sites can still display images.
4. Specify a redirect URL or image to show when hotlinking is blocked (optional).
5. Click **Submit**.

Allowed URLs

Include all domains and subdomains that legitimately serve your content, for example `yourdomain.com` and `www.yourdomain.com`. Omitting your own domains can break images on your site.

When to use it

Enable hotlink protection if you notice high bandwidth usage from external referrers in Awstats or bandwidth reports.

DANUMHOST

Leech Protection

Limit how many times a password-protected area can be accessed within a set period.

Leech protection prevents users from sharing passwords to protected directories by limiting how many times an account can log in within a two-hour window.

Enable leech protection

1. Go to **Security → Leech Protection**.
2. Select the password-protected directory you want to protect.
3. Set the maximum number of logins allowed within two hours (for example 2).
4. Enter an email address to receive alerts when the limit is exceeded.
5. Choose whether to redirect violators to a URL or disable the compromised account.
6. Click **Enable**.

Prerequisites

The directory must already be password-protected using **Directory Privacy** (Directory Indexing/Privacy). Leech protection adds an extra layer on top of basic authentication.

When alerts fire

If a user exceeds the login limit, you receive an email and can disable their directory access until you investigate whether credentials were shared.

DANUMHOST

ModSecurity

Understand the web application firewall that helps protect your cPanel-hosted sites.

ModSecurity is a web application firewall (WAF) that filters HTTP traffic and blocks common attack patterns such as SQL injection and cross-site scripting.

ModSecurity on DanumHost

ModSecurity is typically enabled at the server level on DanumHost cPanel servers. It inspects requests before they reach your applications and may block suspicious activity automatically.

If legitimate requests are blocked

1. Note the error message and the URL or action that triggered the block.
2. Check whether a plugin, theme, or custom form submission matches known WAF rules.
3. Contact DanumHost support with the timestamp, URL, and error details if you believe a false positive occurred.

Reduce false positives

Keep WordPress, plugins, and themes updated. Avoid unusual characters in form fields. If a specific rule blocks valid traffic repeatedly, support can review server-side rule exceptions where appropriate.

DANUMHOST

Two-Factor Authentication

Add an extra layer of security to your cPanel login with two-factor authentication.

Two-factor authentication (2FA) requires a second verification step beyond your password when logging in to cPanel — significantly reducing the risk of unauthorized access.

Enable 2FA

1. Go to **Security → Two-Factor Authentication**.
2. Click **Set Up Two-Factor Authentication**.
3. Scan the QR code with an authenticator app such as Google Authenticator, Authy, or 1Password.
4. Enter the six-digit code from your app to confirm setup.
5. Save your backup or recovery codes in a secure location.

Log in with 2FA

After entering your cPanel username and password, open your authenticator app and enter the current time-based code when prompted.

Best practices

- Do not share authenticator devices or backup codes.
- Reconfigure 2FA if you replace your phone.
- Combine 2FA with a strong, unique cPanel password.

DANUMHOST

SSH Access

Generate SSH keys and connect securely to your DanumHost server from the command line.

SSH (Secure Shell) lets you manage files, run commands, and troubleshoot your hosting account from a terminal — available on DanumHost plans that include shell access.

Generate an SSH key in cPanel

1. Go to **Security → SSH Access** or **SSH/Shell Access**.
2. Click **Manage SSH Keys → Generate a New Key**.
3. Enter a key name, choose a key type (RSA or ED25519), and set a passphrase for extra security.
4. Click **Generate**, then **Authorize** the public key for your account.

Connect from your computer

1. Download the private key or copy it to `~/.ssh/` on your machine.
2. Set permissions: `chmod 600 id_rsa` (Linux/macOS).
3. Connect using `ssh username@your-server-hostname` with the port shown in cPanel (often 22).

If SSH is disabled on your plan, contact DanumHost support to confirm whether shell access can be enabled.

Downloaded from https://danumhost.co.uk/knowledgebase/category/cpanel-security on 30-OCT-2026 9:47AM

DANUMHOST