Protect Configuration Files

What This Does

This protection restricts access to sensitive configuration files within your site.

It prevents these files from being accessed directly via the web.

Why It Matters

Configuration files may contain sensitive information such as:

- database credentials
- API keys
- environment settings
- internal configuration details

If exposed, these files can allow attackers to:

- access your database
- compromise your site
- escalate access to your server

When to Apply It

This protection is recommended for all WordPress sites.

Apply it when:

- configuration files exist within your web-accessible directories
- you want to prevent direct access to sensitive data
- your server does not already restrict access

When Not to Apply It

In most cases, this protection should always be applied.

Only avoid applying if:

- your hosting environment already enforces strict access controls
- custom configurations require public access (rare and discouraged)

How Steel Security Applies This

Steel Security protects configuration files using server-level rules.

Depending on your environment, this may include:

- Apache `.htaccess` restrictions
- Nginx configuration guidance
- IIS web.config rules

These rules block direct web access to known sensitive file types.

What to Expect After Applying

After applying this protection:

- configuration files will not be accessible via browser
- attempts to access them will return an error (e.g., 403 Forbidden)
- your site functionality will remain unchanged

How to Verify

To verify the protection:

1. Attempt to access a known configuration file via your browser
2. Confirm that access is denied

You should not be able to view file contents.

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
2. Disable the control
3. Confirm the change
4. Re-test file access

Access will return to its previous behavior.

Common Issues

File Access Is Blocked

This is expected.

The protection is preventing exposure of sensitive data.

Legitimate Access Is Affected

If a system requires access:

- review how the file is being accessed
- consider alternative secure methods
- revert only if absolutely necessary

Protection Does Not Work

- verify server configuration supports the rules
- check for conflicting server directives
- ensure file paths match expected patterns

Related

- Protect Backup Files
- Disable Directory Listing
- Safe Rollback Practices

Revision #1
Created 2026-04-04 18:49:18 UTC by Jason Wassing
Updated 2026-04-04 18:49:19 UTC by Jason Wassing