Configuration

Configuration

- Configuration and Defaults

Configuration and Defaults

What This Covers

This page explains how Steel Security handles configuration and why it does not include traditional plugin settings.

Steel Security is designed to minimize configuration and provide safe, effective defaults out of the box.

No Settings by Design

Steel Security does not include a traditional settings panel.

This is intentional.

The plugin is designed to:

- reduce complexity
- avoid misconfiguration
- provide consistent, reliable behavior

Most functionality is controlled through actions, not settings.

How Steel Security Is Configured

Instead of settings, Steel Security operates through:

- scan results
- hardening controls
- quarantine actions

This means:

- you act based on findings
- you apply protections intentionally
- you make decisions with context

Why There Are No Settings

Traditional settings often:

- introduce unnecessary complexity
- allow unsafe configurations
- create inconsistent behavior across environments

Steel Security avoids this by using:

- sensible defaults
- controlled actions
- environment-aware behavior

What You Can Control

While there are no global settings, you still have full control over:

- which hardening controls are applied
- which files are quarantined or restored
- how findings are handled

This keeps control focused on **decisions that matter**.

Benefits of This Approach

- fewer configuration mistakes
- faster onboarding
- consistent behavior across sites
- reduced need for ongoing management

This approach is especially beneficial for:

- agencies managing multiple sites
- developers working across environments
- users who prefer simplicity

When Configuration May Still Be Needed

Some actions may still involve environment-specific decisions, such as:

- server-level configurations
- file permissions
- hosting restrictions

These are handled outside of Steel Security where appropriate.

Common Questions

Why can’t I customize scan behavior?

Steel Security focuses on high-signal checks that are relevant across most environments.

Reducing configurability helps ensure consistent and meaningful results.

Will settings be added in the future?

Steel Security prioritizes clarity and safety over configurability.

New options will only be introduced where they provide clear value without increasing complexity.

How do I change how Steel Security behaves?

Behavior is controlled through:

- applying or reverting hardening
- managing quarantined files
- responding to scan findings

Tips

- Trust the default behavior
- Focus on findings and actions rather than configuration
- Avoid overcomplicating your security workflow

What to Do Next

Now that you understand how Steel Security is configured:

1. Run a scan
2. Review findings
3. Apply hardening as needed

Related

- Working with Scan Findings
- Applying Hardening Safely
- Safe Rollback Practices