Troubleshooting

Solve common issues and get your site back to normal quickly.

General Issues

General Issues

Scan Not Running

What This Means

This issue occurs when the Steel Security scan does not run or does not produce results when expected.

Common Symptoms

- the scan page loads but no results appear
- the scan does not start automatically
- findings are not updated
- the scan appears to hang or stall

Possible Causes

This issue may be caused by:

- JavaScript errors in the browser
- server timeouts or resource limits
- plugin conflicts
- incomplete installation or configuration

How to Fix It

Try the following steps:

1. Refresh the Page

- reload the scan page
- ensure the scan is triggered properly

2. Check Browser Console

- open developer tools
- look for JavaScript errors
- resolve any visible issues

3. Disable Other Plugins

- temporarily disable other plugins
- check if the scan runs correctly
- re-enable plugins one at a time

4. Check Server Limits

- ensure your server has sufficient resources
- review timeout settings
- check PHP error logs

5. Verify Installation

- confirm Steel Security is installed and activated correctly
- ensure all required components are present

What to Expect After Fixing

After resolving the issue:

- the scan should run automatically when the page loads
- findings should be generated and displayed
- results should reflect the current state of your site

When to Seek Help

If the issue persists:

- gather error messages or logs
- note recent changes to your site
- contact support with details

Related

- Understanding Scan Findings
- Reviewing Findings

General Issues

Changes Not Applying

What This Means

This issue occurs when changes made through Steel Security do not appear to take effect on your site.

You may apply a hardening control, but the expected behavior does not change.

Common Symptoms

- protections appear enabled but have no effect
- restricted files or endpoints remain accessible
- headers do not appear after being applied
- previously visible behavior remains unchanged

Possible Causes

This issue is often caused by:

- caching (browser, server, or CDN)
- delayed server configuration updates
- conflicting rules or settings
- unsupported server environment

How to Fix It

Try the following steps:

---

1. Clear All Caches

- clear your browser cache
- clear any WordPress caching plugins
- purge CDN caches (if applicable)

---

2. Reload the Page Fully

- perform a hard refresh (e.g., Ctrl+F5 or Cmd+Shift+R)
- test in a private/incognito window

---

3. Check Server Environment

- confirm your server supports the applied control
- ensure configuration changes are allowed
- verify `.htaccess` or server rules are being read

---

4. Review Conflicting Configurations

- check for overlapping rules from other plugins
- review manual server configurations
- ensure no settings override Steel Security changes

---

5. Allow Time for Changes

- some environments may delay configuration updates
- wait briefly and test again

What to Expect After Fixing

After resolving the issue:

- applied protections should take effect immediately
- restricted access should behave as expected
- headers or rules should appear correctly

When to Seek Help

If the issue persists:

- document the specific control applied
- note your server type (Apache, Nginx, IIS)
- check logs or error messages
- contact support with details

Related

- Apache (.htaccess) Hardening
- Nginx Hardening
- IIS (web.config) Hardening

General Issues

Unexpected Site Behavior

What This Means

This issue occurs when your site behaves unexpectedly after applying one or more hardening controls.

This may include broken functionality, missing features, or access issues.

Common Symptoms

- parts of the site stop working
- login or admin access is affected
- integrations fail or behave differently
- pages do not load as expected

Why This Happens

Hardening controls restrict access or behavior to improve security.

In some cases, these restrictions may:

- conflict with plugins or themes
- block required functionality
- interfere with integrations or custom code

This is more likely in complex or customized environments.

How to Fix It

Try the following steps:

---

1. Identify the Change

- determine which hardening control was applied most recently
- consider any recent configuration changes

---

2. Revert the Change

- disable the most recent control
- confirm whether normal behavior returns

---

3. Test Incrementally

- reapply controls one at a time
- test your site after each change
- identify the specific control causing the issue

---

4. Review Requirements

- check if your site relies on the affected functionality
- confirm whether restrictions are appropriate for your use case

---

5. Adjust or Exclude

- modify the configuration if possible
- allow required access where needed
- leave the control disabled if necessary

What to Expect After Fixing

After resolving the issue:

- normal site functionality should be restored
- problematic controls can be adjusted or excluded
- other protections can remain in place

When to Seek Help

If you are unable to resolve the issue:

- document the affected functionality
- note which control caused the issue
- include any error messages or logs
- contact support with details

Key Principle

Security should not come at the cost of breaking your site.

Apply protections in a way that balances security and functionality.

Related

- Safe Rollback Practices
- Applying Hardening Safely
- Restrict Sensitive Endpoints

Access & Lockouts

Access & Lockouts

Access & Lockouts

Unable to Access Admin

What This Means

This issue occurs when you are unable to access the WordPress admin area after applying one or more hardening controls.

Common Symptoms

- unable to log in via `/wp-login.php`
- admin page returns an error (e.g., 403 Forbidden)
- login page does not load
- access is blocked unexpectedly

Why This Happens

Some hardening controls restrict access to sensitive endpoints, including login functionality.

This may occur if:

- access is limited by IP or conditions
- endpoint restrictions are too strict
- server rules block legitimate requests

How to Fix It

Try the following steps:

---

1. Use an Alternate Access Method

- try accessing the site from a different network or device

- disable VPN or proxy services if in use

---

2. Revert the Most Recent Change

If you recently applied a hardening control:

- disable the last applied control
- confirm whether access is restored

---

3. Access via Hosting Panel

If you cannot log in:

- access your site files through cPanel, FTP, or file manager
- locate the Steel Security plugin configuration or rules
- temporarily disable the relevant restriction

---

4. Disable the Plugin (Temporary)

As a last resort:

- rename the Steel Security plugin directory
- this will deactivate the plugin
- restore access to your admin area

You can then re-enable and adjust settings safely.

What to Expect After Fixing

After resolving the issue:

- admin access should be restored
- login functionality should behave normally
- you can reapply protections more carefully

How to Prevent This

- apply hardening controls incrementally
- test access after each change
- ensure your access method is allowed before restricting endpoints

---

When to Seek Help

If you are unable to regain access:

- note recent changes
- gather any error messages
- contact support with details

Key Principle

Always ensure you have a reliable way to access your site before applying restrictive controls.

Related

- Restrict Sensitive Endpoints
- Unexpected Site Behavior
- Safe Rollback Practices

Blocked by Hardening Rules

What This Means

This issue occurs when legitimate requests are being blocked by one or more hardening controls.

This may affect access to certain pages, features, or functionality.

Common Symptoms

- receiving a 403 Forbidden error
- specific pages or endpoints not loading
- features or integrations failing
- inconsistent access depending on location or device

Why This Happens

Hardening controls restrict access to improve security.

In some cases, these restrictions may:

- block legitimate requests
- conflict with plugins or themes
- interfere with integrations or APIs

This is more likely in environments with custom configurations or external services.

How to Fix It

Try the following steps:

---

1. Identify the Blocked Resource

- determine which page, endpoint, or feature is affected
- note any error messages or response codes

---

2. Review Recent Changes

- identify recently applied hardening controls
- consider which control may be responsible

---

3. Adjust the Control

- modify the configuration if possible
- allow necessary access for specific functionality
- reduce overly strict restrictions

---

4. Test Incrementally

- reapply controls one at a time
- test after each change
- confirm which control is causing the issue

---

5. Revert if Necessary

- disable the problematic control
- restore functionality
- re-evaluate whether the protection is required

What to Expect After Fixing

After resolving the issue:

- affected pages or features should function normally
- appropriate protections can remain in place
- unnecessary restrictions can be removed or adjusted

How to Prevent This

- apply hardening controls gradually
- test functionality after each change
- understand how controls affect your environment

When to Seek Help

If the issue persists:

- document the affected functionality
- note which control is involved
- include any error messages
- contact support with details

Key Principle

Security controls should protect your site without interfering with legitimate use.

Related

- Unexpected Site Behavior
- Restrict Sensitive Endpoints
- Safe Rollback Practices

Server & Environment

Server & Environment

Server & Environment

Server Rules Not Working

What This Means

This issue occurs when server-level protections applied by Steel Security do not take effect.

You may enable a hardening control, but the expected behavior does not occur.

Common Symptoms

- restricted files or endpoints remain accessible
- directory listing is still enabled
- PHP execution is not blocked
- changes appear to have no effect

Why This Happens

Server-level rules depend on your hosting environment and configuration.

This issue may occur if:

- your server does not support the required rule type
- configuration overrides are disabled
- rules are not being read or applied
- another configuration is overriding the rules

How to Fix It

Try the following steps:

---

1. Confirm Your Server Type

- identify whether you are using Apache, Nginx, or IIS
- ensure the control you applied is supported in your environment

---

2. Check Apache Configuration (.htaccess)

If using Apache:

- ensure `.htaccess` overrides are enabled (`AllowOverride`)
- confirm the file exists and is readable
- verify no conflicting rules are present

---

3. Check Nginx Configuration

If using Nginx:

- note that `.htaccess` is not supported
- apply rules manually in your Nginx configuration
- reload or restart the server after changes

---

4. Check IIS Configuration (web.config)

If using IIS:

- confirm the `web.config` file is present
- ensure rules are applied correctly
- check for higher-level overrides

---

5. Review Hosting Restrictions

- some hosting providers restrict server-level configuration
- verify whether your hosting plan allows these changes
- consult your hosting provider if needed

What to Expect After Fixing

After resolving the issue:

- server rules should take effect immediately
- restricted behavior should function as expected
- hardening controls will apply correctly

How to Verify

- test access to restricted files or endpoints
- confirm expected responses (e.g., 403 Forbidden)
- re-check behavior after applying fixes

When to Seek Help

If the issue persists:

- note your server type and hosting environment
- document the specific control applied
- include any relevant error messages
- contact support with details

Key Principle

Server-level protections depend on your environment.

Understanding your server configuration is essential for effective hardening.

Related

- Apache (.htaccess) Hardening
- Nginx Hardening
- IIS (web.config) Hardening

Server & Environment

Nginx Configuration Issues

What This Means

This issue occurs when expected protections are not applied on a server running Nginx.

Unlike Apache, Nginx does not support dynamic configuration through `.htaccess`.

Common Symptoms

- hardening controls appear enabled but have no effect
- restricted files or endpoints remain accessible
- security headers do not appear
- no visible change after applying protections

Why This Happens

Nginx uses centralized configuration files instead of per-directory rules.

This means:

- Steel Security cannot modify server behavior automatically
- changes must be applied manually in the server configuration
- rules will not take effect without proper configuration updates

---

How to Fix It

Try the following steps:

---

1. Confirm You Are Using Nginx

- check your hosting environment
- review server response headers
- consult your hosting provider if unsure

---

2. Apply Rules Manually

- locate your Nginx configuration files
- apply the required rules based on Steel Security recommendations
- ensure the configuration reflects the desired protections

---

3. Reload or Restart Nginx

- reload the configuration after making changes
- ensure updates are applied to the running server

---

4. Verify Configuration Scope

- confirm changes are applied to the correct server block
- ensure no other configuration overrides your rules

---

5. Check Hosting Limitations

- some hosting providers restrict access to Nginx configuration
- use available control panel tools if provided
- contact your hosting provider if necessary

What to Expect After Fixing

After resolving the issue:

- server-level protections should take effect
- restricted behavior should function as expected
- hardening controls will align with your configuration

How to Verify

- test access to restricted files or endpoints
- confirm expected responses (e.g., 403 Forbidden)
- inspect headers in browser developer tools

When to Seek Help

If the issue persists:

- document your server environment
- note which controls are not applying
- include configuration details if possible
- contact support or your hosting provider

Key Principle

Nginx requires manual configuration for server-level protections.

Steel Security provides guidance, but implementation depends on your environment.

Related

- Nginx Hardening
- Server Rules Not Working
- Changes Not Applying

Headers & Browser Issues

Headers & Browser Issues

Headers Not Appearing

What This Means

This issue occurs when security headers expected from Steel Security are not visible in your site's responses.

You may have enabled header-related protections, but do not see them in browser tools.

Common Symptoms

- expected headers are missing in the Network tab
- no visible change after enabling header controls
- inconsistent header behavior across requests

Why This Happens

This issue is commonly caused by:

- caching (browser, server, or CDN)
- server configuration not applying changes
- headers being overridden or removed
- testing the wrong request type

How to Fix It

Try the following steps:

---

1. Clear All Caches

- clear your browser cache

- clear any WordPress caching plugins
- purge CDN caches (if applicable)

---

2. Perform a Hard Refresh

- reload the page using a hard refresh (e.g., Ctrl+F5 or Cmd+Shift+R)
- test in a private/incognito window

---

3. Verify the Correct Request

- inspect the main document request (not assets like images or scripts)
- ensure you are checking the correct URL

---

4. Check Server Configuration

- confirm your server supports header rules
- ensure configuration changes are applied
- verify no conflicting rules exist

---

5. Check for Overrides

- other plugins or server settings may override headers
- review any manual header configurations
- ensure Steel Security settings are not being overridden

What to Expect After Fixing

After resolving the issue:

- security headers should appear in responses
- browser developer tools should reflect the correct values
- protections will be enforced as expected

How to Verify

1. open browser developer tools
2. navigate to the Network tab
3. select the main page request
4. review the Response Headers section

Confirm that expected headers are present.

When to Seek Help

If the issue persists:

- note which headers are missing
- document your server type
- include details about caching or CDN usage
- contact support with this information

Key Principle

Header visibility depends on correct configuration, caching behavior, and proper verification.

Related

- Missing Security Headers
- Weak Header Configuration
- Changes Not Applying

Headers & Browser Issues

CSP Breaking Site

What This Means

This issue occurs when a Content Security Policy (CSP) blocks resources required for your site to function properly.

This may result in broken layouts, missing scripts, or non-functional features.

Common Symptoms

- scripts not loading or executing
- styles not applying correctly
- images or fonts missing
- features or integrations not working
- errors appearing in the browser console

Why This Happens

CSP restricts which sources of content are allowed to load.

If the policy is too strict or incomplete:

- required resources may be blocked
- external services may not load
- inline scripts or styles may be prevented

How to Fix It

Try the following steps:

---

1. Check Browser Console

- open developer tools
- look for CSP-related errors or warnings
- identify which resources are being blocked

---

2. Identify Required Sources

- determine which domains or resources are needed
- review any third-party services (analytics, CDNs, integrations)

---

3. Adjust the Policy

- update the CSP to allow required sources
- avoid overly restrictive rules
- apply changes incrementally

---

4. Test After Each Change

- reload your site after updating the policy
- verify that functionality is restored
- continue refining as needed

---

5. Revert if Necessary

If issues persist:

- remove or disable the CSP configuration
- restore normal site behavior
- reapply a simpler policy if needed

What to Expect After Fixing

After resolving the issue:

- blocked resources should load correctly

- site functionality should be restored
- CSP can be refined gradually over time

How to Verify

- reload your site and test all functionality
- confirm that no critical resources are blocked
- review console messages for remaining issues

When to Seek Help

If the issue persists:

- document the blocked resources
- include console error messages
- provide details about your CSP configuration
- contact support with this information

Key Principle

CSP should be applied carefully and refined over time.

Start simple, test thoroughly, and expand only as needed.

Related

- Content Security Policy (CSP)
- Headers Not Appearing
- Unexpected Site Behavior