

Understanding the Dashboard

What This Covers

This guide explains the Steel Security dashboard and how to interpret the information it provides.

The dashboard gives you a high-level view of your site's security posture and helps you prioritize next steps.

What the Dashboard Shows

The dashboard provides a summary of your site's current security state.

It is designed to answer three key questions:

- What risks exist on this site?
 - How severe are those risks?
 - What should I do next?
-

Key Sections

Scan Summary

The Scan Summary reflects the results of your most recent scan.

It includes:

- total findings detected
- breakdown by severity (if applicable)
- overall **Scan Risk Score**

This gives you a quick understanding of your current risk level.

Scan Risk Score

The Scan Risk Score represents the overall risk level of your site based on detected findings.

- Higher scores indicate greater risk
- Lower scores indicate a more secure configuration

The score is intended as a **guideline**, not a perfect measurement.

Focus on the underlying findings rather than the number alone.

Recent Findings

This section highlights the most relevant issues detected during the last scan.

Each finding includes:

- a description of the issue
- why it matters
- recommended next steps

Use this section to quickly identify what needs attention.

Hardening Overview

The dashboard also summarizes available hardening opportunities.

This may include:

- protections that can be applied
- current hardening status
- areas where improvements can be made

Hardening actions are optional and should be applied thoughtfully.

How to Use the Dashboard

A typical workflow:

1. Review your Scan Risk Score

2. Identify high-risk findings
3. Open the Scan page for detailed results
4. Apply hardening where appropriate
5. Re-scan to confirm improvements

The dashboard helps you decide where to focus, not perform the work itself.

What the Dashboard Does Not Do

The dashboard does not:

- run scans automatically
- make changes to your site
- apply hardening actions

It is a **summary and navigation layer**, not an action layer.

When to Check the Dashboard

Use the dashboard:

- after running a scan
 - after applying hardening
 - after updates, migrations, or restores
 - as part of routine maintenance
-

Common Questions

Why does the dashboard not update automatically?

The dashboard reflects the most recent scan results.

To refresh the data, return to the **Scan** page to trigger a new scan.

What should I focus on first?

Start with:

- high-risk findings
- exposed files
- configuration issues

These typically represent the most immediate concerns.

Is a low score “secure”?

A low score indicates fewer detected risks, but no system is ever completely risk-free.

Use the score as a guide, not a guarantee.

Tips

- Use the dashboard to prioritize, not diagnose
 - Always review the full Scan results before making changes
 - Apply hardening incrementally and verify results
-

What to Do Next

After reviewing the dashboard:

1. Open the Scan page for detailed findings
 2. Review individual issues
 3. Begin applying hardening controls
-

Related

- [Running Your First Scan](#)
 - [Scan Risk Score Explained](#)
 - [Applying Hardening Safely](#)
-

Revision #1

Created 2026-04-04 18:48:26 UTC by Jason Wassing

Updated 2026-04-04 18:48:26 UTC by Jason Wassing