Restrict XML-RPC

What This Does

This protection restricts or disables access to the WordPress XML-RPC interface.

It reduces exposure to certain types of automated attacks that target this endpoint.

Why It Matters

XML-RPC is a remote access feature that allows external systems to interact with your WordPress site.

While useful in some cases, it is commonly targeted for:

- brute force login attacks
- pingback and amplification attacks
- automated abuse of authentication endpoints

If not needed, leaving XML-RPC enabled increases your attack surface.

When to Apply It

This protection is recommended for most WordPress sites.

Apply it when:

- you do not use XML-RPC functionality
- your site does not rely on remote publishing tools
- you want to reduce exposure to automated attacks

When Not to Apply It

Do not apply this protection if your site depends on XML-RPC.

This may include:

- certain mobile apps
- remote publishing tools
- integrations that rely on XML-RPC

If unsure, apply cautiously and test functionality.

How Steel Security Applies This

Steel Security restricts access to the XML-RPC endpoint (`xmlrpc.php`).

Depending on your environment, this may include:

- blocking access at the server level
- limiting allowed request types
- restricting access to specific conditions

This prevents unauthorized or unnecessary use of the interface.

What to Expect After Applying

After applying this protection:

- XML-RPC requests will be blocked or restricted
- automated attacks targeting the endpoint will be reduced
- your site functionality will remain unchanged if XML-RPC is not in use

---

How to Verify

To verify the protection:

1. Attempt to access `/xmlrpc.php` in your browser
2. Confirm that access is denied or restricted

Expected results include:

- a 403 Forbidden response
- a blocked or limited response

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 any integrations that rely on XML-RPC

Common Issues

Remote Publishing Stops Working

This indicates XML-RPC was in use.

If needed:

- revert the change
- confirm which tool requires XML-RPC
- consider alternative APIs (e.g., REST API)

Endpoint Still Accessible

- verify server rules are applied correctly
- check for caching or proxy interference
- confirm no conflicting configuration exists

Unexpected Behavior

- test all integrations after applying
- revert if functionality is impacted
- apply more targeted restrictions if needed

Related

- Disable File Editing in Admin
- Protect Configuration Files
- 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