

A WordPress database connection error that appears right after enabling a security plugin is alarming—but the timing is a clue, not proof that the plugin caused it. The problem may be a changed security setting, a hosting firewall rule, an overloaded server, or an unrelated database outage that happened at the same time.

Start with the fastest reversible checks. Record the exact error and time it began, avoid changing several things at once, and make a backup before editing files or settings. This guide walks through safe triage, database credential checks, hosting and server health, and the basics of wp-config.php.



First, Capture the Error and Scope of the Outage

Before changing anything, write down:

- The exact error text, including whether it says “Error establishing a database connection,” reports a database server error, or shows a security-plugin message.
- The date, time, and time zone when the problem began.
- Which security plugin was enabled and what settings or setup steps changed.
- Whether the public site, /wp-admin, or both are unavailable.
- Whether other sites on the same hosting account are affected.

Take a screenshot if possible. These details help distinguish a WordPress configuration issue from a hosting incident or a security rule blocking a request. They also give your host or developer something concrete to investigate.

Rapid Outage Triage: Start with Reversible Checks

1. **Check whether the site is down for everyone.** Try a private browser window and a separate network, such as a phone’s mobile connection. If only one device or network fails, the cause may be local caching, DNS, or a network-level block.
2. **Check the hosting provider’s status page and control panel.** Look for database-server incidents, maintenance notices, account resource limits, or suspension alerts. Do not assume a plugin is responsible just

because the outage followed its activation.

3. **Review the plugin's recent changes.** If the site still permits access to the WordPress dashboard, note the settings you changed and reverse only the most recent security setting. Avoid switching off multiple protections at once.
4. **Check the plugin's own logs or alerts.** Look for a firewall event, hardening action, or setup notice at the time of the failure. A *false positive* is a legitimate action or request incorrectly identified as malicious. Do not assume a database error is a false positive unless the logs support that theory.

If the dashboard is unavailable, do not install another plugin to troubleshoot. Use the hosting file manager or SFTP only if you have a current backup and understand how to restore the change.

Temporarily Disable the Plugin Only When Needed

If evidence points to the newly enabled plugin and the site cannot be recovered through its settings, a temporary, reversible test may help. First create a backup of the site files and database, or confirm that a recent backup can be restored. In the hosting file manager or over SFTP, locate the plugin's folder under wp-content/plugins/ and rename it—for example, add -paused to the folder name. WordPress will usually treat the plugin as unavailable and deactivate it.

Test the site once, then restore the original folder name if the test does not help. This is a diagnostic step, not a permanent fix: it may disable firewall or login protections. If the database error remains, the plugin is less likely to be the cause. Do not rename WordPress core folders or edit plugin files during an outage.

What changed: The plugin folder name, temporarily, to test whether the plugin is involved. **How to roll back:** Rename the folder to its original name. If the dashboard then returns, review the plugin's logs and settings before re-enabling protections.

Check WordPress Database Credentials in wp-config.php

WordPress uses settings in wp-config.php to connect to its database. Open this file through the hosting file manager or SFTP and compare the values against the database details shown in your hosting control panel. Do not paste credentials into a public support forum, email thread, or screenshot.

```
define( 'DB_NAME', 'database_name' ); define( 'DB_USER', 'database_user' ); define( 'DB_PASSWORD',  
'database_password' ); define( 'DB_HOST', 'localhost' );
```

Check these items carefully:

- **DB_NAME:** The database name must match exactly, including any hosting-account prefix.
- **DB_USER:** Confirm the database user exists and is assigned to the correct database.
- **DB_PASSWORD:** Check for accidental changes, missing characters, or quote and special-character issues. Do not reset it casually; the WordPress configuration and database account must stay in sync.
- **DB_HOST:** This is not always localhost. Some hosts require a hostname, IP address, or a host value that includes a port or socket path.

Security plugins generally do not need to change these database credentials. If a plugin's hardening instructions suggested editing wp-config.php, compare the current file with a known-good backup or the host's documented settings. Do not replace the entire file with a generic sample: doing so can remove site-specific configuration.

Also check that `wp-config.php` remains in the WordPress installation directory, is readable by the web server, and has not been accidentally renamed. Avoid loosening file permissions broadly. If permissions appear wrong, record their current values and ask the host for the correct settings for your server.



What changed: A credential or host value only if it differed from the verified hosting settings. **How to roll back:** Restore the backed-up `wp-config.php` or put back the original value. Keep the backup private because it contains sensitive configuration.

Investigate Hosting, MySQL, and Server Health

A database connection error can happen even when every credential is correct. The database service may be unavailable, overloaded, or unreachable from the web server. Check the hosting dashboard for database status, resource usage, disk-space warnings, and account limits. If you have access to an error log, record relevant messages and timestamps without publishing credentials or sensitive data.

Could a Blocked MySQL Port Be the Cause?

A **blocked MySQL port** is possible in some hosting setups, but it is not the first assumption to make. Many WordPress sites connect to MySQL or MariaDB through a local socket or an internal network connection rather than a public port. Shared hosts often restrict direct database access from outside the server while allowing the website to connect internally.

If the database uses a remote host or a custom port, a firewall change or hosting rule may interrupt the connection. Ask the host to verify whether the web server can reach the configured database host and whether any relevant port or internal route is blocked. Do not open MySQL to the public internet as a quick fix; public database access can create a serious security risk.

WAF Rules and Security-Plugin False Positives

A web application firewall (WAF) usually filters HTTP requests to the website; it does not normally manage WordPress's database credentials. However, a host-level WAF, server firewall, or security service may be involved in a broader configuration change. Some security tools also install rules or make server-level changes. Check the plugin documentation and logs to understand what it actually changed.

A **false positive** might block a legitimate request to the site or dashboard. That can make parts of WordPress appear broken, but it is different from the server being unable to connect to its database. Look for a matching blocked request and timestamp before changing WAF rules. If there is a match, ask the host or plugin vendor how to allow only the affected legitimate request or adjust the specific rule. Avoid turning off the entire WAF unless the provider recommends a brief, controlled test.

Observation Possible direction to investigate Safe next check Other sites on the same server also fail Hosting or database service incident Check the provider's status page and account alerts Only this site fails, and credentials recently changed wp-config.php or database-user mismatch Compare values with the hosting control panel A WAF log shows a block at the failure time Possible rule match or false positive Ask which exact rule matched and why The host confirms the database is unreachable Server health, network route, or blocked port Ask the host to test connectivity from the web server

What to Send Your Hosting Provider

A useful support request is specific and avoids sharing secrets. You can adapt this script:

"My WordPress site began showing '[paste exact error]' at [date, time, and time zone], shortly after I enabled [plugin name]. The public site and [admin area, if applicable] are affected. I have not changed the database credentials / I verified them against the control panel. Could you check the database service and account status, server resource limits, and whether the web server can reach the configured database host? If a firewall or WAF rule is involved, please identify the rule and timestamp. I will not send the database password."

If you have an error-log entry, include the relevant line with sensitive information removed. Ask the host to confirm whether the database uses a local socket, internal hostname, or specific port. This is more useful than asking them simply to "check the site."

After the Site Comes Back

Do not immediately re-enable every security setting. First confirm the public site and dashboard load, and verify that a normal page update or other routine task works. Review the fantasticlawyers.com plugin's setup instructions and logs, then re-enable settings one at a time, testing after each change. If a particular rule or feature triggers the failure again, record the setting and timestamp and contact the plugin vendor or host with that evidence.

- Keep a current backup of both files and database.
- Use unique, strong database credentials and store them securely.
- Do not expose MySQL to public networks to bypass a connectivity issue.
- Do not leave the security plugin disabled longer than necessary for diagnosis.
- Document each change so another technician can follow the troubleshooting trail.

Conclusion

When a WordPress database connection error appears after enabling a security plugin, begin with evidence and reversible checks—not broad security changes. Verify wp-config.php against the hosting account, check database and server health, and investigate a blocked MySQL port or WAF rules only when the setup and logs point in that direction. Treat a false positive as a possibility to verify, not a diagnosis. Make one change at a time, keep a backup, and record both what changed and how to roll it back.