QKits Electronics

User Guide

SearchAbuse Protection Module for Magento 2

Module: QKits_SearchAbuse

Version: 2.2.0

Platform: Magento 2.4.x

Website: https://modules.qkits.com

Support: support@qkits.com

Table of Contents

Copyright 2025-2026 QKits Electronics

1. Dashboard Overview

The SearchAbuse Dashboard is your central control panel. Access it from the admin sidebar under **Search Abuse > Dashboard**.

1.1 Status Cards

The top row displays four real-time metrics:

• **Active Bans** (red) — Number of IPs currently banned

• **.htaccess Denies** (amber) — Number of Deny rules in .htaccess

• **Whitelisted IPs** (green) — Protected IP addresses

• **Blocked Terms** (blue) — Custom search terms being blocked

1.2 Quick Actions

• **Refresh .htaccess** — Regenerates the Deny rules block in .htaccess from the current ban list

• **Clean Expired Bans** — Manually removes bans that have passed their expiry time

1.3 Activity Log

The bottom of the dashboard shows recent SearchAbuse activity from system.log, color-coded by type: throttle events (yellow), blocks (red), and ban operations (orange).

2. Managing Bans

2.1 Viewing Active Bans

The Dashboard shows the 10 most recent bans. Click "Manage Bans" for the full list. Each entry shows:

• IP address of the banned visitor

• Reason for the ban (pattern matched, throttle violation, etc.)

• Offense count (progressive penalty level)

• Expiry time or "permanent"

• When the ban was created

2.2 Unbanning an IP

Click the "Unban" button next to any banned IP on the Dashboard or Manage Bans page. This removes the IP from the ban file and regenerates .htaccess automatically.

2.3 Manual Ban via CLI

```
# Ban an IP for 1 hour (3600 seconds) bin/magento qkits:searchabuse:manage ban --ip=1.2.3.4 --reason="manual ban" --duration=3600 # Permanent ban (omit --duration) bin/magento qkits:searchabuse:manage ban --ip=1.2.3.4 --reason="persistent attacker"
```

3. IP Whitelist Management

Whitelisted IPs are completely exempt from throttling and banning. Always whitelist your own IP, office IPs, and any trusted services that interact with your search.

Copyright 2025-2026 QKits Electronics

3.1 Adding IPs via Admin Config

Go to **Stores > Configuration > QKits > Search Abuse Protection > IP Whitelist**. Enter IPs one per line in the textarea and Save.

3.2 Adding IPs via Dashboard

From **Search Abuse > Dashboard > Whitelisted IPs**, click "Manage" to add or remove IPs. You can also use **Search Abuse > Whitelist** from the sidebar menu.

3.3 CIDR Range Support

You can whitelist entire subnets using CIDR notation:

```
192.168.1.0/24 # Entire local network
10.0.0.0/8 # All 10.x.x.x addresses
24.50.35.151 # Single IP
```


Copyright 2025-2026 QKits Electronics

4. Blocked Search Terms

Custom blocked terms are checked in addition to the built-in pattern detection (SQL injection, XSS, etc.). Use these to block spam terms, competitor names, or unwanted search content.

4.1 Managing Terms from the Dashboard

The Blocked Terms section on the Dashboard provides:

• **Add:** Type terms in the input field (comma-separated) and click Add

• **Remove:** Type a term and click Remove, or click the X next to any term

• **Search/Filter:** Typing in the input field filters the list in real-time

• **List/CSV toggle:** Switch between table view and compact CSV view

4.2 Managing Terms from Admin Config

Go to **Stores > Configuration > QKits > Search Abuse Protection > Blocked Search Terms**. The textarea syncs with the file automatically on save.

4.3 How Term Matching Works

Terms are case-insensitive and match anywhere in the search query. If a blocked term is "casino", then searches for "best casino games" or "CASINO online" will both be blocked.

5. Dashboard Ban Button — New in v2.2.0

The admin dashboard Last Search Terms widget now includes a **Ban** button next to each search term. This lets you add a term to the blocked list with a single click, without navigating away from the dashboard.

5.1 Using the Ban Button

1. Go to the Magento admin dashboard (the home page after login).

2. Scroll to the **Last Search Terms** widget in the right column.

3. You will see a fourth column labelled **Block** with a red Ban button on each row.

4. Click **Ban** next to any search term you want to block.

5. The page reloads with a success (or "already blocked") message at the top.

> *The term is immediately added to **var/qkits/qkits_block_terms.txt** and will block any future search containing that term.*

5.2 What Happens After Banning

Action	Result
Click Ban on a new term	Term added to blocked list, page redirects back to dashboard with success message
Click Ban on existing term	Warning: already blocked. No duplicate added.
Empty term	Error: no valid terms found.

Copyright 2025-2026 QKits Electronics

6. Configuration Reference

All settings are at **Stores > Configuration > QKits > Search Abuse Protection**.

Setting	Default	Description
Enable Module	Yes	Master on/off switch
Cooldown Period	30 sec	Minimum time between searches per IP
Violations Before Ban	3	Throttle violations within 1 hour before auto-ban
Max Query Length	200	Searches longer than this are blocked
Auto-Update .htaccess	Yes	Write Deny rules on ban/unban
Max Entry Age	30 days	Deny rules older than this are removed
1st Offense	300 sec	5 minute ban
2nd Offense	1800 sec	30 minute ban
3rd Offense	3600 sec	1 hour ban
4th Offense	86400 sec	24 hour ban
5th+ Offense	(empty)	Permanent ban — leave empty

7. CLI Commands

All commands use: **bin/magento qkits:searchabuse:manage <action> [options]**

Command	Description
list	Show all active bans
ban --ip=X --reason="Y"	Ban an IP (add --duration=N for timed ban)
unban --ip=X	Remove a ban
cleanup	Remove expired bans
apache	Regenerate .htaccess Deny rules

8. How Detection Works

8.1 Defense Layers

SearchAbuse operates at three levels:

• **Apache (.htaccess):** Banned IPs are blocked before PHP loads. Deny rules are injected between marker comments and read on every request.

• **PHP Middleware:** The BanCheckMiddleware plugin checks the ban file on every request as a backup layer (also works on Nginx).

• **Search Observer:** Monitors actual search queries for malicious patterns and applies throttling and progressive bans.

8.2 Built-in Detection Patterns

Copyright 2025-2026 QKits Electronics

Pattern	Detects
special_chars	Brackets, semicolons, backticks, pipes
sql_injection	SELECT FROM, UNION ALL, INFORMATION_SCHEMA, SLEEP()
xss_attempt	alert(), <script>, onerror=, javascript:
sql_commands	UPDATE SET, DELETE FROM, INSERT INTO, DROP TABLE
url_injection	http://, https://, ftp:// in search queries
shell_commands	wget, curl, exec, eval, system
path_traversal	../ sequences and encoded variants
query_length	Searches exceeding max query length

8.3 Progressive Penalty Flow

When abuse is detected, the penalty escalates with each repeat offense from the same IP:

1st offense: 5 min ban → 2nd: 30 min → 3rd: 1 hour → 4th: 24 hours → 5th+: Permanent

9. Log Files and Monitoring

9.1 Log Locations

File	Contents
var/log/system.log	All SearchAbuse events (blocks, bans, throttles, cron)
var/search_abuse_YYYY-MM-DD.log	Daily dedicated SearchAbuse log (auto-rotated)
var/qkits/ban/qkits_banned_ips.txt	Active bans with expiry and offense data

9.2 Monitoring Commands

```
# Watch live activity tail -f var/log/system.log | grep SearchAbuse # Check today's dedicated log cat var/search_abuse_$(date +%Y-%m-%d).log # Count active bans bin/magento qkits:searchabuse:manage list
```

9.3 Log Retention

Daily log files (search_abuse_*.log) are automatically deleted after 30 days. The cron job runs hourly to clean expired bans and is configured in the module's crontab.xml.

Copyright 2025-2026 QKits Electronics