

PUBLIC RELEASE

Phoenix IP Investigation & Block Manager

Installation, configuration and user guide

Version 1.0

CE Phoenix 1.1.0.6 / PHP 8.2

Core-file-free add-on

Lookup public visitor IPs from Who's Online, review network and estimated country information, and apply controlled exact-IP blocks.

1. Overview

Phoenix IP Investigation & Block Manager adds an administrator-controlled investigation and exact-IP blocking workflow to the Phoenix Who's Online page. It uses hooks, a separate manager page and add-on tables; no Phoenix core file is replaced.

Main capabilities

- Turn each public IP shown on Who's Online into an on-demand lookup button.
- Show reverse DNS, RDAP network ownership and address range information.
- Optionally show AbuseIPDB score, ISP and report totals.
- Optionally show IPinfo Lite country-level geolocation, kept separate from registration country.
- Create exact IPv4 or IPv6 database blocks for 24 hours, 7 days, 30 days or permanently.
- Create permanent Apache/LiteSpeed .htaccess blocks, alone or combined with database enforcement.
- Review and remove blocks from Admin, with administrator and creation-time records.

Compatibility and requirements

Item	Requirement
Cart	CE Phoenix 1.1.0.6
PHP	PHP 8.2 with cURL enabled for external lookups
Database	MySQL or MariaDB using InnoDB
Database blocking	Any web server running Phoenix; matches REMOTE_ADDR
.htaccess blocking	Apache 2.4-compatible rules or compatible LiteSpeed server
Admin folder	Standard or renamed; installation instructions cover both

Important

This add-on blocks exact public IP addresses only. It does not block countries, organisations, autonomous systems or CIDR ranges, and it never blocks automatically.

What the lookup means

RDAP describes network registration. IPinfo Lite and AbuseIPDB may estimate the country where an address is being used. For satellite, mobile, VPN, proxy and cloud networks, the estimated country may be the gateway or network exit point rather than the visitor's physical location.

2. Installation

Back up the Phoenix database and catalog-root .htaccess file before installation. Test .htaccess enforcement cautiously and retain hosting file-manager or SSH access for recovery.

New installation

- 1 Extract the release package locally.
- 2 Copy everything inside **catalog/** over the Phoenix shop while preserving the directory structure.
- 3 If Admin has been renamed, copy the contents of this package's **catalog/admin/** into the renamed Admin directory. Do not create a second public /admin/ directory.
- 4 Sign in to Phoenix Admin and open **Tools > IP Investigation & Block Manager**.
- 5 Select **Install database tables**. The operation creates only the add-on tables listed below.
- 6 Configure optional lookup providers, then open **Tools > Who's Online** and test a public IP lookup.

Tables created

Table	Purpose
ip_blocker_blocks	Block method, duration, reason, administrator and timestamps
ip_blocker_settings	Lookup cache, optional provider credentials and .htaccess path
ip_blocker_lookup_cache	Cached administrator-requested lookup results

Core-file status

All PHP files in this release are additional add-on files. No native Phoenix file needs to be edited or overwritten.

3. Configuration

Open **Tools > IP Investigation & Block Manager**. Provider credentials are optional: RDAP and reverse DNS work without an account, while the extra services add more context.

Lookup providers

Provider	Purpose	Configuration
RDAP	Network owner, handle, registration country and address range	Built in; no key
Reverse DNS	Hostname associated with the selected IP	Built in; no key
AbuseIPDB	Abuse confidence score, ISP, usage type and report count	Optional API key
IPinfo Lite	Estimated connection country and ISO code; useful for global networks	Optional API token

Provider setup

AbuseIPDB: create an account and API key at abuseipdb.com/register. Paste the key into the manager and save.

IPinfo Lite: create an account at ipinfo.io/signup. Paste the Lite API token into the manager and save.

Saving settings clears the lookup cache so newly added or removed providers take effect on the next lookup.

Cache duration

Lookup results are cached for 24 hours by default and may be set from 1 to 168 hours. Caching reduces repeat external requests. Use **Purge lookup cache** when fresh data is required immediately.

.htaccess path

Leave the path blank to use the catalog-root .htaccess file. A custom path is accepted only when its filename is exactly .htaccess and it is located inside the catalog directory.

Credential storage

AbuseIPDB keys and IPinfo tokens are stored as plain text in the add-on settings table. Protect Admin access, database accounts and backups. The IPinfo token is sent in an HTTPS Authorization header.

Status panel

The manager reports cURL availability, whether each optional provider is configured, the selected .htaccess path and whether the target file or directory is writable.

4. Investigating and blocking an IP

Lookup procedure

- 1 Open **Tools > Who's Online**.
- 2 Select the blue lookup control beside a public IP address.
- 3 Review the network, address range, registration country and estimated connection country.
- 4 If configured, review AbuseIPDB information as supporting evidence only.
- 5 Enter a short reason, choose a duration and enforcement method, then select **Block this IP** only when appropriate.

Lookup fields

Field	Meaning
Reverse DNS	Hostname returned for the address, when available
Network / range	RDAP registration name and the registered address interval
Network registration country	Country attached to the RDAP network record
Estimated connection country	IPinfo Lite estimate, with AbuseIPDB country as a fallback
Abuse score / reports	Third-party reports; not proof that the current visitor is malicious

Enforcement choices

Method	Available duration	Effect
Database	24 hours, 7 days, 30 days or permanent	Phoenix checks REMOTE_ADDR early and returns HTTP 403 on a match
.htaccess	Permanent only	Web server refuses the IP before Phoenix/PHP starts
Database + .htaccess	Permanent only	Records the block in the manager and enforces at both layers

Self-block protection The manager refuses to add the administrator's current REMOTE_ADDR. This reduces accidental lockout but does not replace careful testing, especially behind proxies.

Removing a block

Open the manager and select **Unblock** beside the record. Database enforcement stops immediately. For .htaccess methods the managed rule section is rebuilt automatically.

5. Security, privacy and server behaviour

Safe decision-making

- Do not block solely because an IP is foreign, hosted, proxied or has an abuse score.
- Confirm behaviour using access logs, request rate, URLs requested and repeated patterns.
- Use a timed database block first when the evidence is uncertain.
- Never treat estimated country data as proof of a person's location.
- The add-on intentionally has no automatic score-based or country-based blocking.

Proxy and Cloudflare warning

V1.0 reads REMOTE_ADDR only. Behind Cloudflare, a reverse proxy or a load balancer, that value may be the proxy rather than the visitor. The add-on deliberately does not trust forwarded-IP headers because an unverified header can be spoofed.

Before using database blocks behind a proxy

Confirm that Who's Online and REMOTE_ADDR contain the real client IP through a trusted server-level proxy configuration. Otherwise a database block could target the proxy shared by many visitors.

External lookup privacy

No external lookup occurs simply by opening Who's Online. When an administrator selects lookup, the selected IP is sent to rdap.org and, when enabled, AbuseIPDB and IPinfo Lite. Review the providers' current privacy terms before enabling optional services.

Request protection

- Lookup and block actions require an authenticated Phoenix administrator session.
- State-changing requests use the Phoenix session form token.
- Only valid public IPv4 and IPv6 addresses are accepted.
- Lookup responses are size-limited, time-limited and restricted to HTTPS.
- Returned provider data is inserted into the popup as text rather than executable HTML.

Resource use

Database enforcement runs early in storefront startup but still requires PHP and a database connection.

Permanent .htaccess enforcement saves more resources because the server rejects the address before Phoenix starts. Lookup services run only on administrator request and results are cached.

6. .htaccess, maintenance and recovery

Managed section

The add-on changes only the content between these markers:

```
# BEGIN PHOENIX IP BLOCKER
... managed Require rules ...
# END PHOENIX IP BLOCKER
```

Backup and replacement

Before replacing an existing file, the add-on creates `.htaccess.ipblocker.bak`. It writes a temporary file, preserves existing permissions where possible and then activates the replacement by rename.

Recovery from a server error

- 1 Use the hosting file manager or SSH; Admin may be unavailable if `.htaccess` syntax is rejected.
- 2 Restore `.htaccess.ipblocker.bak` as the live `.htaccess` file, or remove only the marked Phoenix IP Blocker section.
- 3 Confirm the storefront and Admin open normally.
- 4 Use database enforcement instead if the server is nginx, Apache 2.2 or otherwise incompatible with Apache 2.4 Require rules.

Routine maintenance

- Review permanent blocks periodically and remove those no longer needed.
- Expired timed records remain visible as inactive history until manually removed.
- Use Rebuild managed rules after restoring or manually editing `.htaccess`.
- Purge cached lookup data whenever a fresh provider response is required.
- Rotate external API credentials in line with provider guidance.

Timed rule design

Timed blocks are database-only. A permanent web-server rule cannot reliably expire itself without a scheduled process, so V1.0 prevents timed `.htaccess` selections.

7. Removal, troubleshooting and release notes

Uninstall

- 1 Remove all records from the manager so the managed .htaccess section is rebuilt without blocked addresses.
- 2 Delete the add-on files listed in FILELIST.txt. Apply the Admin paths to the real renamed Admin directory where applicable.
- 3 If the stored data is no longer required, run UNINSTALL.sql against the Phoenix database.
- 4 After checking the live file, manually remove the empty managed section and optional .htaccess backup if desired.

Troubleshooting

Symptom	Check
Popup returns an Admin page	Copy all current hook, language and action files into the correct Admin path; then sign in again
Country is blank	Configure IPinfo Lite, save settings to clear cache, and repeat the lookup
Provider warning	Confirm cURL, outbound HTTPS, token/key validity and the provider's service status
.htaccess is not writable	Use database mode or correct ownership/permissions through the host; do not grant unsafe broad write permissions
Blocked visitor still connects	Confirm the address is exact, the record is active, and REMOTE_ADDR is not a proxy address
Administrator is locked out	Restore the backup or remove the managed .htaccess section using hosting access

V1.0 release summary

First public release. Includes the Who's Online popup workflow, RDAP and reverse-DNS investigation, optional AbuseIPDB and IPinfo Lite enrichment, exact-IP database and .htaccess blocking, timed database rules, self-block protection, lookup caching, managed-rule backup/rebuild, block history and removal controls.

Package support files

File	Purpose
FILELIST.txt	Complete list of PHP files added by the release
UNINSTALL.sql	Optional removal of the three add-on database tables
Phoenix_IP_Investigation_Block_Manager_V1.0_Documentation.pdf	This installation, operation and security guide

Phoenix, E-Commerce made Easy - <https://phoenixcart.org>

Copyright (c) 2026 Mort-Lemur. Released under the GNU General Public License.