Web Proxy Checker

Web Proxy Checker Technical Documentation (PDF Edition)

Vitaly Yakovlev

Table of Contents

1. Introduction

1.1 Technical Documentation: Web Proxy Checker

Web Proxy Checker is a high-performance software with a graphical user interface (GUI) designed for mass validation of proxy server lists. The application is tailored for specialists who work extensively with network proxies (e.g., developers of web scrapers and parsers) and offers deep customization for import, testing, and result export processes.

Web Proxy Checker Webpage: https://optinsoft.net/wpc/

2. Overview

2.1 1. Main Program Window

The main window interface is divided into three functional zones: the tab panel (top section), the global settings block (center section), and the control panel with statistics (bottom section).

2.2 1.1. Tab Panel

Provides navigation between the core sections of the application:

- Proxies: Management of the current proxy list and result export rules.
- Proxy Sources: Configuration of sources for automatic proxy loading.
- Check Settings: Selection of validation modes and filtering parameters.
- HTTP: Configuration of timeouts and header rotation for web-based checks.
- DNS: Management of DNS servers and query parameters.
- Geo IP: Integration of geographic databases.
- Log: Real-time monitoring and debugging of application performance.
- Threads: Visualization of active thread states.
- Locks: Tracking of internal synchronization locks.
- Notifications: Configuration of external alert channels.
- About: Reference and licensing information.

2.3 1.2. Global Settings

Located directly beneath the tabs, these settings apply to the entire pool of verified proxies:

- Default proxy type: Specifies the algorithm used to determine the proxy type if it is not explicitly declared in the source. Available modes: AUTO (automatic detection), HTTPS, SOCKS4, SOCKS5. Recommendation: If the type is known in advance, specify it explicitly to accelerate the validation process. (An individual type specified within source settings overrides this global option).
- Remove duplicates: Automatic removal of duplicate entries before a session begins.
- Shuffle: Randomizes the order of the proxy list prior to launching the test sequence.

2.3.1 1.3. Control Panel and Statistics

The bottom section of the interface aggregates technical metrics and control elements:

- Control Buttons: Start (initiates verification), Stop (forces a halt), and Close (exits the application).
- Process Indicators: Current session progress bar, text status message (e.g., "Checking..."), elapsed check time counter (Elapsed), and the number of successfully read proxies (Read).
- Thread Parameters: Check Threads (number of concurrent parallel threads), Async tasks per thread (number of asynchronous tasks per thread), and Re-check every X seconds (the interval for automated verification restarts).
- Statistical Counters:
- Good Proxies: The number of valid proxies.
- Bad Proxies: The number of non-functional or rejected proxies.
- Active Checkers: The count of currently active verification modules.
- Bytes Received / Bytes Sent: Volume of incoming and outgoing network traffic.
- Exact Application Start Time: (e.g., `Application started at 2026-07-12 11:44:45`)
- Current Working Directory: (e.g., `C:\Program Files\WebProxyChecker`).

3. Proxy List Management and Result Exporting

3.1 2. Proxy List Management and Result Exporting (Proxies Tab)

3.2 2.1. Interactive Table

The central element of this tab is the proxy list, configured with the following column structure: host, port, type, user, pass, sid, status, add time, check time, duration, anonymity, external IP, country, city, state, postal code. Directly below the table are the item management buttons: Delete, Edit, Move Up, Move Down, Select All, Unselect All, Delete All.

3.3 2.2. Manual Addition (Add... Dialog)

Clicking the Add... button opens a dialog window with two tabs:

1. Single Proxy: Input fields for adding individual proxies manually — Host, Port, User, Password, SID, Type.
2. Proxy List: A multi-line edit text field for bulk insertion. The user can specify the proxy type (default, HTTPS, SOCKS4, SOCKS5, AUTO) and set a line-parsing template (e.g., `TEXT(user:pass@host:port[:type])`). An automated generation function for unique session identifiers (SIDs) is also available, featuring SID Tag (e.g., `#SID#`), SID Length, and SID Count parameters.

3.4 2.3. Result Export Settings

The bottom section of the tab controls data exporting to external files. These settings are distributed across 4 sub-tabs. Each sub-tab includes an Overwrite checkbox (replaces the file contents instead of appending to the end) and a text field for inputting paths separated by a semicolon `;` (to simultaneously duplicate the output to multiple locations), for example:

```
C:\temp\p-good.txt;C:\temp\p-good-%%date%%.txt;C:\temp\p-good-{FP}.txt
```

3.5 2.3.1. Good Proxies

Web Proxy Checker supports splitting the final output file into parts using the Split checkbox. Clicking the pen icon button opens the Edit File Path dialog, which is split into two tabs:

1. Tags: A list of macros for dynamic file name generation:
   - `%%date%%` — current date (e.g., `2026_07_12`).
   - `%%date:yyyy_mm_dd%%` — current date with a customizable format.
   - `%%datetime%%` — current date and time (e.g., `2026_07_12_19_15_47`).
   - `%%datetime:yyyyy_mm_dd_hh_nn_ss%%` — current date and time with a custom format.
   - `%%time%%` — current time (e.g., `19_15_47`).
   - `%%time:hh_nn_ss%%` — current time with a custom format.
2. Parts: Allows configuring file splitting using the `{FP}` tag. If you specify `Part1` and `Part2` in the parts list, the program will split the export into two roughly equal segments, generating file names such as `p-good-Part1.txt` and `p-good-Part2.txt`.

3.6 2.3.2. Bad Proxies

This section mirrors the settings, logic, and path macros of the Good Proxies tab; however, the file splitting (Split) functionality is disabled for this result type as it is unnecessary.

3.7 2.3.3. Fastest Proxies

Allows saving a "top" list of servers with the lowest response latency. You can specify the maximum number of hosts to retain alongside three specialized parameters:

- Save partial results after check each X proxies: Flushes intermediate results to the file during the verification process, without waiting for the entire session to conclude.
- Min fastest proxies: The minimum capacity threshold. If the number of valid proxies falls below this value, the program will not overwrite the existing results file, protecting it from data corruption.
- Fresh proxies first (checkbox) used in conjunction with the fresh proxy duration: X seconds parameter: Prioritizes testing newly added proxy servers for immediate deployment to your user software.

3.8 2.3.4. Proxies for Country (Geographic Sorting)

Provides automated filtering and allocation of proxy addresses into distinct files based on country codes using the `{CC}` macro.

Usage Example: If you set the country list string to `US;CA;GB` and the path to `C:\Temp\p-good-{CC}.txt`, the application will automatically generate files such as `p-good-US.txt`, `p-good-CA.txt`, and so forth.

3.9 2.4. Output Formatting (Output Format)

The application offers three basic output line templates:

1. `TEXT(user:pass@host:port[:type])`
2. `TEXT(host:port[:type:user:pass])`
3. `TEXT(host,port,[type,user,pass])`

The `TEXT(` prefix and the closing parenthesis are UI designations indicating a text format; they are not written to the actual output file. Square brackets indicate optional parameters.

Output line structure modifiers (checkboxes):

- Out proxy type prefix: Prepends a type marker to the very beginning of the line (`#` for HTTP, `+` for SOCKS4, `*` for SOCKS5). When activated, the type suffix at the end of the line (`[:type]`) is omitted (e.g., `#127.0.0.1:8888`).
- Don't out proxy type: Completely excludes protocol information from the output data.
- Out resolved IP / Out anonymity level / Out SID as User
- Geographic Modifiers: Out resolved IP country, Out resolved IP state, Out resolved IP city, Out resolved IP postal code.

4. Data Sources

4.1 3. Data Sources (Proxy Sources Tab)

This section is engineered to automate the collection of proxy lists. The primary interface element is a data table featuring the following columns: path, format, proxy type, extract, process type. Each row contains a checkbox for rapidly enabling or disabling that specific source from the synchronization loop. To the right of the table are the management control buttons: Add..., Edit, Delete, View File, Explore to file, Move Up, Move Down, Check All, Uncheck All, Check Selected, Select All, Unselect All.

4.2 3.1. Source Parameters (Add Source Dialog)

A source can be configured as either a local file path or a remote URL network asset.

- File Path/URL: The path pointing to the proxy server source. Adjacent buttons include ... (browse), View (inspects contents inside an internal viewer window), and Explore to file (opens the target directory inside Windows Explorer).
- Format: Selects one of three standard text-parsing templates (identical to Section 2.4).
- HTTP Headers: Configures custom request headers (Accept, Referer, User Agent) to bypass remote web server restrictions when fetching lists.
- SID Tag: An option to enable automated SID generation, containing SID Tag, SID Length, and SID Count parameters.

4.3 3.2. Advanced Parsing (Regular Expressions)

To extract proxies from unstructured text payloads or complex HTML source code, regular expression engines are utilized:

- Extract Pattern: A regular expression (Regex) pattern used to capture the target data block. For example, given the following HTML line: `<tr><td class="left"><script>document.write(Base64.decode("MTI3LjAuMC4x"))</script></td><td><span class="fport">1088</span></td></tr>`

  The pattern `decode\("([^"]+)".+<span class="fport"[^>]+>([0-9]+)` will locate the target match: `decode("MTI3LjAuMC4x"))</script></td><td style=""><span class="fport" style="">1088`, yielding Group 1: `MTI3LjAuMC4x` and Group 2: `1088`.
- Extract Rule: A structural template to assemble a standardized proxy string using the captured Regex groups ($1, $2, etc.). It supports text literals and built-in conversion string functions:

a. `decode_base64(...)` — Decodes Base64-encoded strings.

b. `decode_url(...)` — Decodes URL-encoded strings.

Example Rule: For the payload scenario above, the rule decode_base64($1):$2 transforms the raw input into the standard format: 127.0.0.1:1088.

- Extract from tag: Narrows down the Regex scanning surface area to a specific HTML tag. It requires a tag name (e.g., tr) and an inspection scope context within it: body (inner text contents) or attribute (value of a specific tag attribute).
- Extract SID: Allows extracting pre-existing SIDs directly from the raw source content rather than generating them, using an identical set of independent Pattern and Rule parameters.
- Testing Utilities: The Subject text box is used to paste code fragments manually. The Load button fetches data into it directly from the designated File Path/URL, while the Test button executes a parsing pass to visually verify the correctness of the configured regular expressions.
- Exclude: Inverts the processing logic of the selected source. When enabled, any proxy found matching these extraction rules will be actively purged from the final verification list.

4.4 3.3. Global Source Parameters (Beneath the Table)

- Append: Appends newly loaded proxy servers to the end of the existing list. If this flag is untoggled, the primary working proxy pool is completely wiped clean before every import cycle.
- Min. X proxies in source: A fail-safe threshold barrier. If a source yields fewer than X proxies (e.g., a remote website encounters an error), the application ignores the update and preserves the existing working proxy pool, preventing operational failures in connected downstream software.
- Save all loaded proxies to file: Duplicates all collected raw, unverified proxies into a unified single file for subsequent external analysis.

5. Verification Modes and Parameters

5.1 4. Verification Modes and Parameters (Check Settings Tab)

The application supports 6 specialized validation modes, selectable at the top of the tab.

5.2 4.1. Available Modes

1. Check for URL: Tests proxy suitability for loading web pages (HTTP/HTTPS traffic).
2. Check for IMAP: Verifies the availability of incoming mail servers using the IMAP protocol.
3. Check for SMTP: Verifies email sending capabilities through a static SMTP server with fixed parameters.
4. Check for delivery: Dynamic delivery verification. The application automatically resolves the target SMTP server based on the domain and MX records of the recipient specified in the To field.
5. Check for connect: An express test to verify basic TCP network connection establishment with the proxy.
6. Load and combine: A service mode that skips network testing. It only performs collection, deduplication, shuffling, and merging of proxies from all sources into a single file.

5.3 4.2. Check for URL Mode Settings

- Request: Selection of the HTTP method (GET / POST), input field for the target URL, and the Handle redirect limit for redirect chains (e.g., maximum of 15).
- Parameters and Headers: The Parameters field accepts Key=Value strings. For the POST method, these are compiled into an application/x-www-form-urlencoded request body. The HTTP Headers field allows overriding default headers.
- Network Delays: Timeout retries (number of retries upon timeout) and Delay after check (pause duration after a check to prevent blocking by the target server).
- Validation Conditions (Success/Fail Conditions): Three rules based on regular expressions:

a. Check fails if response matches regular expression (Failure on match — protection against CAPTCHAs and blocking placeholders).

b. Check fails if response does not match regular expression (Failure on mismatch with the expected page HTML code).

c. Check succeeded if redirect location matches reg.ex. (Success status if the redirect URL matches the pattern).

5.4 External IP and Country Tabs (Inside Check for URL)

These tabs allow extracting network metadata from the response body or HTTP headers.

- The Fail check if external IP (country) is not found checkbox rejects the proxy if the data cannot be parsed.
- The Pattern and Rule parameter pairs configure the parser (e.g., for IP: pattern = `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`, rule = `$0`).
- The Extract from cookie option redirects the parser to search for the IP and country code inside a specific cookie by its name, bypassing the response body.

5.5 4.3. Check for IMAP Mode Settings

- Authorization Parameters: Host, Port fields, and the SSL encryption toggle.
- Login Checkbox: If disabled, the proxy is validated based on a successful TCP connection and receiving the server's welcome banner. If enabled, the application performs full authentication using the credentials from the Username/Password fields.

5.6 4.4. Check for SMTP and Check for delivery Mode Settings

For Check for SMTP, the following are configured: Host, Port, SSL (session encryption from startup), STARTTLS (switching to TLS within the session), and the Break on parameter.

The Break on parameter determines the stage of the SMTP protocol that is considered sufficient to mark the proxy as functional. Stop options include: HELO, AUTH, MAIL FROM:, RCPT TO:, DATA, RSET, QUIT.

The Check for delivery mode only contains the Break on setting, as server parameters are calculated on the fly. Both modes rely on the global SMTP Settings configuration.

6. SMTP Settings and Macros

6.1 5. SMTP Settings

The detailed configuration tab for email-based verifications is divided into 7 thematic sub-tabs:

- To: A list of target recipient email addresses.
- From: A list of sender accounts.
- Subject: A list of email subject lines.
- Body: The text block containing the email body.
- SMTP Servers: A preset table for domains configured with the following columns: Domain, Protocol, Server Host, Port, SSL, START TLS.
- SMTP Commands: A step-by-step transaction execution script with macro support. Example of an executable script:

```
EHLO [{%PROXY_HOST%}]
{%IFSET:STARTTLS%}STARTTLS{%ENDIFSET%}
{%IFSET:STARTTLS%}EHLO [{%PROXY_HOST%}]{%ENDIFSET%}
AUTH LOGIN
{%BASE64_BEGIN%}{%FROM_EMAIL%}{%BASE64_END%}
{%BASE64_BEGIN%}{%FROM_PASS%}{%BASE64_END%}
MAIL FROM:<{%FROM_EMAIL%}>
RCPT TO:<{%TO_EMAIL%}>
DATA
MIME-Version: 1.0
Date: {%EMAIL_DATE%}
To: {%TO_EMAIL%}
From: {%FROM_EMAIL%}
Subject: {%SUBJECT%}

{%BODY%}
.
RSET
QUIT
```

- Filters: Advanced evaluation rules for mail service responses:

a. By Greeting: Check fails if greeting matches, Check fails if greeting does not match, Check succeeded if greeting matches.

b. By Command Responses: Rule sets for Check fails if SMTP response matches / does not match and Check succeeded if SMTP response matches.

   Logic Example: Mapping the `RCPT` command and the `mailbox unavailable` regular expression to a `Check succeeded` rule ensures that a functional proxy server is not falsely rejected when encountering a non-existent recipient mailbox.

6.2 Reference Guide for Supported Macros: {% ... %}

The following macros can be used within the text input fields of the To, From, Subject, Body, and SMTP Commands sub-tabs:

Tag	Syntax / Example	Description
INCLUDE	{%INCLUDE:C:\file.txt%}	Full inclusion of the contents of an external text file.
TEXTF	{%TEXTF:C:\file.txt%}	Reads the entire text string from the specified file.
ROT	{%ROT:A	B
ROT$	{%ROT$:A	B
ROTF	{%ROTF:C:\file.txt%}	Sequential iteration (rotation) of lines from the specified file.
ROTF$	{%ROTF$:C:\file.txt%}	Rotates file lines and locks the selected line for the duration of the message.
RNDF	{%RNDF:C:\file.txt%}	Extracts a random line from the specified file.
RNDF$	{%RNDF$:C:\file.txt%}	Extracts a random line and locks its value within the current message.
WROTF	{%WROTF:C:\file.txt%}	Selects the next chronological word from the specified file.
SROTF	{%SROTF:C:\file.txt%}	Selects the next chronological sentence from the specified file.
RND	{%RND:%}	Generates a random string based on a specified character pattern template.
RND$	{%RND$:%}	Generates a random string based on a template and locks its value inside the message.
RNDIP	{%RNDIP:0.0.0.0-1.1.1.1%}	Outputs a random IP address from within the specified range boundaries.
DATETIME	{%DATETIME%}	Current date and time in a compacted format string (e.g., 20190123154539).
EMAIL_DATE	{%EMAIL_DATE%}	A timestamp structured according to the RFC 2822 standard for email headers.
URL	{%URL:http://site.com%}	Automatic URL encoding (converts special characters to %NN escape codes).
CHR	{%CHR:10%}	Inserts a control character into the stream using its decimal ASCII code.
E / EMPTY	{%E%} / {%EMPTY%}	An empty token delimiter tag.
REPEAT	{%REPEAT(1,10)%} X{%ENDREPEAT%}	Repeats a string a random number of times within the designated range boundary.
SHUFFLE	{%SHUFFLE%} Lines{%ENDSHUFFLE%}	Shuffles line items randomly within the boundaries of the block.
BASE64	{%BASE64%}Text{%ENDBASE64%}	Encodes block content elements into a Base64-compliant character string.
QP	{%QP%}Text{%ENDQP%}	Encodes block content elements into a Quoted-Printable format.
EMAIL / TO_EMAIL	{%EMAIL%} / {%TO_EMAIL%}	The full email address value of the recipient destination.
DOMAIN / TO_DOMAIN	{%DOMAIN%} / {%TO_DOMAIN%}	The domain segment portion extracted from the recipient email address.
ACCOUNT / TO_ACCOUNT	{%ACCOUNT%} / {%TO_ACCOUNT%}	The local-part inbox nickname string (left side of the @ sign) of the recipient box.

Tag	Syntax / Example	Description
NAME / TO_NAME	{%NAME%} / {%TO_NAME%}	The display name (alias moniker string) assigned to the recipient.
PASS / TO_PASS	{%PASS%} / {%TO_PASS%}	The recipient account password string.
FROM / FROM_EMAIL	{%FROM%} / {%FROM_EMAIL%}	The full email address value of the message sender account.
FROM_DOMAIN	{%FROM_DOMAIN%}	The domain segment portion extracted from the sender email address.
FROM_ACCOUNT	{%FROM_ACCOUNT%}	The local-part inbox nickname string of the sender mailbox.
FROM_NAME	{%FROM_NAME%}	The display name moniker string assigned to the sender.
FROM_PASS	{%FROM_PASS%}	The sender account password credentials string (utilized for SMTP authentication).
SUBJECT	{%SUBJECT%}	Dynamic injection of the currently evaluated email subject line.
BODY	{%BODY%}	Dynamic injection of the pre-processed email body text block.
MAILLISTCOLUMN	{%MAILLISTCOLUMN0%}...31	Refers to custom columns within the mailing list dataset (valid indices: 0 to 31).

7. Additional Verifications and Filters

7.1 6. Additional Verifications and Filters (Bottom Part of Check Settings)

7.2 6.1. Host Structure Validation

- Check proxy IP: Strict validation of the proxy host. Lines containing invalid IPs or alphabetical domains instead of literal IP addresses are automatically rejected.
- Check proxy host: Performs a mandatory preliminary DNS resolution for proxy hosts using alphabetical domain names.

7.3 6.2 External IP Address Identification

The Resolve external IP checkbox activates a request to a specialized web server specified in the Resolve IP URL field (e.g., `http://test-ipv6.com`). Clicking the link opens a dialog window where the Extract IP Pattern and Extract IP Rule fields configure the parsing of the returned IP address from the response body (e.g., from a JSON callback).

Resolve IP URL Example:

```
http://ipv4.test-ipv6.com/ip/
```

Extract IP Pattern Example:

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
```

Extract IP Rule Example:

```
$0
```

7.4 6.3 Anonymity Level Control

The Check for anonymous proxy checkbox activates a request to an echo server specified in the Anonymous proxy check URL field (e.g., `http://httpbin.io`), which returns all received HTTP headers. Clicking the link opens the Anonymous Proxy Check dialog, containing the following settings:

- "Forwarded" patterns: A list of regular expressions to detect traffic forwarding headers (`X-FORWARDED-FOR`, `FORWARDED`). Example:

```
("?)X[-_]FORWARDED[-_]FOR\1: ?("?)(.*)\2
("?)FORWARDED\1: ?("?)(.*)\2
```

- Extract "Forwarded" rule: An instruction for assembling the header value (e.g., `$3`).
- Mark proxy as "non-elite" if there are matched "Forwarded" patterns: Automatically assigns a "Non-elite" status to the proxy if there are matches within the Non-elite proxy patterns list (headers like `VIA`, `CLIENT-IP`, `PROXY-CONNECTION`, `X-CLUSTER-CLIENT-IP`). Example:

```
("?)VIA\1: ?("?)(.*)\2
("?)X[-_]CLUSTER[-_]CLIENT[-_]IP\1: ?("?)(.*)\2
("?)CLIENT[-_]IP\1: ?("?)(.*)\2
("?)PROXY[-_]CONNECTION\1: ?("?)(.*)\2
```

- Self IP list: A database of the user's real, local IP addresses. If any of these are detected in the echo response, the proxy is immediately flagged as Transparent.
- Extract real IP / Extract external IP: Regex patterns and rules for parsing `X-REAL-IP` and `REMOTE-ADDR` headers.

Extract real IP Example:

```
("?)X[-_]REAL[-_]IP\1: ?("?)(.*)\2
```

Extract external IP Example:

```
("?)REMOTE[-_]ADDR\1: ?("?)(.*)\2
```

- Non-anonymous proxy action: The control action to apply to non-anonymous proxies. Options include: None (ignore), Decline transparent proxies (reject transparent), Decline non-elite proxies (reject non-elite).

7.5 6.4 Checking IP Existence in RBL Lists

- The RBL check checkbox enables verification of the proxy IP against spam filters and blacklists. In the text field to the right of the checkbox, you can list servers separated by commas, for example: sbl-xbl.spamhaus.org,dnsbl.sorbs.net,bl.spamcop.net,combined.njabl.org. The RBL check link opens a window with detailed configurations:
- RBL Servers: A list of RBL hosts.
- Min. RBL positives (>=1): The sensitivity threshold. If set to 2, a proxy will be rejected only if it is simultaneously found in at least two different independent blacklists.
- Save proxies list in RBL to file / Save proxies not listed in RBL to file: Separate exports for clean and blacklisted proxy servers. These fields support path separation via a semicolon ;, the date macro %%date%%, and the Overwrite option.
- Re-check RBL'd proxies: A checkbox that allows re-checking proxy servers already identified as blacklisted in RBL (disabled by default to save network traffic).

7.6 6.5 Geo-location

The Find country geo location by using Geo IP database toggle enables matching the IP address with a local database to determine its geographic location.

7.7 6.6 Country Filtering

The Country filter toggle activates filtering based on the proxy's location. The filter operates with two parameters:

- Mode: Allow (only allow specified countries) or Disallow (block specified countries).
- Country list: A comma-separated list of country codes, for example: `CN,RU`.

7.8 6.7. rDNS Verification

The rDNS check toggle activates a Reverse DNS lookup operation to verify whether the proxy IP address has a valid domain name associated with it.

7.8.1 6.8. Ping

Enabling the ping proxy host option forces the proxy checker to send low-level ICMP requests (Ping) to verify the availability of the network node.

8. System and Service Tabs

8.1 7. System and Service Tabs

8.2 7.1. HTTP Tab

These parameters are focused on optimizing the performance of the Check for URL mode:

- Rotate User Agent: This checkbox enables cyclic rotation of browser identifiers. Available modes include List (the user inputs a list of UAs directly into the interface text field) and File (specifies a direct path to a plain text file containing a set of User Agents).
- Timeouts: Independent adjustments for critical network event wait times in seconds — Connection Timeout, Read Timeout, and Async Timeout.
- Accept: Configures the global HTTP header used for verification requests (e.g., `text/html, */*`).

8.3 7.2. DNS Tab

Configuration for domain name resolution:

- Custom DNS Servers: This checkbox switches the application from using the operating system's default DNS servers to a custom, user-defined text list of servers.
- Query Parameters: DNS query timeout (wait duration for a query response) and DNS query retries (number of retries upon a failed attempt).

8.4 7.3. Geo IP Tab

Starting from version 2, the application supports integration with MaxMind geographic databases exclusively in the modern binary .mmdb format. This tab specifies the local path to the database file.

Attention: The legacy plain text .csv file format is no longer supported.

8.5 7.4. Log Tab

Event monitoring panel. It outputs real-time text messages regarding application actions and features verbosity toggles:

- Detailed Log: Outputs extended technical details about all internal processes.
- IMAP Log: Activates verbose logging of IMAP sessions and raw commands.
- SMTP Log: Activates verbose logging of the command exchange sequence with SMTP servers.

8.6 7.5. Threads and Locks Tabs

Service panels for visual inspection of resource allocation:

- Threads: A dynamic table displaying the status and utilization of running threads.
- Locks: Monitoring of internal system synchronization locks to prevent data collisions.

8.7 7.6. Notification Tab

Integration with the Telegram messenger for remote monitoring of long-running validation tasks. The application sends an alert if a session begins to take an abnormally long time.

- Integration Settings: Telegram Bot ID (bot token) and Telegram Chat ID (recipient's chat ID).
- Trigger Condition: A checkbox and numerical field for Notify when elapsed seconds exceed (execution time limit in seconds; an alert is dispatched if exceeded).

8.8 7.7. About Tab

Contains foundational information about the software: the official commercial name, current release version index, and registration details of the license holder.

9. Links

- Program website