IP Monitor Configuration App – Documentation

Purpose

This application provides a **GUI for configuring, monitoring, and managing network IP blocking**. It works with the main monitoring script to block/unblock IPs using Windows Firewall, supports manual and automatic blocking, and allows configuration of allowed IP ranges.

Main Features

- **Configure Allowed IP Range:**
  Set the allowed IP prefix and range (start/end), and specify always-allowed IPs.
- **Manual Block/Unblock:**
  Manually block any IP (even in the allowed range) and manually unblock them.
- **Automatic Block/Unblock:**
  Automatically block IPs outside the allowed range and unblock them if they become allowed (unless manually blocked).
- **View Blocked IPs:**
  Separate popups for auto-blocked and manually blocked IPs.
- **Firewall Integration:**
  Adds/removes Windows Firewall rules for blocked/unblocked IPs.
- **Security Event Logging:**
  Logs block/unblock events with timestamp, IP, MAC, vendor, and reason.
- **Report Viewer:**
  View a report of all block/unblock events.
- **Alert Mode Toggle:**
  Switch between Telegram and PLC alert modes.

How It Works

1. Configuration

- **Allowed Prefix:**
  Example: 192.168.1.
- **Allowed Range Start/End:**
  Example: 1 to 245
- **Always Allowed IPs:**
  List of IPs always allowed, regardless of range.

Configuration is saved to ip_monitor_config.json.

---

2. Block Lists

- **blocked_ips.json:**
  Tracks all currently blocked IPs (auto and manual).

- **manual_blocked_ips.json:**
  Tracks IPs manually blocked by the user (never auto-unblocked).

---

3. Blocking Logic

- **Manual Block:**
  When you manually block an IP, it is added to
  both blocked_ips.json and manual_blocked_ips.json, and firewall rules are created.
- **Auto Block:**
  IPs detected by the main script that are not allowed are auto-blocked and added
  to blocked_ips.json.

---

4. Unblocking Logic

- **Manual Unblock:**
  Only possible via the "Manually Blocked IPs" popup. Removes IP from both block lists and
  deletes firewall rules.
- **Auto Unblock:**
  When the allowed range or always-allowed IPs are changed, auto-blocked IPs that are now
  allowed are unblocked (unless they are manually blocked).

---

5. Popups

- **Show Auto Blocked IPs:**
  Displays only auto-blocked IPs (no unblock button).
- **Show Manual Blocked IPs:**
  Displays only manually blocked IPs (with unblock button).

---

6. Security Event Logging

- **log_security_event:**
  Logs every block/unblock event to security_events.json with timestamp, event type, IP, MAC,
  vendor, and reason.

---

7. Report Viewer

- **Show Report:**
  Displays all security events in a table, color-coded for block/unblock.

---

8. Alert Mode

- **Toggle Alert Mode:**
  Switch between "Online" (Telegram) and "Offline" (PLC) alerting.
  Saves the mode to config.

Key Functions

- **load_config / save_config:**
  Load and save configuration from/to JSON.
- **load_blocked_ips / save_blocked_ips:**
  Load and save auto-blocked IPs.
- **load_manual_blocked_ips / save_manual_blocked_ips:**
  Load and save manually blocked IPs.
- **add_blocked_ip_simple:**
  Manually block an IP (adds to both lists and firewall).
- **unblock_selected:**
  Manually unblock selected IPs (removes from both lists and firewall).
- **unblock_newly_allowed_ips:**
  Auto-unblock IPs that become allowed (skips manual blocks).
- **cleanup_orphaned_block_rules:**
  Removes firewall rules for IPs that are now allowed (skips manual blocks).
- **show_blocked_ips_window / show_auto_blocked_ips_window / show_manual_blocked_ips_window:**
  Popups for viewing blocked IPs.
- **log_security_event:**
  Log block/unblock events.
- **show_report:**
  View all security events.

Typical Workflow

1. **Configure allowed range and always-allowed IPs.**
2. **Manually block/unblock IPs as needed.**
3. **View auto-blocked and manually blocked IPs in separate popups.**
4. **Change configuration as needed; auto-blocked IPs are unblocked if they become allowed, manual blocks are persistent.**
5. **View security event report for audit trail.**
6. **Toggle alert mode between Telegram and PLC.**

Important Notes

- **Manual blocks are persistent:**
  IPs in manual_blocked_ips.json will NOT be auto-unblocked, even if they become allowed by config.
- **Auto blocks are dynamic:**
  IPs blocked automatically will be unblocked if they become allowed.
- **Firewall rules:**
  All block/unblock actions add/remove Windows Firewall rules.
- **Run as administrator:**
  Required for firewall rule changes.

- **All JSON files are stored in the script directory.**