Signal Lynx

Signal Shield Product Guide

This guide is evergreen and applies to all modern releases of the Signal Shield application. It will be updated periodically to reflect major feature additions and changes in functionality.

Applicable To: WindowsInstallations (64-bit)

Document Updated: December 24, 2025

Overview

Welcome to the official Product Guide for Signal Shield, the one-click hardening and setup utility that turns any Windows PC into a secure, always-on webhook receiver for your automated trading pipeline. It installs and configures a hardened reverse proxy, strict firewall rules, and background services so your trading bot (e.g., Lynx-Relay) can safely receive alerts over HTTPS and process them locally — with your API keys never leaving your machine.

Signal Shield is the essential first step in deploying the Signal Lynx trading suite. It handles the complex server configuration so you don't have to, creating a fortified foundation upon which Lynx-Relay can operate with maximum security and reliability.

The Workflow: Your 3-Step Deployment

Understanding the roles of Signal Shield and Lynx-Relay is crucial for success. Your entire automated trading deployment follows this simple, secure path:

1. **Fortify Your Rig** — Run the Signal Shield installer to harden and prime your PC for automation. This guide covers this step in detail.
2. **Arm the Relay** — Launch Lynx-Relay and load your encrypted exchange API keys into its local Vault.
3. **Go Weapons-Hot** — Point your TradingView alerts to your secure webhook URL and watch your signals become live trades, executed automatically.

Table of Contents

---

1. Introduction to Signal Shield

1.1. Our Philosophy: Your Edge, Your Keys

We built our tools on a simple principle: **your strategy and your credentials should live on your hardware.** You've heard "Not Your Keys, Not Your Coins." We believe the same applies to your trading automation. Signal Shield helps you keep it that way by securing the single most important entry point where trading signals reach your machine.

1.2. What Signal Shield Does: Your One-Button Bodyguard

Signal Shield is a secure, GUI-driven installer that turns a standard Windows PC into a hardened, 24/7 webhook receiver in minutes. It is your personal bodyguard for automated trading, handling the complex and error-prone server configuration required for a professional-grade setup. It automates the installation of a reverse proxy, generates SSL certificates for encryption, writes strict firewall rules, and provisions background services so your trading executor can run with minimal babysitting.

1.3. About This Guide & The New Workflow

This guide is the single source of truth for installing, activating, and operating Signal Shield. It assumes you will later run **Lynx-Relay** (or a similar local executor) on the same PC to convert the verified alerts into live exchange orders.

With the introduction of the Inno Setup installer, deploying Signal Shield is easier than ever. You will download a single .exe file that walks you through the entire process, from license activation to final system verification.

2. Key Features at a Glance

- **One-Click Hardening:** Automated setup of a reverse proxy (NGINX), TLS encryption, background services, and system health checks. Get your PC trade-ready in minutes, no IT degree required.
- **VIP-Only Access:** The inbound webhook endpoint is locked behind a strict IP allowlist and rate-limiter. By default, only localhost and curated, official TradingView IP addresses are accepted, shielding your PC from unwanted access.
- **Always-On Services:** Background services are installed and configured to start automatically on boot, ensuring your webhook path stays available across reboots. Because the market never sleeps.
- **Local-Only Secrets:** No API keys are ever uploaded or handled by Signal Shield. Its sole purpose is to prepare the PC for local execution tools like Lynx-Relay, which keep your keys on your disk, under your control.
- **Friendly GUI:** A native Windows setup experience with a clear, step-by-step process, progress logs, EULA flow, and error reporting.
- **Fast Rollback & Repair:** Includes a built-in uninstaller for clean removal and a "Repair" function to easily restore the correct configuration if needed.

3. System Requirements

- **OS:** Windows 10 (64-bit), Windows 11 (64-bit), or Windows Server 2016/2019/2022 (64-bit).
- **Permissions: Local Administrator** rights are required to install services, configure firewall rules, and manage SSL certificates. The installer will prompt for elevation.
- **Network:** A stable, always-on broadband connection.
- **Disk:** Approximately 500 MB of free disk space for tools, logs, and certificates.

4. Before You Begin (Pre-Install Checklist)

For a smooth installation, please verify the following:

1. **You have Administrator rights** on the target PC. The installer must be run as an administrator.
2. **Port 443 is not already in use.** This port is standard for HTTPS and is required by Signal Shield. If you have other web server software (like IIS, Apache, XAMPP) running, you must stop and disable that service first.
3. You intend to run your trading executor (e.g., **Lynx-Relay**) on the same machine.
4. (Optional but Recommended) Add an exclusion in your antivirus software for the installation directory (C:\SignalLynx\ and C:\nginx\) to prevent interference with service installations.

5. Installation — One-Click Setup & Final Configuration

Signal Shield is distributed via a dedicated installer that simplifies the entire process.

1. **Run the Signal Shield Installer (.exe).**
    - Download the installer from your Signal Lynx account page.
    - Double-click the .exe file. You will be prompted by Windows User Account Control (UAC) to allow the application to make changes; this is required.
2. **Accept the EULA.**
    - You will be prompted to read and accept the End User License Agreement (EULA). You must scroll to the bottom and agree to proceed.
3. **Activate Your License.**
    - The main application window will appear. In the "License Key" field, enter the key provided to you after purchase. Your key can be found on your Signal Lynx account page: www.signallynx.com/account/downloads.
    - Click **"Activate"**. The application will verify your license with our servers. Upon success, the status will change to **"Active"** in green.
4. **Run the Setup.**
    - Once activated, the **"Run Setup"** button will be enabled. Click it to begin.
    - Signal Shield will now go to work, automatically performing all configuration steps. You can monitor the progress in real-time on the "Status" tab and see detailed logs in the "Detailed Log" tab.
    - **Note:** This process may take several minutes, as Signal Shield may need to download and install required dependencies. Please be patient.
5. **Finish & Verify Software Installation.**
    - Upon completion, Signal Shield performs a final health check. If all steps are successful, you will see a confirmation message. The software portion of the setup is now complete.

6 . CRITICAL FINAL STEP: Configure Your Network (Port Forwarding)

IMPORTANT: This is the most common reason webhooks fail to arrive.
Signal Shield has successfully configured **your computer**, but it **cannot** configure your internet router or your Virtual Private Server (VPS) provider's firewall.
For external signals from TradingView to reach your computer, you must ensure that incoming traffic on **TCP Port 443** is allowed and forwarded to this machine's local IP address.

Action Required: Configure Your Network

*These instructions are also available in the **"Router Help"** tab of the Signal Shield application.*

If you are running on a home/office network:

- **Step 1: Log In to Your Router**
  - Identify your Default Gateway IP; This can be found by running the following prompt in “Windows Command Prompt (Windows Button -> Command Prompt) and entering

    ipconfig

    Locate the line that says "Default Gateway" (common examples: 192.168.0.1, 192.168.1.1, or 10.0.0.1).

    Copy/paste that Default Gateway IP into your web browser address bar and hit enter. This will bring you to your router's administration panel.

  - Log into your router, using the router Admin password
  - NOTE: This is not the same as your WIFI-Password. It is usually located on your router (unless you changed it during router set up)
- **Step 2: Create a Port Forwarding Rule**
  - Find the "Port Forwarding," "Virtual Server," or "NAT" section in your router's settings.
  - Create a new rule with the following settings:
    - **External/Internal Port:** 443
    - **Protocol:** TCP
    a. **Device IP / Forward to IP**: Enter the IP provided to you on the Router Help Tab of Signal Shield (this is your LAN/private IP).
    b. If you wish to independently verify, you may use the "IPv4 Address" shown by ipconfig.

IMPORTANT: This "Device IP / Forward to IP" value is a LAN/private IP (ex: 192.168.x.x). It is ONLY used inside your router for port forwarding. Do NOT paste a 192.168.x.x LAN IP into TradingView. TradingView must send to a public HTTPS URL/IP.

6. **If you are running on a VPS (e.g., AWS, Vultr, DigitalOcean):**
    - There is no “router port forwarding” on a VPS. You must allow inbound traffic using the provider firewall / security group.
    - Log in to your VPS provider's control panel.
    - Navigate to the "Networking", "Security Group", or "Firewall" section for your server instance.
    - Allow inbound TCP traffic on port 443 (ideally restricted to TradingView IPs + your admin IP, if your setup supports it).
    - Also ensure the VPS operating system firewall allows inbound TCP 443.
7. **RESTART THE COMPUTER**
    - ***Ensure you have restarted your computer post Signal Shield Install/Configuration.***
    - Some of the installed services require initialization on boot up

6. What Signal Shield Installs & Configures

Signal Shield performs a series of automated actions to create a secure and stable environment. Here is exactly what it does:

6.1. Reverse Proxy (NGINX)

- Installs and configures **NGINX**, a professional-grade web server, to act as a reverse proxy.
- Listens for incoming HTTPS traffic on **TCP port 443**.
- Securely forwards validated webhook requests to your local trading app, which runs on http://127.0.0.1:5000.
- Exposes a /ping endpoint for quick, easy health checks.
- Enforces per-IP request throttling (rate limiting) to prevent denial-of-service attacks.

6.2. TLS Certificates for Encryption

- Installs **OpenSSL** if not already present on the system.
- Generates a local, self-signed SSL certificate and private key to enable encrypted HTTPS traffic between TradingView and your PC.

6.3. Windows Firewall Rules

- Creates a specific inbound rule in the Windows Defender Firewall named "Signal Shield - Webhook Firewall Rule".

- This rule applies a **default allowlist**, permitting traffic on port 443 *only* from known TradingView IP addresses and your local machine.
- All other external traffic attempting to reach this port is automatically denied at the firewall level.

6.4. Always-On Background Services (NSSM & Redis)

- Installs **NSSM (the Non-Sucking Service Manager)** to register NGINX as a proper Windows service. This ensures it starts automatically on boot and runs reliably in the background.
- Installs **Memurai (a Redis-compatible datastore)** as a Windows service. This provides a high-performance local database used by advanced applications like Lynx-Relay for state management.

6.5. System Integrity Checks

- Installs the **Microsoft VC++ Redistributable** if it is missing, a common dependency for many of the tools used.
- Verifies that all components are correctly configured and services are running before reporting success.

7. How It Works (The Data Flow)

The data flow is designed for maximum security, ensuring your sensitive API keys never leave your machine.

1. **Incoming HTTPS Request:** A TradingView alert fires, sending a request to your public IP address on port 443.
2. **Network Firewall (Router/VPS):** Your network hardware or VPS firewall must be configured to allow and forward this traffic to your PC. **This is the step you configure manually.**
3. **Signal Shield Interception:** Signal Shield's NGINX service receives the request. It first checks if the source IP is on the allowlist (i.e., is it from TradingView?). If not, the request is dropped.
4. **Internal Forwarding:** If the request is valid, NGINX forwards it internally to http://127.0.0.1:5000/webhook, where Lynx-Relay is listening.
5. **Local Execution:** Lynx-Relay processes the webhook and executes the trade using your locally stored, encrypted API keys.

You can verify end-to-end reachability at any time by visiting https://<your-host-ip-or-domain>/ping. A successful response will show "ok".

8. First-Time Activation & Licensing

Signal Shield is a licensed product. During the first launch, you will be required to enter your license key to activate the software and enable the setup functionality. This key is validated against the Signal Lynx License Manager. Once activated, the key is securely cached on your local machine.

The license key is available in your account's arsenal and download page of the website (https://www.signallynx.com/account/downloads)

9. Daily Operations & Maintenance

Once installed, Signal Shield is designed to be "set and forget."

- **Automatic Startup:** All configured services (NGINX, Memurai) will start automatically when your computer boots up.
- **No Manual Intervention:** You do not need to manually start or stop any services during normal operation. The system is designed to run 24/7.

10. Repair, Uninstall, & Rollback

- **Repair:** If you encounter configuration issues after installation (e.g., you accidentally deleted a file), you can run the Signal Shield application again and click the **"Repair"** button. This will re-run the entire setup process, overwriting existing configurations with the correct defaults.
- **Uninstall (Full):** To completely remove Signal Shield, use the provided uninstaller entry in Windows "Apps & Features". This will stop and remove the services, delete the firewall rule, and remove all related configuration files and certificates.

11. Troubleshooting

11.1. Your First Step: Always Check the Logs

Before trying anything else, your first diagnostic step should always be to check the **"Detailed Log"** tab in the Signal Shield GUI. This tab is your most valuable tool for troubleshooting. It gives you the raw intelligence needed to understand the root cause of a problem.

- **Look for Simplified Messages:** For many common issues, Signal Shield translates complex technical errors into user-friendly explanations. Look for these first.
- **Use the Full Context:** For more complex issues, the log provides raw technical messages and full context for any errors.
- **Check the Timestamps:** All log entries are timestamped, helping you pinpoint exactly when an issue occurred.
- **Help Us Help You: The "Send Error Report" Button**
  If you see an unexpected error in this tab, we kindly ask for your help. Please click the **"Send Error Report"** button. This action anonymously sends the technical error details directly to our development team. **No sensitive data is ever included.** This report

simply gives us the context we need to understand the problem, identify bugs, and release improvements.

11.2. Common Problems & Solutions

- **Symptom:** Portion of install failed
    - **Fix:** Restart computer, re-run installer. Ensure you restart your computer post install
    - Sometimes other programs will lock out the SignalShield Installer - Windows Update will do this routinely, even if it is running in the background. Its recommended to restart your computer and then re-run the Signal Shield Software. A full Install will not damage any successfully configured system or parameters(s).
- **Symptom:** TradingView alerts never reach Lynx-Relay/ TradingView alerts will fire, but nothing shows up on the Lynx-Relay Notification window or in telegram
    - **Fix 1: *Ensure you have restarted your computer post Signal Shield Install/Configuration. You may rerun the Signal Shield Software post restart.***
        - Some of the installed services require initialization on boot up
    - **Fix 2: Port Forwarding not enabled on Router.**
        - This is the **most common issue** after a fresh install. It is almost always caused by a network configuration problem outside of Signal Shield's control. Please carefully review and complete the steps in **Section 5, Step 6: Configure Your Network (Port Forwarding)**.
    - **Fix 3: LAN IP vs Public IP vs Routing (Most Common Confusion)**
        - There are TWO different IPs involved:
            - 1) LAN / Private IP (used for router port forwarding):
                - This is the IP shown in the Router Help tab (ex: 192.168.0.167)
                - This is the IP your router forwards traffic TO; You can confirm it via Command Prompt (Windows button -> command prompt):

                  ipconfig

                  (use the “IPv4 Address” line)

            - 2) Public / “Base” IP (what the internet sees):
                - This is the IP returned by the powershell command (Windows button -> powershell)

                  Invoke-RestMethod "https://api.ipify.org"

    - TradingView webhook URL MUST be a public HTTPS URL (not 192.168.x.x).However, using the Public IP only works if inbound routing is actually possible:
        - Home/office router: you must port-forward external 443 -> LAN IP shown in Router Help.
        - Shared networks / CGNAT / shared apartment Wi-Fi: port forwarding often cannot be configured (or won't route to your device). In this case a tunnel URL (Cloudflare Tunnel / ngrok) or host the receiver on a VPS.
- **Symptom:** The NGINX service fails to start, or the installation fails with a "port conflict" error.
    - **Fix 1:** ***Ensure you have restarted your computer post Signal Shield Install/Configuration. You may rerun the Signal Shield Software post restart.***
    - **Fix 2:** This almost always means another application is using **port 443**. Open a Command Prompt as Administrator and run

        ```
        netstat -ano -p TCP | find ":443"
        ```

        This will show you the Process ID (PID) of the application using the port. Use Task Manager to identify and stop that application (common culprits are IIS, Apache, Skype, or other web servers). Then, click "Repair" in Signal Shield or rerun the installer in full (re-running will not negatively impact the system). Ensure to restart your computer after completing Signal Shield.

- **Symptom:** The health check (https://<your-host>/ping) does not return "ok" or times out.
    - **Fix:**
        - First, confirm you have completed the network configuration in **Section 5, Step 6**.
        - Ensure the nginx and Memurai services are running in the Windows Services app (services.msc).
        - Ensure your Lynx-Relay application is running and listening on port 5000.

11.3. Contacting Support

If you have worked through this guide and the logs but are still facing persistent issues, we are here to help. When reaching out, providing detailed information will allow us to resolve your issue much faster.

- **Support Channels:**
    1. **Primary:** www.signallynx.com/contact_us
    2. **Community:** Reach out on our official **Telegram** (https://t.me/SignalLynx) or **X/Twitter** (@SignalLynx) pages.

- **Information to Provide:**
    1. Your **Signal Lynx License Key**.
    2. A **detailed description** of the problem, including when it started and what you were doing at the time.
    3. Any steps you have already taken to try and resolve it.
    4. **If you are having Signal Shield Install issue - Screenshots** of the Signal Shield window, especially the **"Status"** tab and the **"Detailed Log"** tab.
    5. Relevant copy-pasted excerpts from the **Detailed Log** that correspond to the time the issue occurred. If you used the "Send Error Report" button, please let us know.
    6. Copy of your setup_gui_runtime.log, from your Signal Shield folder.

12. Security Notes & Best Practices

- **Administrator Account Security:** Since Signal Shield runs with administrator privileges, ensure your Windows user account has a strong, unique password.
- **Keep Windows Updated:** Regularly install Windows security updates to protect the underlying operating system.
- **Physical Security:** Your trading machine's security is your responsibility. Ensure it is in a physically secure location.

  SIGNAL LYNX ADMINS AND SUPPORT WILL NEVER ASK FOR YOUR EXCHANGE API KEYS OR PASSWORDS/PASSPHRASES. FURTHERMORE - YOU SHOULD NEVER PROVIDE THESE TO ANYONE.

13. Legal, Risks, and Disclaimers

This section provides a summary of key risks, disclaimers, and terms associated with the use of Lynx-Relay and Signal Shield. It is not a replacement for our full legal agreements. By installing, accessing, or using the Signal Lynx software, you acknowledge that you have read, understood, and agree to be bound by our full, legally binding terms.

13.1. Governing Documents

Our complete legal framework can be found online at www.signallynx.com/legal. Your use of the software is governed by these documents in their entirety:

- Terms of Service (TOS/EULA)
- Privacy Policy
- Billing & Refunds Policy
- DMCA Policy

13.2. Key Disclaimers and Acknowledgment of Risk

The Signal Shield software and all related services are provided "AS IS" and "AS AVAILABLE," without warranty of any kind, express or implied. We expressly disclaim all warranties, including but not limited to merchantability and fitness for a particular purpose. There is no guarantee of service, uptime, or uninterrupted availability.

Automated trading is a high-risk activity. While Signal Shield and Lynx-Relay are robust tools, they cannot eliminate the inherent risks of trading cryptocurrencies. You acknowledge and agree that:

- Trading is highly speculative and involves a significant risk of **partial or total loss of funds.**
- Market conditions can change rapidly, and unforeseen technical issues can occur at any time. This includes, but is not limited to: internet outages, exchange API failures or downtime, power interruptions, operating system errors, software bugs, and **user configuration errors.**
- **Signal Lynx is not responsible for any financial outcomes.** We are not liable for missed trades, "bots gone wild," losses due to market conditions, or any damages arising from your use of or inability to use the software.

Signal Lynx is a technology company. We provide software tools for execution assistance only. We are not a broker-dealer, investment adviser, or financial institution. **No content, documentation, or communication from Signal Lynx constitutes financial, legal, or tax advice.** You are solely responsible for your trading strategies, decisions, risk controls, and outcomes.

Signal Shield and Lynx-Relay are self-hosted products, which means you are responsible for the security of the environment where they run. This includes OS hardening, firewall configuration (beyond what Signal Shield provides for external access), anti-malware, access controls, and proper credential hygiene for your computer and exchange accounts.

13.3. A Note on Responsible Trading

Automated trading can be intense and demanding. We strongly encourage all users to practice responsible trading habits.

- **Never trade with money you cannot afford to lose.**
- Understand the risks of every strategy you deploy.
- Maintain emotional discipline and avoid compulsive decision-making.

If you feel that your trading is becoming compulsive or negatively impacting your life, we strongly encourage you to seek help from professional resources dedicated to trading psychology and gambling addiction support.

---

14. Appendix A — Manual Configuration (Fallback)

In the rare instances where the Signal Shield installer fails to configure your computer, you can perform the steps manually using the instructions below.

14.1. Configure Windows Firewall Inbound Rule (Port 443)

1. **Open Windows Defender Firewall:** Go to Control Panel > System and Security > Windows Defender Firewall.
2. **Advanced Settings:** On the left side, click “Advanced settings.”
3. **Inbound Rules:** Right-click on Inbound Rules, then select New Rule...
4. **Rule Type:** Select Port, then click Next.
5. **Protocol and Ports:** Choose TCP and for "Specific local ports," type 443. Click Next.
6. **Action:** Select Allow the connection and click Next.
7. **Profile:** Check the boxes for Domain, Private, and Public. For a VPS, **Public** is recommended. Click Next.
8. **Name:** Enter a rule name, e.g., “NGINX HTTPS” and click Finish.
9. **Whitelist TradingView IPs:**
    - Find the rule you just created, right-click it, and select Properties.
    - Go to the **"Scope"** tab. Under "Remote IP address," select "These IP addresses" and click "Add...".
    - Add the following official TradingView IP addresses:
        - 52.89.214.238
        - 34.212.75.30
        - 54.218.53.128
        - 52.32.178.7

14.2. Configure NGINX

14.2.1. Install NGINX for Windows

1. Download the latest Mainline version of NGINX for Windows from nginx.org.
2. Extract the ZIP file to C:\nginx\. Your file structure should look like this:
    - C:\nginx\nginx.exe
    - C:\nginx\conf\nginx.conf

14.2.2. Generate SSL Certificates

1. **Install OpenSSL:** Visit https://slproweb.com/products/Win32OpenSSL.html and download the latest "Light" Win64 OpenSSL installer. Run the installer with default settings.
2. **Generate Certificate:**
    - Open a Command Prompt as Administrator and navigate to the OpenSSL bin folder (e.g., cd "C:\Program Files\OpenSSL-Win64\bin").

Run the command:

openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout selfsigned.key -out selfsigned.crt

- For "Common Name": use localhost
    i. If you will access this receiver via a domain name, use that domain as the Common Name and set nginx server_name to match.
- Create a new folder: C:\nginx\certs\.
- Copy the generated selfsigned.key and selfsigned.crt files into C:\nginx\certs\.

14.3. Recommended nginx.conf File Contents

Below is the entire sample configuration file with TradingView IP whitelisting. Copy and paste this content into C:\nginx\conf\nginx.conf, replacing the existing content.

```
 worker_processes  auto;
error_log  logs/error.log warn;
pid        logs/nginx.pid;

events {
   worker_connections  1024;
}

http {
   include       mime.types;
   default_type  application/octet-stream;

   log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                     '$status $body_bytes_sent "$http_referer" '
                     '"$http_user_agent" "$http_x_forwarded_for"';

   access_log  logs/access.log  main;

   sendfile        on;
   tcp_nopush      on;
   keepalive_timeout  65;

   # --- Rate limit zone ---
   # 10 requests/sec per client IP, keep state in a 1MB shared zone.
   limit_req_zone $binary_remote_addr zone=webhook:1m rate=10r/s;

   server {
      listen       443 ssl;
      server_name  localhost;
```

```
ssl_certificate      C:/nginx/certs/selfsigned.crt;
ssl_certificate_key  C:/nginx/certs/selfsigned.key;

add_header X-Content-Type-Options "nosniff" always;
add_header X-Frame-Options "DENY" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;

root   "C:/nginx/html";
client_max_body_size 1m;

location /ping {
   return 200 "ok\n";
}

location /webhook {
   # Allow traffic from localhost and official TradingView IPs
   allow 127.0.0.1;
   allow ::1;
   allow 52.89.214.238;
   allow 34.212.75.30;
   allow 54.218.53.128;
   allow 52.32.178.7;
   # Deny all other traffic
   deny  all;

   # Apply the rate limit zone defined above
   limit_req zone=webhook burst=20 nodelay;

   proxy_pass http://127.0.0.1:5000;
   proxy_http_version 1.1;
   proxy_set_header Host              $host;
   proxy_set_header X-Real-IP         $remote_addr;
   proxy_set_header X-Forwarded-For   $proxy_add_x_forwarded_for;
   proxy_set_header X-Forwarded-Proto $scheme;

   proxy_read_timeout  15s;
   proxy_send_timeout  15s;
}

error_page  403 /403.html;
location = /403.html {
   internal;
}
```

```
        error_page   500 502 503 504  /50x.html;
        location = /50x.html {
            internal;
        }
    }
}
```

14.4. Start NGINX

1. Open a Command Prompt and navigate to C:\nginx.
2. Run the command: nginx.exe
3. If it starts without errors, NGINX is now listening on port 443. To make it a permanent service, you would need to use a tool like NSSM, which is what the automated installer handles.

---

15. Appendix B — Files, Paths, & Services

- **Install Roots (defaults):**
    - Reverse proxy: C:\nginx
    - Tools: C:\nssm, OpenSSL in C:\Program Files\OpenSSL-Win64\bin (or fallback)
- **TLS Artifacts:**
    - Certs folder: C:\nginx\certs
    - Default files: selfsigned.crt, selfsigned.key
- **Reverse Proxy Config Highlights:**
    - Rate limit zone: 10 r/s per client IP; burst with no delay at the /webhook location.
    - Security headers and client_max_body_size set.
    - Locations: /ping → 200 ok, /webhook → proxy to http://127.0.0.1:5000.
- **Default Allowlist:** 127.0.0.1, ::1, plus curated TradingView IPs.
- **Local Data & State:** %LOCALAPPDATA%\SignalLynx\
    - License key cache, EULA acceptance state, and dismissed app-messages.
- **Logs:**
    - Reverse proxy: C:\nginx\logs\access.log, C:\nginx\logs\error.log
    - Setup/runtime: %LOCALAPPDATA%\SignalLynx\setup_gui_runtime.log