



Cyber Unified Defense Platform

Getting Started Guide

From installation to your first completed scan — about 10-15 minutes

Version 5.47.9

Updated August 30, 2026

DADavisDesigns: Cyber Defenders

Welcome

This guide walks a new administrator through setting up Cyber Unified Defense Platform end to end: installing the server, logging in for the first time, deploying an agent to your first endpoint, confirming the dashboard is receiving live data, and running your first network scan. Expect the whole process to take roughly 10-15 minutes on a typical Windows Server or workstation.

Built and tested extensively in our own lab environment, but every network is different — your feedback during this trial directly shapes fixes and improvements. Something feel off? Let us know.

Before you begin

You will need: a Windows machine to host the server (Windows 10/11 or Windows Server), dual-core 2 GHz+ CPU (quad-core recommended for 5+ monitored endpoints), 4GB+ RAM (8GB+ recommended), 25GB+ free disk space (grows with endpoint count and retention settings), administrator rights on that machine, and network access to the endpoints you plan to monitor. No manual dependency installation is required — the installer provisions everything it needs silently.

Step 1 — Install the Server

Run the Cyber Unified Defense Platform Server installer (LANGuardianPro_Server_Setup.exe) on the machine that will host the platform. This is typically a dedicated server or always-on workstation on your network, since agents and the dashboard both depend on it being reachable.

1. Right-click the installer and choose “Run as administrator.”
2. Accept the license agreement and choose your install location (the default is recommended).
3. The installer silently provisions all required dependencies — Python runtime, packet-capture driver, and supporting services — with no additional prompts.
4. When the installer finishes, the Cyber Unified Defense Platform server and its watchdog process start automatically and are configured to launch on system boot.
5. Open a browser on the same machine (or any device on your network) and navigate to the server’s address, e.g. `http://<server-ip>:5000`.
6. A system tray icon also starts automatically and may prompt for a Registration ID the first time it runs. Enter 00710 to complete tray registration.

Tip

Note the server’s IP address during installation — you will need it again when deploying agents to other endpoints.

Manual Start (If the Server Doesn’t Start Automatically)

If the dashboard doesn’t come up after installation or a restart, the server can be started manually. Open PowerShell as Administrator and run:

```
& "C:\Python312\python.exe" "C:\LAN Guardian Pro\Server\app.py"
```

This runs the server directly and keeps the window open so any startup error is visible — double-clicking `app.py` directly will not show errors, since the window closes immediately if it crashes.

Step 2 — First Login

The dashboard loads to a login screen on first access.

1. Log in with the default credentials: username admin, password admin.
2. You will be required to set a new password immediately — the default credentials cannot be used going forward.
3. Review and accept the End User License Agreement (EULA) to proceed.
4. A 30-day trial license is generated from within the platform itself — go to Settings → License → Manage License, enter your business name under Generate Trial Key for Customer, click Generate Trial Key, then copy the generated key into the License Key field above and click Activate.
5. You will be prompted to set up multi-factor authentication (TOTP) for your admin account. Use an authenticator app (Google Authenticator, Microsoft Authenticator, Authy, etc.) to scan the QR code and complete setup.

Security note

MFA is strongly recommended for every administrator account, not just the default admin — additional accounts can be created under Settings → Users.

Step 3 — Deploy Your First Agent

Cyber Unified Defense Platform monitors endpoints through a lightweight agent. The fastest way to install one is with a one-command install link, generated from the dashboard.

1. From the dashboard, go to Settings → License, open License Management, and use Generate Distributable Install Link.
2. Choose the target platform (Windows or Linux) and generate an install link. Each link is single-use and tied to a token, so it is safe to send directly to the target machine.
3. On the target endpoint, run the generated one-line command:

Windows (PowerShell, run as administrator):

```
iwr <install-link> | iex
```

Linux (bash — sudo required):

```
curl -fsSL <install-link> | sudo bash
```

Linux Is Fully Supported

The one-command install works identically on Linux — the curl | sudo bash link above installs, registers, and begins reporting the same way the Windows command does, no separate Linux-specific setup required. The leading sudo is required — the installer checks for root and exits immediately with an error if run without it. The agent is installed and runs as root, which is necessary for system-level enforcement actions such as DNS Sinkholing (writing to /etc/hosts).

4. The agent installs silently, registers itself with the server, and begins reporting within about a minute.
5. For environments where a one-line install isn't practical (locked-down endpoints, imaging pipelines), a pre-configured package (agent script, one-click installer, and Task Scheduler autostart registration) is available for Windows endpoints from Endpoint Agents → Deploy Agent, where the server URL and

install folder can be set before downloading. This option is Windows-only; Linux endpoints should use the one-command install link above.

Step 4 — Verify the Dashboard

Once your first agent checks in, confirm the platform is receiving live data:

- Devices count in the top banner should increase to reflect the new endpoint.
- The endpoint should appear under Devices with a green/active status and a recent “last seen” timestamp.
- The Security Score should recalculate (a fresh install typically starts at 100/A with no findings yet).
- Under EDR Console, you should begin seeing process and internet-activity telemetry from the new endpoint within a few minutes.

If nothing appears after 5 minutes

Confirm the endpoint can reach the server’s IP and port over your network (no firewall blocking), and that the install command completed without errors. See the Troubleshooting section of the Administrator Guide for agent check-in issues.

Step 5 — Run Your First Scan

1. Go to Network → Scheduled Scan and click Run Now (or wait for the automatic scan, which runs on a regular interval by default).
2. The scan discovers devices via ARP/ping sweep across every subnet the server has a network interface on — including a segmented IoT or guest VLAN, if the server has been given a network connection into it — and lists new ones under New Device Alerts.
3. Review each discovered device and either Approve known/trusted devices or flag unrecognized ones for investigation.
4. Once your device inventory is approved, DNS Monitoring, Traffic Monitoring, and DHCP Monitoring all begin baselining normal activity automatically.

Step 6 — Keeping Agents Updated

New agent builds are distributed from the Endpoint Agents page rather than reinstalled by hand on every endpoint.

1. Go to Endpoint Agents and locate the Agent Update Package panel.
2. Click Choose File and select the agent package downloaded from the Cyber Unified Defense Platform website, then click Import & Stage.
3. Once staged, online agents pick up the new version automatically on their next check-in — no separate action required. Use Push Update to All if you want to prompt every agent to check immediately rather than wait.
4. Each endpoint card shows its active version and whether it is current, so you can confirm the rollout completed without checking machines individually.

That's it — your platform is installed, your first endpoint is reporting, and your network baseline is underway. From here, the Administrator Guide covers every module in depth, along with best practices and common workflows for day-to-day use.