

Deployment Quick-Start

This guide walks through a standard WireTrace deployment from initial server installation to first assets appearing on the dashboard. The entire process - server, sensor, and verification - takes under 15 minutes with no internet dependency.



Total deployment time: under 15 minutes. Server: ~10 min | Sensor: ~60 sec | First asset: ~30 sec after sensor connects.

PREREQUISITES

Server Host

- Ubuntu 22.04 or 24.04 LTS (physical or VM)
- Minimum: 4 vCPU, 16 GB RAM, 200 GB SSD
- SSH access with sudo privileges
- Network connectivity to sensor host(s)

Sensor Host

- Ubuntu 22.04 or 24.04 LTS (physical or VM)
- Minimum: 4 vCPU, 8 GB RAM, 40 GB disk
- Capture NIC connected to SPAN/TAP port
- Management NIC with connectivity to server

STEP 1 - INSTALL THE WIRETRACE SERVER

1a Transfer the Installer

Copy the WireTrace self-extracting installer to the server host. The installer is a single .run file (~1.3 GB) that contains all components, container images, and configuration.

```
scp wiretrace-server-v1.3.3.run tracer@<SERVER_IP>:/tmp/
```

1b Run the Installer

Execute the installer with root privileges. It will extract all components, load container images, configure the environment, and start all services. No internet required.

```
chmod +x /tmp/wiretrace-server-v1.3.3.run
sudo /tmp/wiretrace-server-v1.3.3.run
```

The installer prompts for: installation directory (default: /opt/wiretrace), server IP address, and deployment mode (clean install or upgrade). All defaults are safe to accept.

1c Verify Server is Running

Once installation completes, open the WireTrace UI in a browser. Log in with the default admin credentials provided by the installer.

```
https://<SERVER_IP>
```

All services should show healthy in the system status. The dashboard will be empty until a sensor is connected.

STEP 2 - DEPLOY A SENSOR

2a Generate an Activation Token

In the WireTrace UI, navigate to **Settings → Sensors → Add Sensor**. Enter a name for the sensor and generate an activation token. Copy the token - it is used once during sensor enrollment.

2b Install the Sensor

Transfer the sensor package to the sensor host and run the setup script. Provide the server IP and activation token when prompted.

```
sudo ./setup-sensor.sh
```

The sensor installs, enrolls with the server using the activation token, and begins capturing traffic from the configured SPAN/TAP interface immediately.

STEP 3 - VERIFY FIRST ASSETS

3a Check the Dashboard

Within 30 seconds of the sensor connecting to a SPAN port with active traffic, devices will begin appearing in the WireTrace dashboard. Each device is classified with vendor, model, OS, and protocol details as traffic is observed.

3b Validate Classifications

Navigate to **Asset Inventory** and verify that discovered devices match expected network assets. Check that vendor, device type, and protocol assignments are accurate. Classification confidence improves over time as more traffic patterns are observed.

3c Review Security Insights

Navigate to **Security Insights** to review automated findings: cleartext credentials, TLS certificate issues, exposed management interfaces, and protocol-level observations. Findings are generated continuously as traffic is analyzed.

STEP 4 - ONGOING OPERATIONS

4a Add More Sensors

Repeat Step 2 for each additional network segment. Each sensor requires its own activation token. Sensors can be added at any time without restarting the server or disrupting existing monitoring.

4b Configure Alerting

Set up email alerts, syslog forwarding, or webhook notifications for security findings, behavioral deviations, and threat detections. Navigate to **Settings → Integrations** to configure output channels.

TROUBLESHOOTING

No Assets Appearing

- Verify the SPAN port is mirroring active traffic
- Confirm the sensor capture NIC is in promiscuous mode
- Check sensor logs for connection errors to server
- Verify network path between sensor and server

Sensor Not Connecting

- Verify the activation token was entered correctly
- Check firewall rules between sensor and server
- Confirm the server IP is reachable from sensor host
- Review sensor logs for authentication errors

WHAT HAPPENS NEXT

Over the first 24-48 hours, WireTrace builds behavioral baselines for every discovered device. Classification accuracy improves as more protocol patterns are observed. Security insights, compliance evidence, and threat detections become richer as the platform accumulates traffic history. No additional configuration required - the platform learns continuously from observed traffic.

Deployed in Minutes. Value from Day One.

