Flintnet User Guide

Version: 1.0.0-beta
Audience: Network Administrators

Table of Contents

---

1. Getting Started

What Flintnet Does

Flintnet monitors your network in real time. Once deployed, it:

- Discovers devices on your subnet automatically
- Polls SNMP-enabled devices for interface utilisation and system information
- Captures network traffic and tracks flows between devices
- Detects suspicious ARP activity — rogue devices, ARP spoofing, duplicate IPs
- Detects traffic anomalies using statistical analysis
- Sends email alerts when something needs your attention

What You Need

- A Linux server or VM on the same network segment as the devices you want to monitor
- Docker and Docker Compose installed on that server
- SNMPv2c enabled on your managed switches and routers (community string `public` by default)

- A modern browser — Chrome or Edge recommended

First-Time Setup

1. Copy the `docker-compose.yml` and `.env.example` files to your server
2. Rename `.env.example` to `.env`
3. Open `.env` and set `FLINTNET_CIDR` to your subnet (e.g. `192.168.1.0/24`)
4. Set `FLINTNET_SNMP_COMMUNITY` to match your devices' SNMP community string
5. Run `docker compose up -d`
6. Open `http://<your-server-ip>` in your browser

---

2. Logging In

When you open Flintnet for the first time you will see the login screen.

Agent URL — enter the address of the Flintnet agent, including the port. If the UI and agent are on the same server this will be `http://<your-server-ip>:3000`.

API Token — if you set `FLINTNET_API_TOKEN` in your `.env` file, enter it here. If you left it blank, leave this field empty.

Click **Connect**. If the connection succeeds you will go directly to the Dashboard.

Your session is saved in the browser. The next time you open Flintnet you will go straight to the Dashboard without needing to log in again.

To log out, click **Logout** at the bottom of the left sidebar. This clears your saved session and returns you to the login screen.

---

3. Dashboard

The Dashboard gives you an at-a-glance view of current network activity.

What You Will See

Traffic Stats — total packets and bytes captured since the agent started.

Active Flows — a live table of network flows. Each row shows the source IP and port, destination IP and port, protocol (TCP or UDP), packet count, and byte count. The table updates in real time.

Anomalies — a list of flows where traffic has deviated significantly from the baseline. See Anomalies for more detail.

Real-Time Updates

The Dashboard updates automatically without needing a page refresh. Data is pushed from the agent via a persistent connection. If the connection drops (for example, if the agent restarts) the UI will reconnect automatically within a few seconds.

---

4. Devices

The Devices screen shows every device Flintnet has discovered on your monitored subnet.

Device Cards

Each device is shown as a card containing:

- **IP address** — the device's IP
- **SNMP badge** — green `SNMP` if the device responded to SNMP, grey `No SNMP` if it did not
- **Device type** — router, switch, server, firewall, printer, or unknown
- **Description** — the SNMP `sysDescr` value if available
- **Interface utilisation bars** — live in/out bandwidth utilisation per interface, colour coded:
  - 🟢 Green — below 50%
  - 🟡 Amber — 50% to 80%
  - 🔴 Red — above 80%

Clicking a Device

Click any device card to open the Device Detail screen for that device.

Discovery

Flintnet discovers devices by scanning the subnet defined in `FLINTNET_CIDR`. Discovery runs automatically on startup and periodically thereafter. New devices appear on the Devices screen as they are found.

If a device does not appear, check that:

- It is within the monitored subnet
- It is reachable from the Flintnet server
- SNMPv2c is enabled if you expect it to show SNMP data

---

5. Device Detail

The Device Detail screen opens when you click a device card. It shows everything Flintnet knows about a specific device.

Device Info

- IP address, device type, SNMP reachability status
- System description (`sysDescr`) and system object ID from SNMP

Interface Utilisation

Live in/out bandwidth utilisation bars for each interface on the device. These update in real time via the same SSE connection as the Devices screen.

ARP Entries

The ARP section shows the MAC address history for the device — each MAC address that has been associated with this IP, along with:

- **Manufacturer** — derived from the MAC address OUI
- **First seen** — when this MAC was first observed
- **Last seen** — the most recent time this MAC was seen
- **IP history** — previous IP addresses this MAC has used, with timestamps

Multiple ARP entries for one device can indicate MAC address changes over time, which may be normal (device replacement) or suspicious (MAC spoofing).

Security Alerts

The Security Alerts section shows the most recent security events associated with this device — up to 20 entries. Each alert shows the event type and the relevant details (IPs, MACs, timestamps).

Alert types you may see:

Alert Type	What It Means
`rogue_device`	A device was seen for the first time — not previously known
`arp_spoof_detected`	A MAC address is claiming multiple IPs, or an IP has changed MAC unexpectedly
`duplicate_ips`	Two devices are both claiming the same IP address

---

6. Security Alerts

The Security screen shows a live feed of all security events detected across your network.

Alert Types

Rogue Device — Flintnet has seen a MAC address it has not encountered before. This could be a new legitimate device or an unauthorised device connecting to your network. Review the manufacturer and IP to determine if it is expected.

ARP Spoof Detected — A device is either claiming multiple IP addresses from a single MAC (possible ARP cache poisoning) or an IP address has suddenly started using a different MAC address (possible MAC spoofing or ARP spoofing attack). Investigate immediately.

Duplicate IP — Two devices are both claiming the same IP address. This is typically a misconfiguration (static IP conflict) but can also indicate an attack. Check which devices are involved and resolve the conflict.

Email Notifications

If SMTP alerting is configured, Flintnet will send an email for each of the above event types. A 5-minute cooldown per device prevents your inbox from being flooded if an event fires repeatedly. See Configuring SMTP Email Alerts.

---

7. Anomalies

The Anomalies screen shows network flows where traffic volume has deviated significantly from the established baseline.

Flintnet uses a statistical method (EWMA — Exponentially Weighted Moving Average) to build a baseline for each flow. When a flow's byte count deviates significantly from its baseline, it is flagged as an anomaly.

What to Look For

An anomaly does not necessarily mean something is wrong. Legitimate causes include:

- A large file transfer or backup job
- A software update being pushed to devices
- Increased usage during business hours

Suspicious causes include:

- Data exfiltration — an internal device sending large volumes of data to an external IP
- A compromised device communicating with a command-and-control server

- A lateral movement attack spreading through your network

Use the source and destination IPs, port numbers, and protocol to determine whether the flow is expected.

---

8. Network Topology

The Topology screen displays a live diagram of your network, showing how devices are connected to each other.

Connections are discovered using LLDP (Link Layer Discovery Protocol) and CDP (Cisco Discovery Protocol) data polled from your managed switches and routers. Devices that do not support LLDP/CDP will not appear as connected nodes.

Reading the Diagram

- Each node represents a device, labelled with its IP address
- Lines between nodes represent physical or logical connections discovered via LLDP/CDP
- Node position is calculated automatically — you can scroll and zoom to navigate

If Devices Are Missing

If a device does not appear in the topology:

- Confirm LLDP or CDP is enabled on the device
- Confirm the device is SNMP-reachable (check the Devices screen)
- Some devices (end-user workstations, printers) do not support LLDP and will not appear

---

9. Configuring SMTP Email Alerts

Flintnet can send email notifications when security events or traffic anomalies are detected.

Setup

Open your `.env` file and fill in the SMTP settings:

```
FLINTNET_SMTP_HOST=smtp.yourprovider.com
FLINTNET_SMTP_PORT=587
FLINTNET_SMTP_USER=alerts@yourdomain.com
FLINTNET_SMTP_PASSWORD=yourpassword
FLINTNET_ALERT_EMAIL=admin@yourdomain.com
```

Restart the agent after making changes:

```
docker compose restart flintnet-agent
```

What Triggers an Email

Event	Trigger
Rogue device	Unknown MAC address seen for the first time
ARP spoof detected	MAC claiming multiple IPs, or IP changing MAC
Duplicate IP	Two MACs claiming the same IP
Traffic anomaly	Flow traffic significantly above baseline

Cooldown

To prevent email flooding, Flintnet will not send more than one email per device per event type within a 5-minute window. If the same event fires repeatedly within that window, only the first email is sent.

Supported SMTP Providers

Flintnet uses STARTTLS for SMTP delivery and works with any standard SMTP relay including:

- Office 365 / Microsoft 365
- Gmail (requires App Password if 2FA is enabled)
- SendGrid
- Amazon SES
- Your own on-premises mail relay

---

10. Troubleshooting

No devices appearing on the Devices screen

- Check that `FLINTNET_CIDR` is set correctly in your `.env` file
- Confirm the Flintnet server is on the same Layer 2 network segment as the devices
- Check the agent logs: `docker compose logs flintnet-agent`

SNMP badge shows "No SNMP" for all devices

- Confirm SNMPv2c is enabled on your devices
- Check that `FLINTNET_SNMP_COMMUNITY` matches the community string configured on your devices
- Confirm there is no firewall blocking UDP port 161 between the Flintnet server and your devices

No interface utilisation bars on device cards

- Interface utilisation requires SNMP to be reachable on the device
- Allow up to 60 seconds after discovery for the first utilisation reading to appear

Not receiving email alerts

- Confirm all `FLINTNET_SMTP_*` variables are set in your `.env` file
- Check the agent logs for SMTP errors: `docker compose logs flintnet-agent`
- Verify your SMTP credentials by testing them with another mail client
- Check your spam folder

The UI shows a connection error

- Confirm the agent is running: `docker compose ps`
- Confirm the Agent URL on the login screen matches the server IP and port 3000 — if it is showing an old or incorrect address, clear the field and re-enter the correct URL before clicking Connect
- Check that port 3000 is not blocked by a firewall on the server

Getting More Help

Visit https://flintnet.io/support to submit a support request.