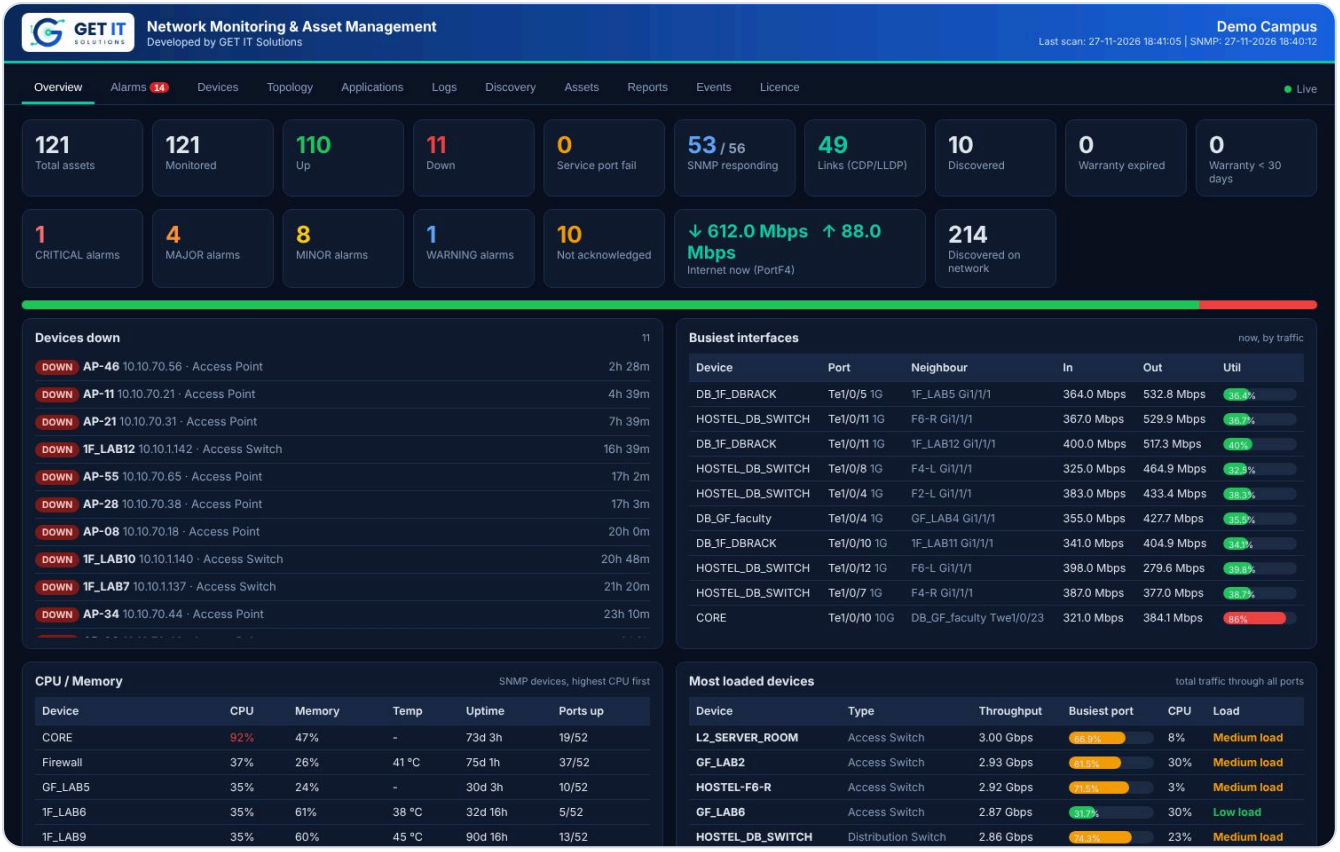
GET IT SOLUTIONS

GET IT NMS

Network Monitoring & Asset Management – User Manual



Version 3.3 · Windows · © Get IT Solutions, Lucknow · www.getitsolutions.in

Contents

1. What GET IT NMS does
2. System requirements
3. Installation
4. Activation, trial and licence
5. First login and security
6. Adding devices
7. Enabling SNMP, LLDP and syslog on your devices
8. The dashboard, tab by tab
9. Alerts by e-mail and Telegram
10. Updates
11. NMS Control – start, stop, restart
12. Backup and moving to a new PC
13. Troubleshooting
14. Support

1. What GET IT NMS does

GET IT NMS watches every device on your network from one web dashboard:

- **Monitoring** – ping every 60 seconds, plus CPU, memory, temperature, uptime and every port (status, speed, traffic, errors) through SNMP.
- **Topology** – a live network map drawn automatically from CDP / LLDP.
- **Alarms** – Critical / Major / Minor / Warning alarms with root-cause suppression, acknowledge, snooze and escalation.
- **Bandwidth & applications** – internet usage, top applications, users and websites from firewall syslog and NetFlow.
- **Assets** – model, serial, firmware and MAC collected automatically, plus purchase, warranty, licence and AMC dates with expiry alerts.
- **Discovery** – finds switches, APs, CCTV, printers, PCs and UPS on your subnets.

Everything runs on one Windows PC inside your network. No cloud service is used for monitoring data.

2. System requirements

Item	Requirement
Operating system	Windows 10 / 11 Pro, or Windows Server 2016 / 2019 / 2022 (64-bit)
Hardware	4 GB RAM and 10 GB free disk for up to 300 devices; 8 GB RAM for 500+ devices. The PC should run 24×7.

Software	Windows PowerShell 5.1 (built into Windows). Nothing else to install – no SQL, no Java.
Network	Fixed IP address. Reach to devices on ICMP (ping) and UDP 161 (SNMP). Devices send syslog to UDP 514 and NetFlow to UDP 2055 on this PC. Dashboard on TCP 8080.
Internet	Only for online activation, the 30-day licence check and updates (HTTPS to getitsolutions.in). Air-gapped sites use offline keys.

3. Installation

1. Download **GETIT-NMS-Setup.zip** from **www.getitsolutions.in/nms** and extract it (right-click → Extract All). Keep all files of the folder together.
2. Double-click **Setup.bat**. Windows asks for administrator permission – click **Yes**.
3. The wizard runs a **System check** (Windows version, PowerShell, free ports 8080 / 514 / 2055, disk, internet). Fix any red item and press **Check again**.
4. **Activation** – choose online code, offline key or free trial (see chapter 4).
5. **Install folder** – default `C:\GETIT-NMS`.
6. **Organisation** – your site name, logo and support contact shown on the dashboard.
7. **Network** – the wizard detects this PC's IP. Enter the SNMP community you will use on your devices (example `MyNmsRO`) and the subnets for discovery.
8. **Devices** – start with an empty list, import a CSV, or let discovery find devices.
9. **Admin password** – set the dashboard login password.
10. Press **Install**. Setup copies the files, opens the Windows firewall ports, creates the service **GETIT NMS Service** (starts with Windows, restarts itself if stopped) and opens the dashboard.

> Upgrading? Run the new Setup.bat on the same PC. Your settings, devices and licence are kept – choose "Upgrade: keep the licence already installed".

> If Windows Defender or another antivirus blocks the setup, make sure the files came from getitsolutions.in and contact Get IT Solutions support – do not switch your antivirus off.

4. Activation, trial and licence

Open the **Licence** tab (or the Activation page in Setup). The Machine ID of the PC is shown there.

Option	When to use	How
Free trial	Try the full product for 30 days (up to 50 devices). One trial per computer.	Enter organisation, e-mail and 10-digit phone → **Start trial**. Internet needed.
Online activation code	Normal licence. Code looks like `XXXX-XXXX-XXXX-XXXX-XXXX`.	Paste the code → **Activate online**. One code works on one computer. NMS re-checks every 30 days automatically.
Offline licence key	Air-gapped networks without internet.	Send your Machine ID to Get IT Solutions, paste the key you receive (`GETIT-…`) → **Install key**.

Licence states

State	Meaning
ACTIVE / TRIAL	Everything works.

NOT ACTIVATED	New install – 7 days to activate, then the dashboard becomes read-only.
DEACTIVATED	Offline site: the re-activation period (normally 180 days) is over. Send **Machine ID + Request code** from the Licence tab to Get IT Solutions and install the re-activation key. Online site: the PC could not reach the licence server for 30 days – connect to the internet and press **Check with GET IT server now**.
GRACE	Licence end date passed – 30 days to renew. Everything still works.
EXPIRED / BLOCKED	Read-only: monitoring and the dashboard keep running, but settings, devices and updates can't be changed.

Moving to a new PC? Ask Get IT Solutions to **transfer** the licence, then activate the same code on the new PC.

5. First login and security

1. Open **http://<NMS-PC-IP>:8080** in any browser (example `http://10.10.50.4:8080`).
2. Log in as **admin** with the password set in Setup.

Run **Security-Setup.ps1** from the install folder (right-click → Run with PowerShell) to:

- change the admin password (stored as a salted hash),
- add **viewer** users who can only look,
- allow the dashboard only from your IT subnets (IP allow-list),
- lock the install folder so only administrators can open it.

After 5 wrong passwords a login source is locked for 15 minutes.

> Do not publish port 8080 on the internet. For remote access use VPN, or restrict the firewall rule to fixed source IPs.

6. Adding devices

One by one

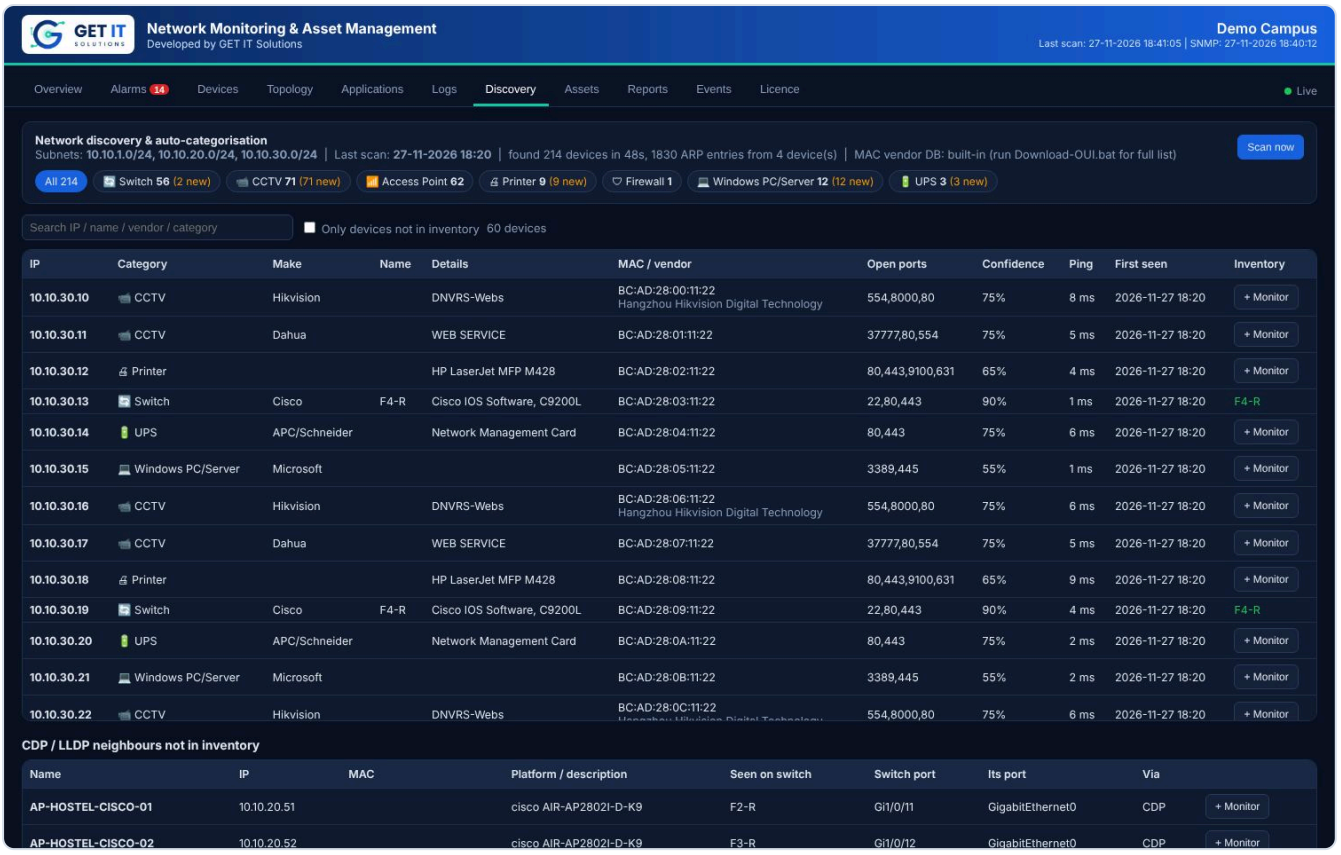
Devices or **Assets** tab → **+ Add device**. Enter name, IP and type. Optional: location, vendor, model, serial, purchase date, warranty start / end, supplier, invoice, licence end date and AMC. Leave SNMP on “auto” – NMS tries your community and switches SNMP on when the device answers.

Many at once

Use **NMS Control → Edit devices** to open `devices.csv` in Excel. One row per device; columns include Name, IP, Type, Location, Monitor, SNMP, ConnectedTo, UplinkPort and the asset fields. Save and press **Restart**.

From discovery

Discovery tab → **Scan now**. Found devices are grouped by category (switch, CCTV, AP, printer, PC, UPS). Click **+ Monitor** to add one.



Discovery – devices found on the network, with category, make and open ports

Editing many assets

In **Assets**, tick the devices (for example 60 access points bought together) and press **Edit selected** to fill purchase date, warranty and supplier once for all of them.

7. Enabling SNMP, LLDP and syslog on your devices

Use SNMP v2c **read-only** with your own community name, and allow only the NMS PC. Never use “public” or “private”. In the examples the NMS PC is `10.10.50.4` and the community is `MyNmsRO` – replace both with your values (the community must match the one set in Setup).

Cisco IOS / IOS-XE (Catalyst)

```
conf t
 ip access-list standard NMS-SNMP
  permit host 10.10.50.4
 exit
 snmp-server community MyNmsRO RO NMS-SNMP
 snmp-server ifindex persist
 snmp-server location Building-A Floor-1 Rack-2
 cdp run
 lldp run
 logging host 10.10.50.4
 logging trap informational
end
write memory
```

Cisco CBS / SG small business switches

```
snmp-server server
snmp-server community MyNmsRO ro 10.10.50.4 view Default
lldp run
logging host 10.10.50.4
```

Cisco WLC (AireOS)

```
config snmp community create MyNmsRO
config snmp community accessmode ro MyNmsRO
config snmp community ipaddr 10.10.50.4 255.255.255.255 MyNmsRO
config snmp community mode enable MyNmsRO
```

Sophos Firewall

Administration → SNMP: enable SNMP agent, add community `MyNmsRO` with v2c and the NMS PC as manager. Device access: allow SNMP on the LAN zone. System services → Log settings: add a syslog server `10.10.50.4` UDP 514, format **Device standard format (legacy)**, and tick the logs you need (firewall, web filter, application, events).

Fortinet FortiGate

```
config system snmp community
 edit 1
  set name MyNmsRO
  config hosts
   edit 1
    set ip 10.10.50.4 255.255.255.255
   next
  end
 next
end
config log syslogd setting
 set status enable
 set server 10.10.50.4
end
```

Other devices

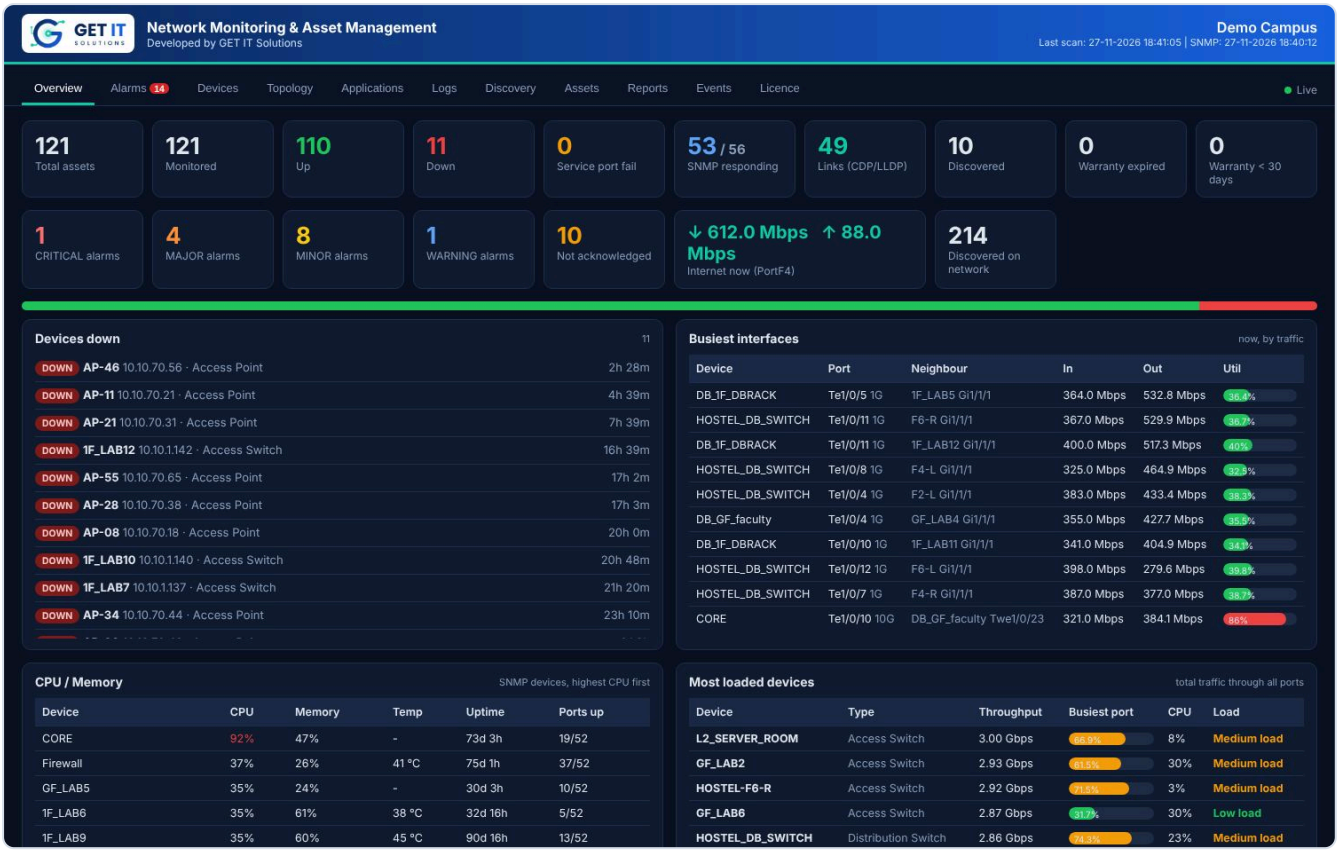
HPE Aruba, Juniper, MikroTik, Ruckus, D-Link, TP-Link, Windows / Linux servers, printers and UPS cards: enable SNMP v2c read-only with the same community and allow the NMS PC. Switch on LLDP so the topology map can draw the links.

> NetFlow / sFlow: point the exporter on your firewall or core switch to `10.10.50.4` UDP 2055 to get per-application and per-user traffic.

8. The dashboard, tab by tab

Overview

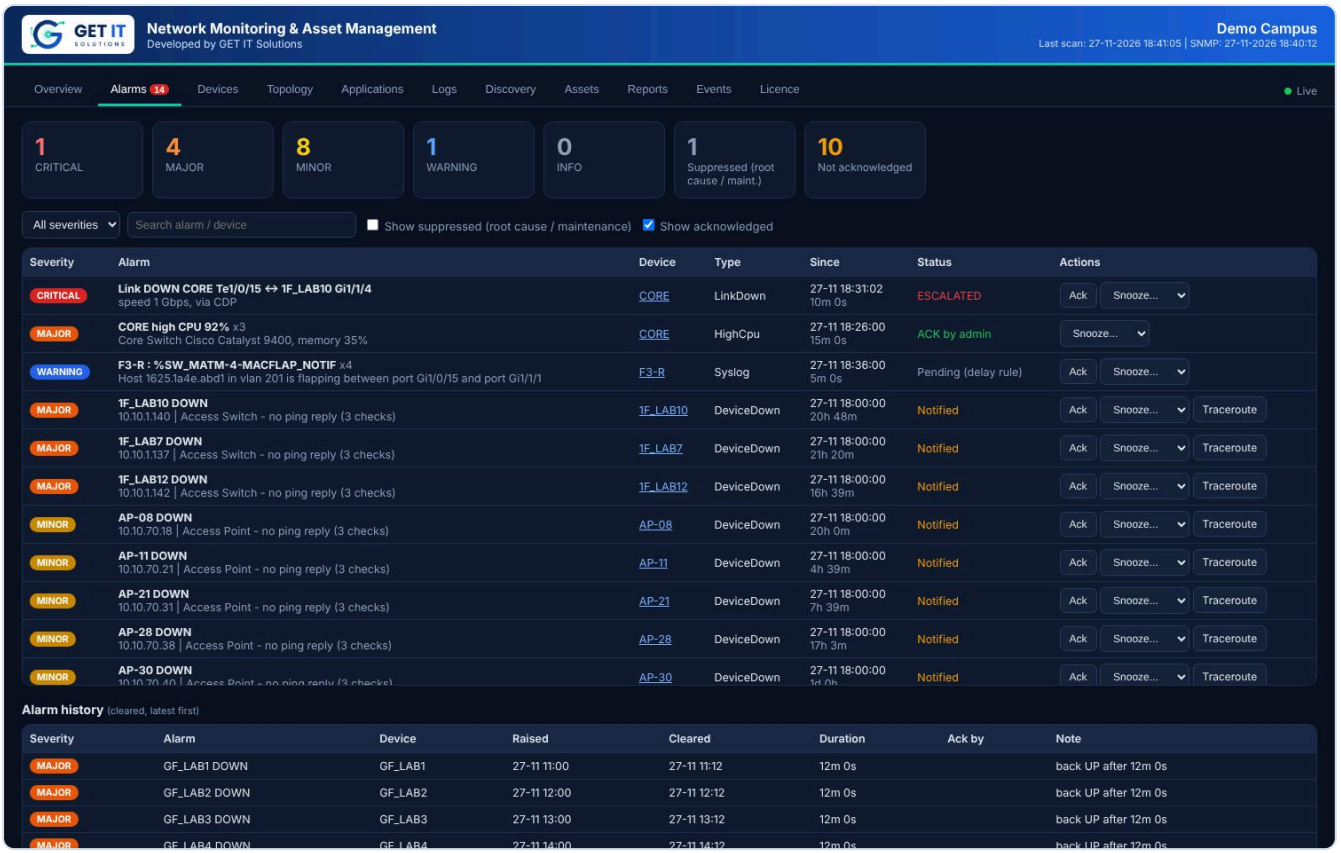
Totals (assets, up, down, SNMP responding, links), alarms by severity, live internet bandwidth, devices down, busiest interfaces, CPU / memory / temperature and most loaded devices. The page refreshes by itself.



Overview

Alarms

Every open alarm with severity, device, type and time. **Ack** marks it as seen, **Snooze** silences it for a time, **Traceroute** checks the path to a down device. Child devices behind a failed uplink are suppressed automatically (root cause). Cleared alarms move to **Alarm history**.



Alarms

Devices

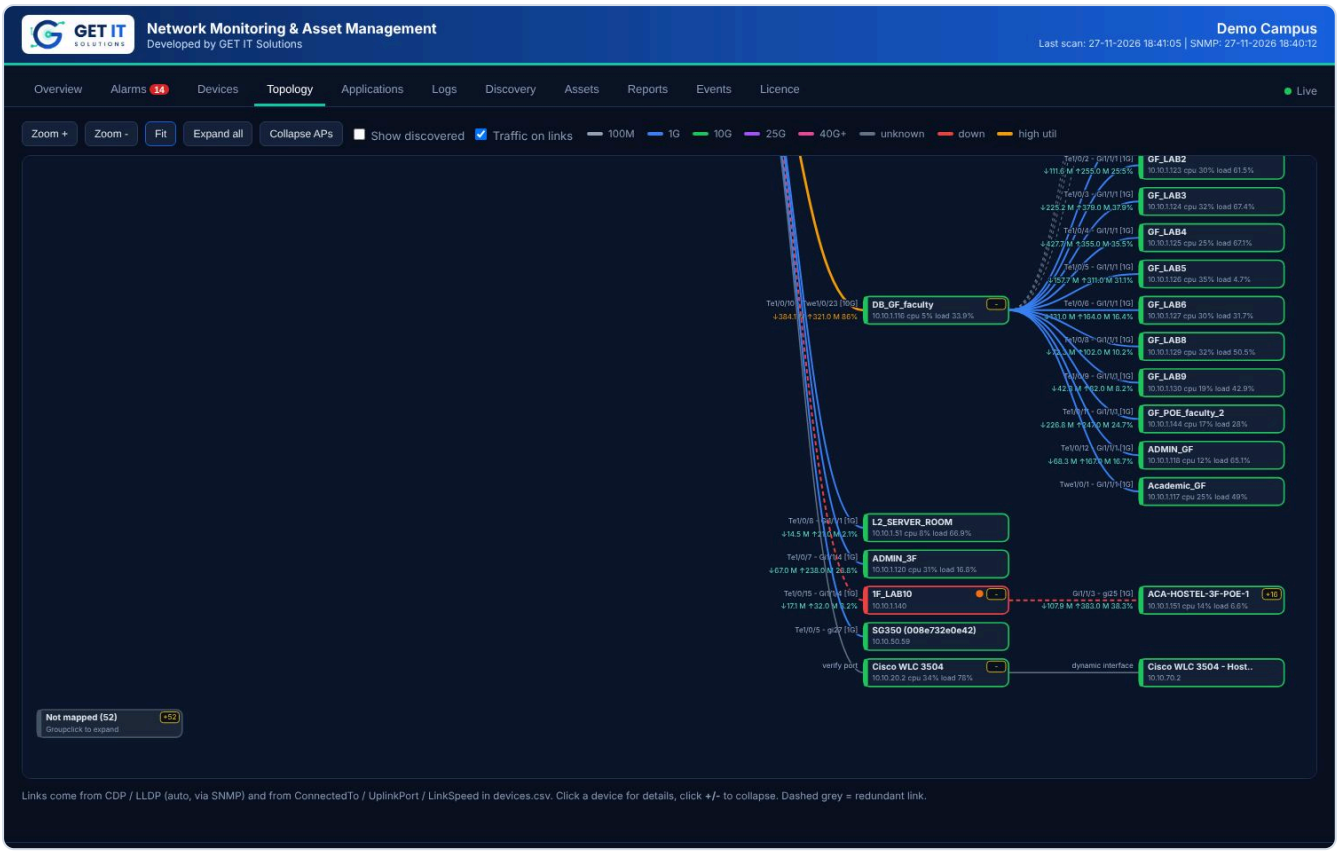
Searchable list with status, IP, type, location, response time, CPU and memory. Click a device for details: system information, every port with speed and traffic, traffic and ping graphs (1 h / 6 h / 24 h / 7 days), neighbours and active alarms. **Edit device / asset details** changes its information.



Device details

Topology

Map from CDP / LLDP and from the ConnectedTo / UplinkPort columns. Colours show link speed (1G blue, 10G green, 25G violet, 40G+ pink); red dashed = link down, orange = high utilisation. Use **Fit**, **Zoom**, **Collapse APs** and click +/– on a node to fold its branch.



Topology

Applications

Internet bandwidth, download / upload totals, peak usage, top applications, top users and top websites from firewall logs or NetFlow, for 1 h, 6 h, 24 h or 7 days.



Applications

Logs

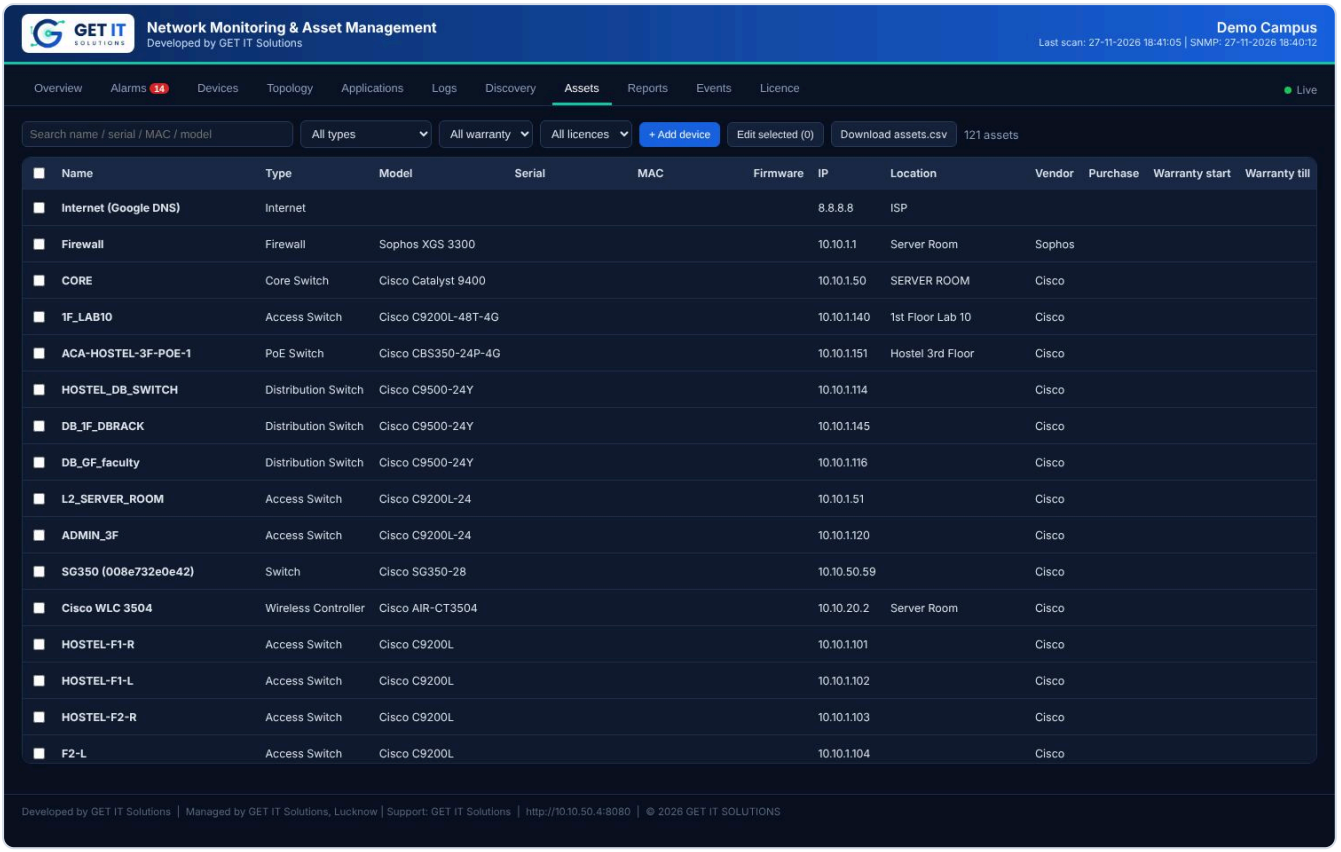
Central syslog from switches, firewall and controllers, searchable by device, severity and text. Important messages (link down, MAC flap, config change, high temperature) also raise alarms.

Discovery

See chapter 6.

Assets

Complete inventory: name, type, model, serial, MAC, firmware, IP, location, vendor, purchase date, warranty start / end, supplier, invoice, licence and AMC. Filters show warranty or licence **expired** or **ending in 30 days**. **Download assets.csv** exports the register for audits.



Assets

Reports

Availability per device, downtime, alarm counts and top problem devices for a chosen period – printable and exportable.

Events

Time-line of everything NMS did: device up / down, SNMP polls, discovery runs, licence checks and updates.

Licence

Licence status, Machine ID, request code, online activation, offline key and updates (see chapters 4 and 10).

9. Alerts by e-mail and Telegram

Open **NMS Control → Edit settings** (config.json) and fill one or both sections, then press **Restart**:

```
"Email": { "Enabled": true, "SmtpServer": "smtp.yourmail.com", "Port": 587,
           "Username": "nms@yourdomain.com", "Password": "app-password",
           "From": "nms@yourdomain.com", "To": "it-team@yourdomain.com" },
"Telegram": { "Enabled": true, "BotToken": "123456:ABC...", "ChatId": "-100123456" }
```

Under **Alerting** you can choose which severities are sent, delay rules (for example alert only if down for 3 minutes) and escalation. A daily summary report can be e-mailed every morning (**DailyReport**).

10. Updates

- **Online**: when Get IT Solutions publishes an update, the Licence tab shows **Update available**. Press **Install update**.
- **Offline**: copy the update file (`NMS-Patch-x.y.z.zip`) to the PC, Licence tab → **Choose file** → **Install patch file**.

Only updates signed by Get IT Solutions are accepted. NMS backs up the old files first, installs the update and restarts itself within about one minute. **Rollback** restores the previous version. Your settings, devices, history and licence are never touched by an update.

11. NMS Control – start, stop, restart

Open **NMS Control** from the desktop or Start menu (or `NMS-Control.ps1` in the install folder).

Button	What it does
Start / Stop / Restart	Controls the GETIT NMS Service. Restart after changing settings or devices.
Open dashboard	Opens the web dashboard.
Open logs	Opens the logs folder (useful for support).
Edit settings / Edit devices	Opens config.json / devices.csv.
Refresh status	Shows whether the service and port 8080 are running.

> The service has a watchdog: if NMS stops, Windows starts it again within 1–5 minutes. To replace files manually, press Stop, copy the files and press Start straight away.

12. Backup and moving to a new PC

Copy these files from the install folder regularly (or let your backup software do it): `config.json`, `devices.csv`, `inventory.json`, `users.json` and the `history` folder. To move: install NMS on the new PC, stop it, copy the files back, ask Get IT Solutions to transfer the licence, start NMS and activate.

13. Troubleshooting

Problem	What to check
Dashboard does not open	NMS Control → Refresh status. If “not responding”, press Restart and wait 40 seconds. Check that no other program uses port 8080 and that the Windows firewall rule “GETIT NMS” exists. From another PC, also check the network path to TCP 8080.
“This script contains malicious content” / antivirus block	Use only files from getitsolutions.in and contact support with a screenshot of the antivirus alert. Do not switch off the antivirus.
Device shows DOWN but works	The device may block ping (ICMP). Allow ping from the NMS PC, or set Monitor = No and use a service port check.
No CPU / ports for a device (“no SNMP”)	Community name must match exactly; the device ACL must allow the NMS PC; UDP 161 must be open in any firewall between them. Test from the NMS PC: `snmpwalk` or the Device details page after 5 minutes.
Topology links missing	Enable CDP / LLDP on switches (`lldp run` on Cisco). Links appear after the next SNMP poll (5 minutes).
No firewall applications / users	Syslog must be sent to UDP 514 of the NMS PC in the format given in chapter 7, and the Windows firewall must allow UDP 514.
Licence: “server not reachable”	The PC needs HTTPS access to getitsolutions.in. Allow it in your firewall / proxy, then press **Check with GET IT server now**.
Licence: “already used on another computer”	One code works on one PC. Ask Get IT Solutions to transfer it.

14. Support

Get IT Solutions, Lucknow – Sophos Partner, GeM registered seller.
Website: **www.getitsolutions.in** · Product page: **www.getitsolutions.in/nms**
E-mail: **info@getitsolutions.in** · 24/7 support: **+91 82990 87647**

We install NMS, configure SNMP / syslog on your switches and firewall, train your team and provide yearly licences and AMC.