



ENGINEERING PRODUCTS
FOR MODERN OPERATIONS

User Guide

Monitor • Manage • Troubleshoot
with Confidence

-  Complete Visibility
-  Simpler Operations
-  Faster Troubleshooting
-  Greater Control



How to use this guide

This guide is organized around the way an operator actually works: get access, discover devices, monitor health, investigate alarms, understand topology, report findings, and then administer the platform. The chapter structure follows the supplied NMS User Guide mind map, while the procedures are grounded in the current **ArkayNMS** operating documentation.

GUIDE CONVENTION Blue callouts contain operational notes. Orange numbered steps are action sequences. Screenshots show the product UI as represented in the supplied ArkayNMS walkthrough.



How data moves through ArkayNMS

- SNMP polling and ICMP provide reachability and device health signals.
- Traps, syslog and flow telemetry are sent from network devices to the NMS.
- Configuration backup uses SSH/Telnet when enabled.
- The collected data feeds Inventory, Alarms, Topology, Grafana and reports.

Chapter	Focus
1. Introduction	What ArkayNMS is, what it monitors, and how the platform fits together.
2. Getting Started	Access, login, license, roles and first-time setup.
3. NMS Dashboard	Fleet health, sites, devices and recent alarms.
4. Device Management	Sites, device types, MIBs, discovery, inventory and device workspace.
5. Network Monitoring	SNMP, ICMP, traps, flows, syslog, parameters and RouteInsight.
6. Alerts & Alarms	Severities, active/history views, acknowledgement and notifications.
7. Events	Event sources, trap logs, histories and event-to-alarm context.
8. Network Topology	Automatic, semi-automatic and manual maps, links, paths and exports.
9. Reports	Parameter exports, inventory reporting and Grafana views.
10. Search & Filtering	How to locate devices, events, alarms and time windows quickly.
11. Troubleshooting	Common failure patterns and a practical investigation flow.
12. Administration	Users, permissions, settings, licensing and configuration backup administration.
13. Best Practices	Operational habits that keep monitoring useful and maintainable.
14. FAQ	Common questions and quick answers.
15. Glossary	Plain-language definitions of the main NMS terms.
16. Support	How to report issues and what information to provide.

Guide roadmap

Use the supplied mind map as the high-level navigation model for this manual. Each branch below is expanded into a complete working chapter.



ArkayNMS User Guide information architecture supplied with the project.

• 01 Introduction

Understand ArkayNMS before you start operating it.

What is ArkayNMS?

ArkayNMS is an on-premise, agentless network monitoring and management platform for multi-vendor enterprise networks. The platform combines device discovery, SNMP monitoring, reachability checks, traps, flow telemetry, syslog, alarms, topology, configuration backup, dashboards and analytics in one operating workflow.

What ArkayNMS monitors

Signal / capability	Purpose
SNMP polling	Collect device parameters such as CPU, memory, interface counters, uptime and vendor-specific health data.
ICMP reachability	Measure reachability, packet loss, RTT and basic availability.
SNMP traps	Receive asynchronous device events and turn them into searchable trap history and alarms.
NetFlow / IPFIX / sFlow	Collect flow records and analyze traffic patterns, top talkers and protocols.
Syslog	Ingest device logs and use severity, source and pattern rules for analysis and alerting.
Network topology	Represent L2/L3 device relationships and links for dependency and outage analysis.
Configuration backup	Capture running/startup configuration, compare snapshots and detect drift.
Grafana analytics	Provide deeper time-series views for alarms, syslog, NetFlow, availability and vendor dashboards.

Who should use this guide?

- Network operators who monitor devices, investigate alarms and review dashboards.
- Network administrators who onboard devices, configure monitoring, notifications, users and settings.
- Support and engineering teams who need repeatable troubleshooting workflows.

AGENTLESS MODEL : Nothing needs to be installed on routers or switches. Devices are polled via SNMP; traps, syslog and flow records are forwarded to the ArkayNMS server.

Platform at a Glance

- **ArkayNMS** is a centralized **Network Monitoring & Management** platform that collects network telemetry and provides visibility into the infrastructure.
- **SNMP Polling**
 - a) ArkayNMS polls network devices using **SNMP**.
 - b) Communication from NMS to devices uses **UDP port 161**.
 - c) Used to collect device health, performance, interface, and other monitoring data.
- **ICMP Reachability**
 - a) ArkayNMS uses **ICMP** to check whether devices are reachable.
 - b) Helps identify devices that are **up, down, or unreachable**.
- **Configuration Backup**
 - a) ArkayNMS can retrieve and back up device configurations.
 - b) Uses **SSH (TCP 22)** or **Telnet (TCP 23)** for device access.
- **SNMP Traps**
 - a) Network devices can send **SNMP traps** to ArkayNMS.
 - b) Traps are received on **UDP port 162**.
 - c) Enables near real-time notification of device and network events.
- **Syslog**
 - a) Network devices send **syslog messages** to ArkayNMS.
 - b) Syslog traffic is received on **UDP port 1514**.
 - c) Provides event and log information for troubleshooting and monitoring.
- **NetFlow / IPFIX / sFlow**
 - a) ArkayNMS receives **flow telemetry** from supported network devices.
 - b) Used for **traffic patterns, bandwidth utilization, top talkers, and application/network flows**.

ArkayNMS Monitoring & Management Capabilities

The collected data is used across the platform for:

- **Inventory** – Centralized information about monitored devices and network assets.
- **Alarms** – Detection and visibility of faults, events, and threshold violations.
- **Topology** – Visualization of network devices and their logical connectivity.
- **Grafana** – Dashboards and visualization of monitoring and performance data.
- **Reports** – Generation of network performance, availability, capacity, and operational reports.

Telemetry Flow: Network Devices → ArkayNMS → Inventory / Alarms / Topology / Grafana / Reports

• 02 Getting Started

Get access, validate the platform and complete the recommended first setup.

Accessing the NMS

Service	Typical URL
Web UI	http://<server-ip>/
Web API	http://<server-ip>:8080/
Grafana	http://<server-ip>:3000/

Login and logout

Sign in

- 1 Open the Web UI.
- 2 On the login page, enter Username and Password.
- 3 Click Sign In.
- 4 Use Single Sign-On only when Keycloak SSO is configured.
- 5 Use the profile menu to log out and end the session.

Forgot password

Password reset

- 1 Click Forgot Password?.
- 2 Enter the registered Email Address.
- 3 Click Send Password Reset Email.
- 4 Open the email and complete the Reset Password flow.

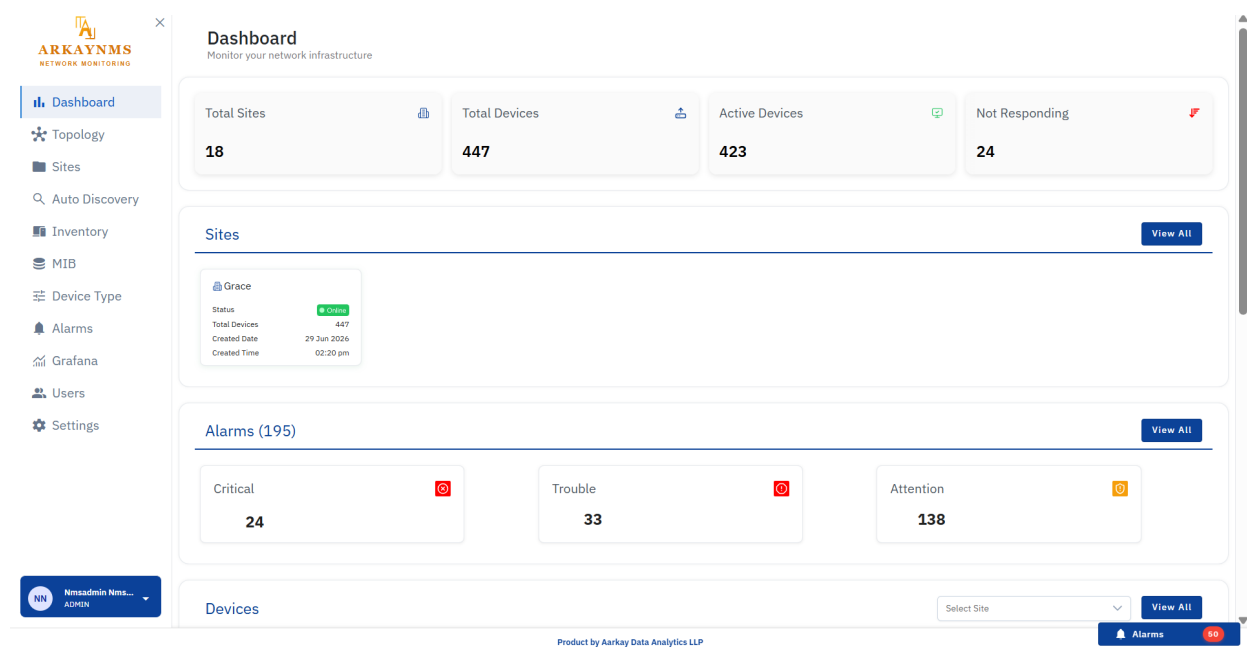
License activation

When a valid license is not present, the UI opens the license management flow before normal Home access. Remote requests can be submitted from the pre-login flow; air-gapped deployments can generate a request file and import the license key returned by the issuer.

Recommended first-week setup

1. Sign in as an administrator and confirm the licensed device/user counts.
2. Set Settings -> Display & Time so timestamps and "today" windows use the correct timezone.
3. Configure Notification Provider Settings for SMTP (and SMS if required).
4. Create the real site tree before registering devices.
5. Confirm Device Types such as Switch, Router, Firewall and WLC.
6. Import vendor MIBs beyond DEFAULT where needed.
7. Review the DEFAULT parameter group, create vendor-specific groups and set thresholds.
8. Configure common trap groups such as linkDown and authentication events.
9. Run Auto Discovery for one subnet and register devices with site/type/groups.
10. Spot-check device settings, then verify Device Summary and View Params.
11. Open Topology and use Automatic first; correct missing links with Semi-automatic or Fully manual views.
12. Create a notification profile for Critical conditions on core devices.
13. Configure at least a small test set for traps/syslog and confirm data appears in Alarms/Grafana.
14. Create an Operator account and grant only the required view permissions.
15. Agree data-retention periods with storage and compliance needs.

You will end up with something like this



ArkayNMS dashboard - supplied application walkthrough screenshot.

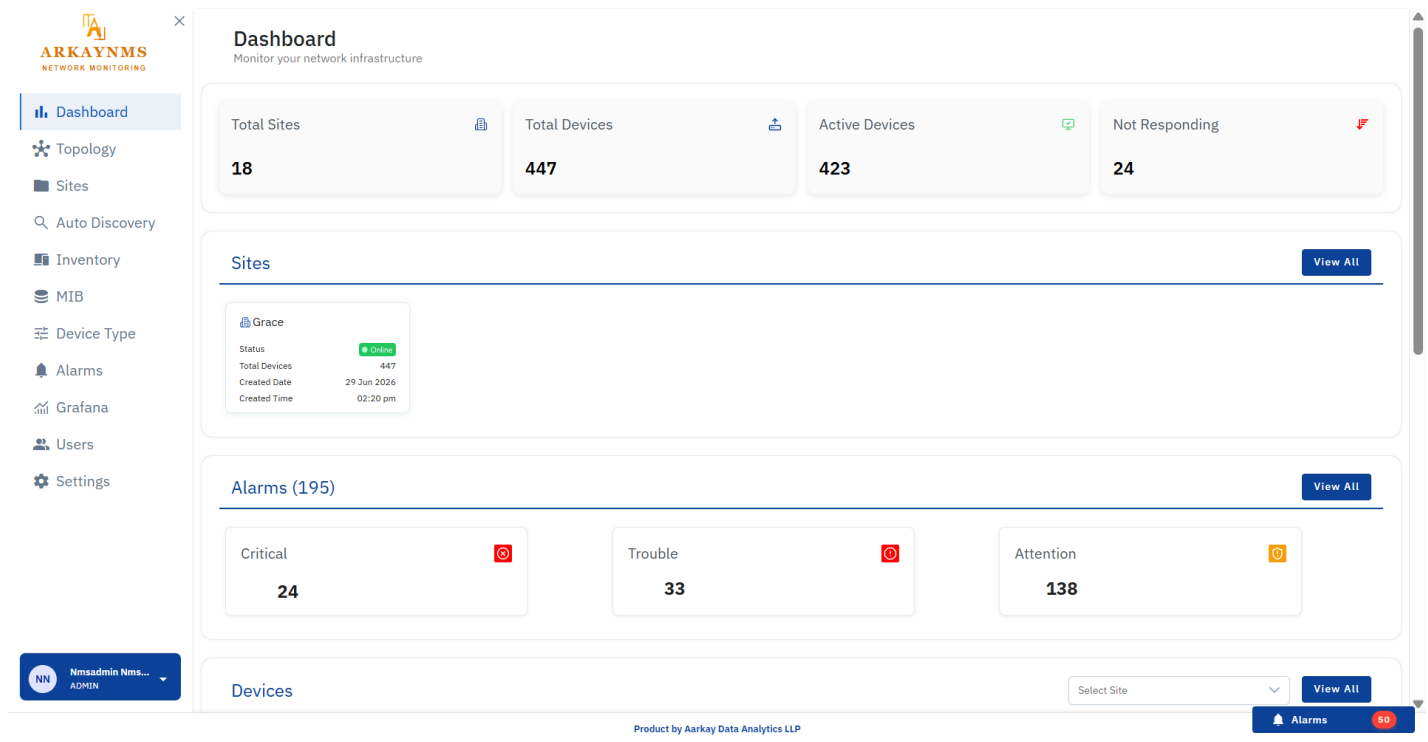
03 NMS Dashboard

Start every health check from a single fleet view.

Dashboard overview

The landing dashboard summarizes sites and devices and gives operators an immediate view of alarm severity, device health and recent activity. Use it as the first stop before drilling into an individual device.

KPI	Meaning
Total Sites	Sites in the site tree.
Total Devices	Managed devices in Inventory.
Active Devices	Devices currently reachable/responding.
Not Responding	Devices that are unreachable or not polling.

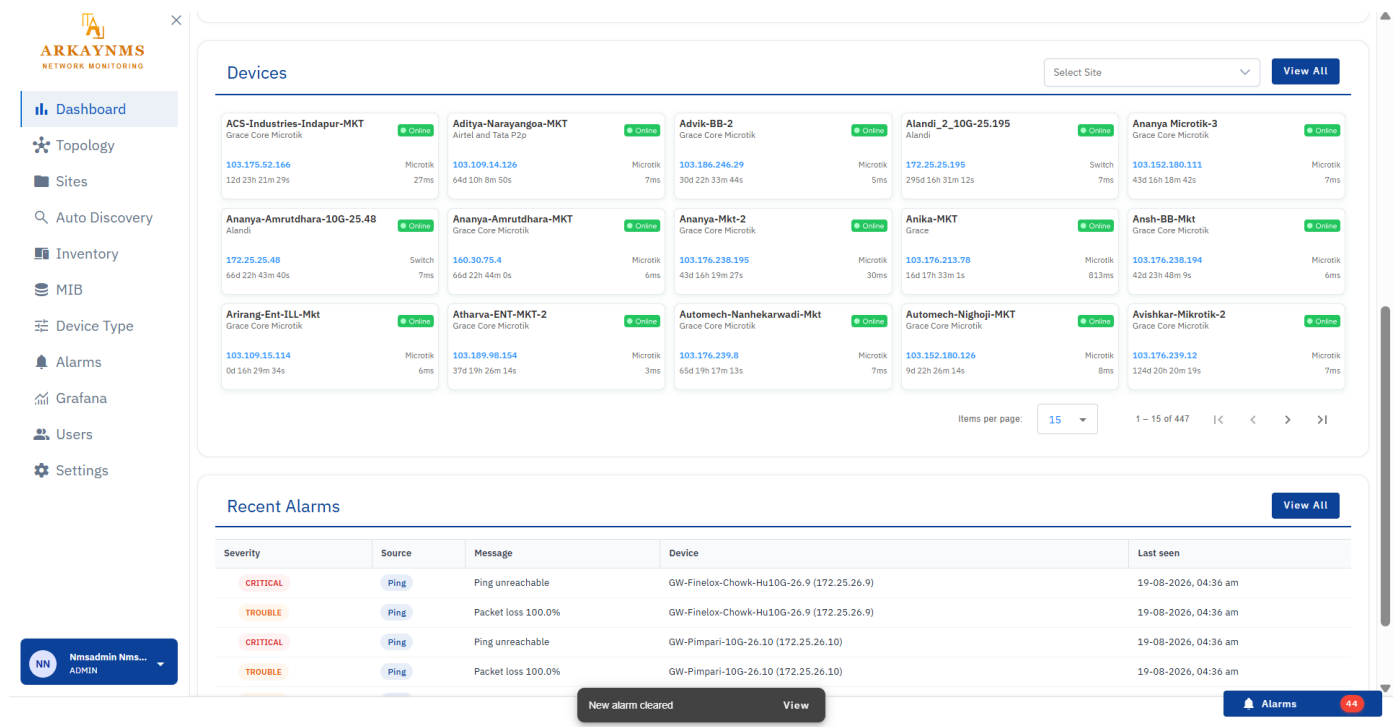


The screenshot displays the ArkayNMS Dashboard interface. On the left is a sidebar with navigation links: Dashboard (selected), Topology, Sites, Auto Discovery, Inventory, MIB, Device Type, Alarms, Grafana, Users, and Settings. The main content area is titled 'Dashboard' with the subtitle 'Monitor your network infrastructure'. It features four KPI cards at the top: Total Sites (18), Total Devices (447), Active Devices (423), and Not Responding (24). Below these are three sections: 'Sites' (showing a card for 'Grace' with status 'Online', 447 total devices, and creation details), 'Alarms (195)' (showing counts for Critical: 24, Trouble: 33, and Attention: 138), and 'Devices' (with a 'Select Site' dropdown and a 'View All' button). At the bottom right, there is an 'Alarms' button with a red circle containing the number 50. The footer of the dashboard area reads 'Product by Arkay Data Analytics LLP'.

Dashboard: fleet-level KPI cards, sites and alarm summary.

Reading the dashboard

- Use KPI cards to spot a change in fleet size or availability.
- Open site cards to move from a fleet view to a location-specific view.
- Use Critical, Trouble and Attention alarm counts to choose the next investigation.
- Use the device area to open an IP directly into the device workspace.
- Use Recent Alarms or View All for the complete incident queue.



The screenshot shows the ARKAYNMS dashboard with a sidebar on the left containing navigation links: Dashboard, Topology, Sites, Auto Discovery, Inventory, MIB, Device Type, Alarms, Grafana, Users, and Settings. The main content area is divided into two sections: 'Devices' and 'Recent Alarms'.

Devices Section: This section displays a grid of 15 device cards, each representing a different site. Each card shows the site name, IP address, status (Online), and a 'View All' button. The devices are arranged in a 3x5 grid.

Site Name	IP Address	Status
ACS-Industries-Indapur-MKT	103.175.52.166	Online
Aditya-Narayangoa-MKT	103.109.14.126	Online
Advik-BB-2	103.186.246.29	Online
Alandi_2_10G-25.195	172.25.25.195	Online
Ananya Microtik-3	103.152.180.111	Online
Ananya-Amrutdhara-10G-25.48	172.25.25.48	Online
Ananya-Amrutdhara-MKT	160.30.75.4	Online
Ananya-Mkt-2	103.176.238.195	Online
Anika-MKT	103.176.213.78	Online
Ansh-BB-Mkt	103.176.238.194	Online
Arirang-Ent-ILL-Mkt	103.109.15.114	Online
Atharva-ENT-MKT-2	103.189.98.154	Online
Automech-Nanhekarwadi-Mkt	103.176.239.8	Online
Automech-Nighoji-MKT	103.152.180.126	Online
Avishkar-Mikrotik-2	103.176.239.12	Online

Recent Alarms Section: This section displays a table of recent alarms. The table has columns for Severity, Source, Message, Device, and Last seen. There are four alarms listed, all with a severity of 'CRITICAL' or 'TROUBLE'.

Severity	Source	Message	Device	Last seen
CRITICAL	Ping	Ping unreachable	GW-FineloX-Chowk-Hu10G-26.9 (172.25.26.9)	19-08-2026, 04:36 am
TROUBLE	Ping	Packet loss 100.0%	GW-FineloX-Chowk-Hu10G-26.9 (172.25.26.9)	19-08-2026, 04:36 am
CRITICAL	Ping	Ping unreachable	GW-Pimpri-10G-26.10 (172.25.26.10)	19-08-2026, 04:36 am
TROUBLE	Ping	Packet loss 100.0%	GW-Pimpri-10G-26.10 (172.25.26.10)	19-08-2026, 04:36 am

At the bottom of the dashboard, there is a status bar showing 'New alarm cleared', 'View', and 'Alarms 14'.

Dashboard lower section: device list and recent alarms.

OPERATOR HABIT Do not treat a green dashboard as proof that an application is healthy. Use device parameters, latency/loss, interface health, topology and path data when symptoms persist.

• 04 Device Management

Build and maintain the device inventory that everything else depends on.

Sites

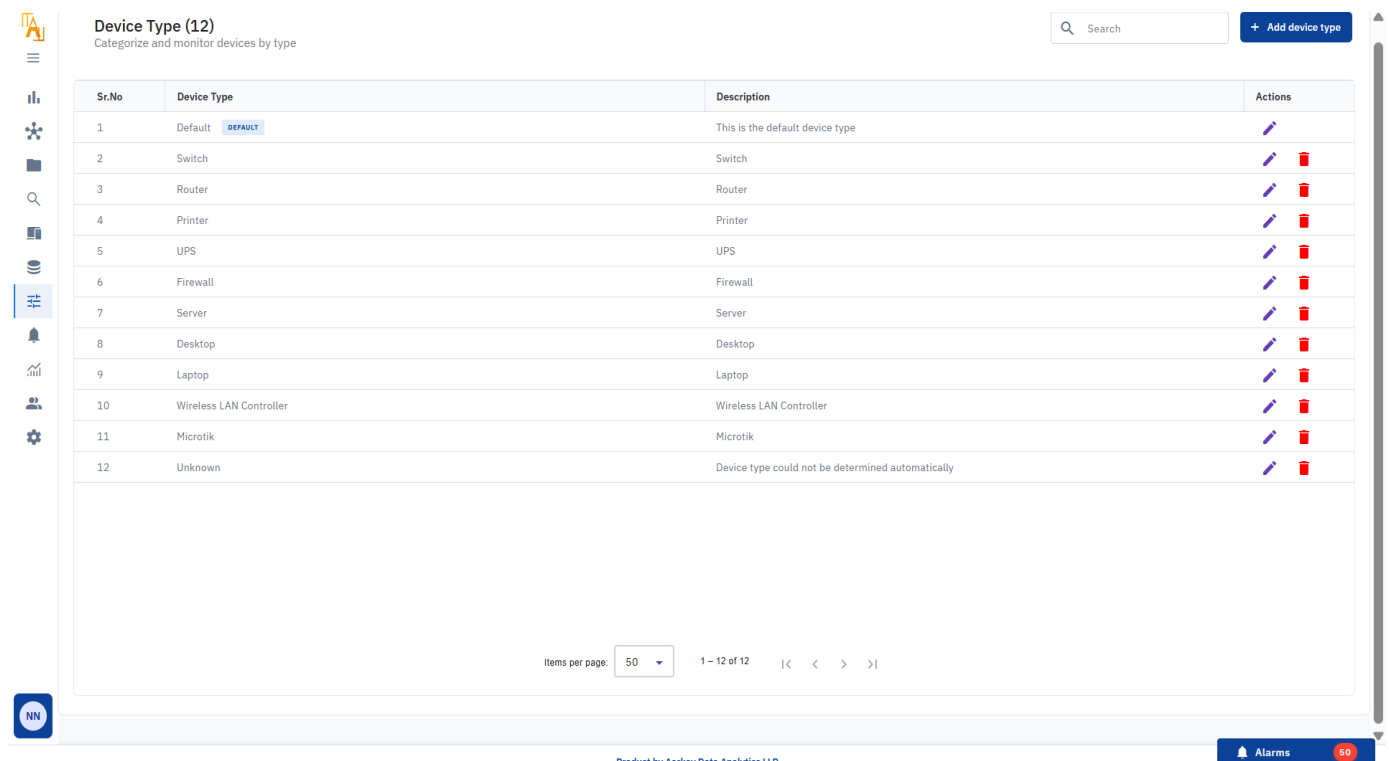
Sites group devices by branch, customer, data center or region. Inventory, topology, users and reports can be site-scoped. Create the site tree before registering devices.

Create a site

- 1 Open Sites.
- 2 Click Add Site.
- 3 Enter Site Name.
- 4 Optionally select a parent for the site hierarchy.
- 5 Click Add.

Device Type

Device types categorize the fleet and influence topology icons and device-specific tabs such as WLC Details. The built-in DEFAULT type is seeded by the platform.



Device Type (12)
Categorize and monitor devices by type

Search + Add device type

Sr.No	Device Type	Description	Actions
1	Default DEFAULT	This is the default device type	 
2	Switch	Switch	 
3	Router	Router	 
4	Printer	Printer	 
5	UPS	UPS	 
6	Firewall	Firewall	 
7	Server	Server	 
8	Desktop	Desktop	 
9	Laptop	Laptop	 
10	Wireless LAN Controller	Wireless LAN Controller	 
11	Microtik	Microtik	 
12	Unknown	Device type could not be determined automatically	 

Items per page: 50 1 - 12 of 12 |< < > >|

Product by Arkay Data Analytics LLP

Alarms 50

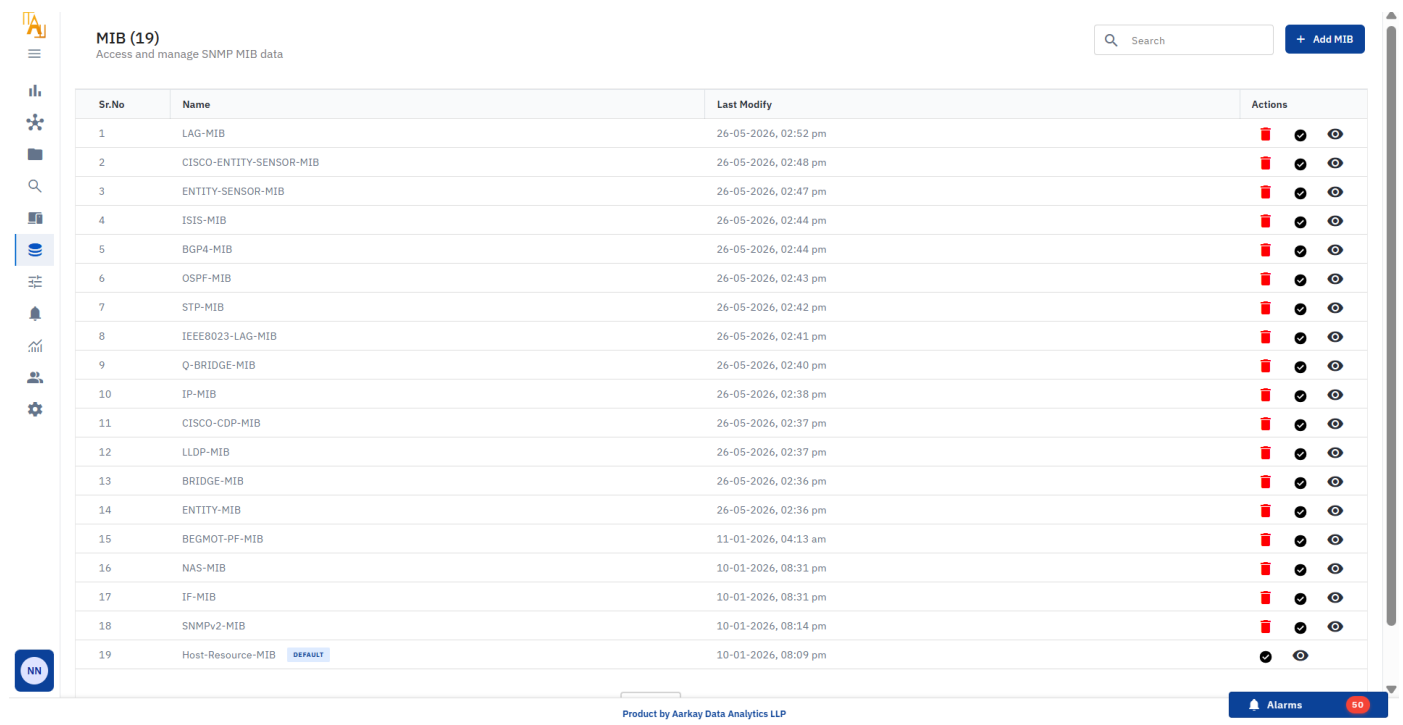
Device Type management screen.

MIB

A MIB is the vendor dictionary used to resolve SNMP OIDs into meaningful parameters and traps. Import vendor MIBs so the OID Browser can locate them without code changes.

MIB is the one which decides what to monitor and what not. MIB has all the relevant SNMP OIDs in a tree like structure, select the MIB parameters you want to monitor, they'll get automatically added in NMS parameters.

You can import the MIBs/ export them for your easiness of process.



MIB (19)
Access and manage SNMP MIB data

Search + Add MIB

Sr.No	Name	Last Modify	Actions
1	LAG-MIB	26-05-2026, 02:52 pm	  
2	CISCO-ENTITY-SENSOR-MIB	26-05-2026, 02:48 pm	  
3	ENTITY-SENSOR-MIB	26-05-2026, 02:47 pm	  
4	ISIS-MIB	26-05-2026, 02:44 pm	  
5	BGP4-MIB	26-05-2026, 02:44 pm	  
6	OSPF-MIB	26-05-2026, 02:43 pm	  
7	STP-MIB	26-05-2026, 02:42 pm	  
8	IEEE8023-LAG-MIB	26-05-2026, 02:41 pm	  
9	Q-BRIDGE-MIB	26-05-2026, 02:40 pm	  
10	IP-MIB	26-05-2026, 02:38 pm	  
11	CISCO-CDP-MIB	26-05-2026, 02:37 pm	  
12	LLDP-MIB	26-05-2026, 02:37 pm	  
13	BRIDGE-MIB	26-05-2026, 02:36 pm	  
14	ENTITY-MIB	26-05-2026, 02:36 pm	  
15	BEGMOT-PF-MIB	11-01-2026, 04:13 am	  
16	NAS-MIB	10-01-2026, 08:31 pm	  
17	IF-MIB	10-01-2026, 08:31 pm	  
18	SNMPv2-MIB	10-01-2026, 08:14 pm	  
19	Host-Resource-MIB DEFAULT	10-01-2026, 08:09 pm	 

Product by Aarkay Data Analytics LLP Alarms 50

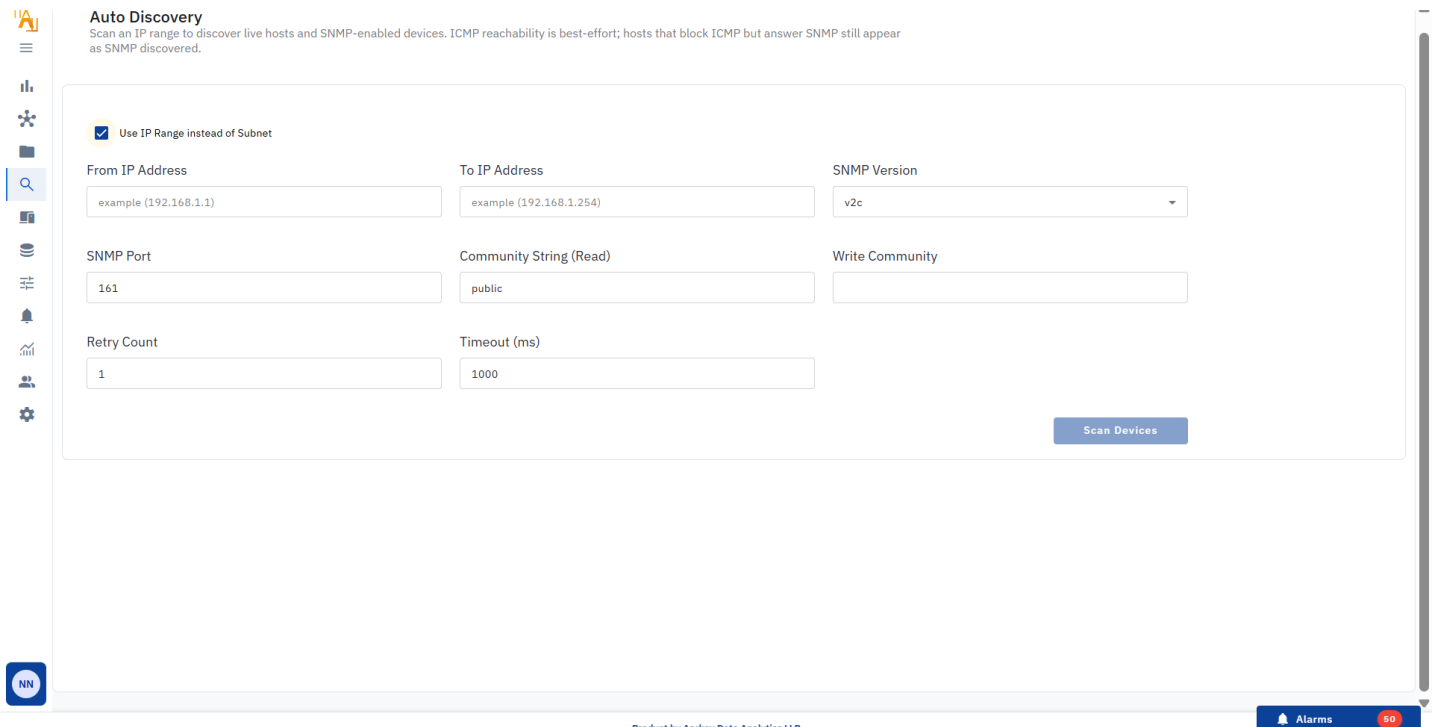
MIB library and OID management.

Auto Discovery

Auto Discovery scans a subnet or IP range and identifies live/SNMP-enabled devices. ICMP is best-effort, so a host that blocks ping can still appear as SNMP discovered if it answers SNMP.

Run a discovery scan

- 1 Open Auto Discovery.
- 2 Choose subnet or Use IP Range instead of Subnet.
- 3 Enter the CIDR or from /To IP addresses.
- 4 Set SNMP version v1, v2c or v3 and the SNMP port (typically 161).
- 5 Enter the appropriate community or SNMPv3 credentials.
- 6 Set retry count and timeout.
- 7 Click Scan Devices.



Auto Discovery
Scan an IP range to discover live hosts and SNMP-enabled devices. ICMP reachability is best-effort; hosts that block ICMP but answer SNMP still appear as SNMP discovered.

☒ Use IP Range instead of Subnet

From IP Address example (192.168.1.1)	To IP Address example (192.168.1.254)	SNMP Version v2c
SNMP Port 161	Community String (Read) public	Write Community
Retry Count 1	Timeout (ms) 1000	

[Scan Devices](#)

Product by Arkay Data Analytics LLP

Alarms 90

Auto Discovery configuration screen.

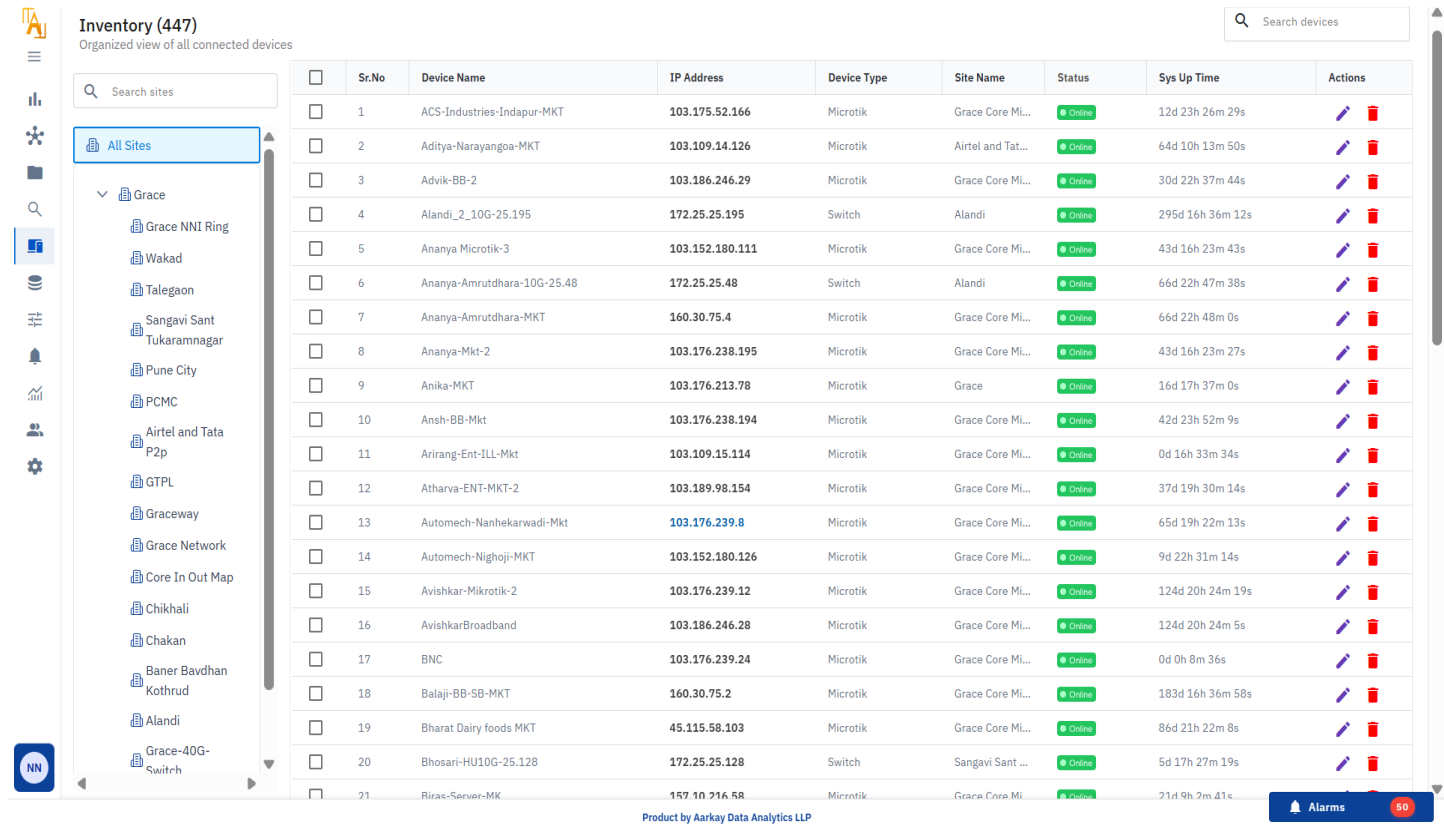
Register discovered devices

Registration

- 1 Filter the discovery results with Search by IP or Name and status filters.
- 2 Click Add Device for one device or select multiple rows for bulk registration.
- 3 Set Select Site and Device Type; add Parameter Groups and Trap Groups when needed.
- 4 Choose monitoring interval and optional remarks.
- 5 Click Register Device or Register All Devices.

Inventory

Inventory is the source of truth for managed devices. Search by device, scope by site, and use row actions to edit, delete or maintain topology links.



Inventory (447)
Organized view of all connected devices

Search sites

All Sites

- Grace
 - Grace NNI Ring
 - Wakad
 - Talegaon
 - Sangavi Sant Tukarnanagar
 - Pune City
 - PCMC
 - Airtel and Tata P2p
 - GTPL
 - Graceway
 - Grace Network
 - Core In Out Map
 - Chikhali
 - Chakan
 - Baner Bavdhan Kothrud
 - Alandi
 - Grace-40G-Switch

	Sr.No	Device Name	IP Address	Device Type	Site Name	Status	Sys Up Time	Actions
☐	1	ACS-Industries-Indapur-MKT	103.175.52.166	Microtik	Grace Core Mi...	Online	12d 23h 26m 29s	
☐	2	Aditya-Narayangoa-MKT	103.109.14.126	Microtik	Airtel and Tat...	Online	64d 10h 13m 50s	
☐	3	Advik-BB-2	103.186.246.29	Microtik	Grace Core Mi...	Online	30d 22h 37m 44s	
☐	4	Alandi_2_10G-25.195	172.25.25.195	Switch	Alandi	Online	295d 16h 36m 12s	
☐	5	Ananya Microtik-3	103.152.180.111	Microtik	Grace Core Mi...	Online	43d 16h 23m 43s	
☐	6	Ananya-Amrutdhara-10G-25.48	172.25.25.48	Switch	Alandi	Online	66d 22h 47m 38s	
☐	7	Ananya-Amrutdhara-MKT	160.30.75.4	Microtik	Grace Core Mi...	Online	66d 22h 48m 0s	
☐	8	Ananya-Mkt-2	103.176.238.195	Microtik	Grace Core Mi...	Online	43d 16h 23m 27s	
☐	9	Anika-MKT	103.176.213.78	Microtik	Grace	Online	16d 17h 37m 0s	
☐	10	Ansh-BB-Mkt	103.176.238.194	Microtik	Grace Core Mi...	Online	42d 23h 52m 9s	
☐	11	Arirang-Ent-ILL-Mkt	103.109.15.114	Microtik	Grace Core Mi...	Online	0d 16h 33m 34s	
☐	12	Atharva-ENT-MKT-2	103.189.98.154	Microtik	Grace Core Mi...	Online	37d 19h 30m 14s	
☐	13	Automech-Nanhekarwadi-Mkt	103.176.239.8	Microtik	Grace Core Mi...	Online	65d 19h 22m 13s	
☐	14	Automech-Nighoji-MKT	103.152.180.126	Microtik	Grace Core Mi...	Online	9d 22h 31m 14s	
☐	15	Avishkar-Mikrotik-2	103.176.239.12	Microtik	Grace Core Mi...	Online	124d 20h 24m 19s	
☐	16	AvishkarBroadband	103.186.246.28	Microtik	Grace Core Mi...	Online	124d 20h 24m 5s	
☐	17	BNC	103.176.239.24	Microtik	Grace Core Mi...	Online	0d 0h 8m 36s	
☐	18	Balaji-BB-SB-MKT	160.30.75.2	Microtik	Grace Core Mi...	Online	183d 16h 36m 58s	
☐	19	Bharat Dairy foods MKT	45.115.58.103	Microtik	Grace Core Mi...	Online	86d 21h 22m 8s	
☐	20	Bhosari-HU10G-25.128	172.25.25.128	Switch	Sangavi Sant ...	Online	5d 17h 27m 19s	
☐	21	Biras-Server-MK	157.10.216.58	Microtik	Grace Core Mi...	Online	21d 9h 2m 41s	

Product by Aarkay Data Analytics LLP

Alarms 50

Device Inventory: searchable, site-organized device registry.

Device workspace

Click an IP address in Inventory to open the device workspace. The workspace exposes Device Summary, WLC Details (when applicable), Configure Params, Configure Traps, View Params and Config Backup.

- You see the Availability
- SystemUpTime
- Site Name
- Monitoring Intervals
- Device name, configure traps, parameters etc.

Configuration backup

Enable Network Config Backup only after credentials and vendor command sets are present under Settings. Running and startup snapshots can be viewed, compared, marked as golden, downloaded and - when supported - restored.

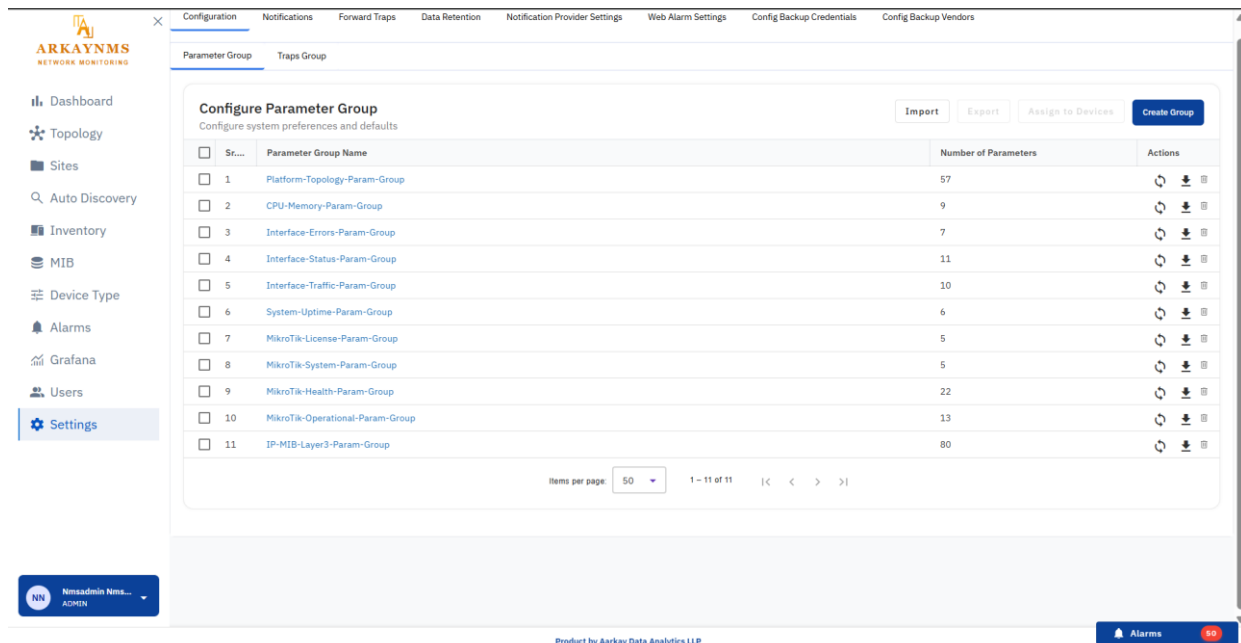
SAFETY NOTE Configuration restore is a change operation. Use it only when the vendor collector and target device support the restore action and the saved configuration is known to be appropriate.

• 05 Network Monitoring

Collect parameters, reachability, traps, flows, syslog and path data.

SNMP parameter monitoring

Parameter groups are reusable OID templates. They can be attached to devices, polled at defined intervals and associated with threshold conditions that generate alarms.



Parameter Group Configuration: reusable monitoring templates.

Add a parameter and thresholds

Configure Params workflow

- 1 Open a device and select Configure Params.
- 2 Attach a Parameter Group or choose Add Parameter.
- 3 Enter the OID or use OID Browser to locate it from a MIB.
- 4 Set Parameter Name, Refresh Interval, Unit and Display Name.
- 5 Choose Param Usage: Log Only, Monitor Only or Both Monitor And Log.
- 6 Optionally define Critical, Trouble, Attention and Realarm conditions.
- 7 Save the parameter.

View live values and history

- Use View Params to fetch current scalar values and inspect indexed tables.
- Set From Date and To Date to review history and trends.
- Use consolidated min/average/max values and detailed data for analysis.
- Export to PDF or Excel when the account has View Reports permission.

Reachability and availability

Per-device ICMP checks provide packet loss and RTT. SNMP availability shows whether the SNMP agent responds. The two tests answer different questions, so a device can respond to ping while SNMP still fails.

REMEMBER Ping asks "is the IP reachable?" SNMP asks "is the management agent responding with the expected security parameters?" A mismatch can come from a wrong community, ACL, SNMPv3 key or related device-side policy.

SNMP traps

ArkayNMS receives traps on UDP 162, decodes and persists them, evaluates trap processor rules and can turn them into unified alarms. Trap history is available per device and across the fleet.

Flow telemetry

NetFlow v5/v9, IPFIX and sFlow records can be collected for traffic analysis. Grafana can expose top talkers, protocol mix and exporter-oriented views.

Syslog

Syslog can be received over UDP/TCP and analyzed by volume, severity, top sources and searchable event data. Pattern rules can raise unified alarms.

RouteInsight

RouteInsight performs hop-by-hop path probes from a probe host to a destination and exposes latency, loss, hop count and critical-hop information. Create a probe first, then add a path service.

RouteInsight quick start

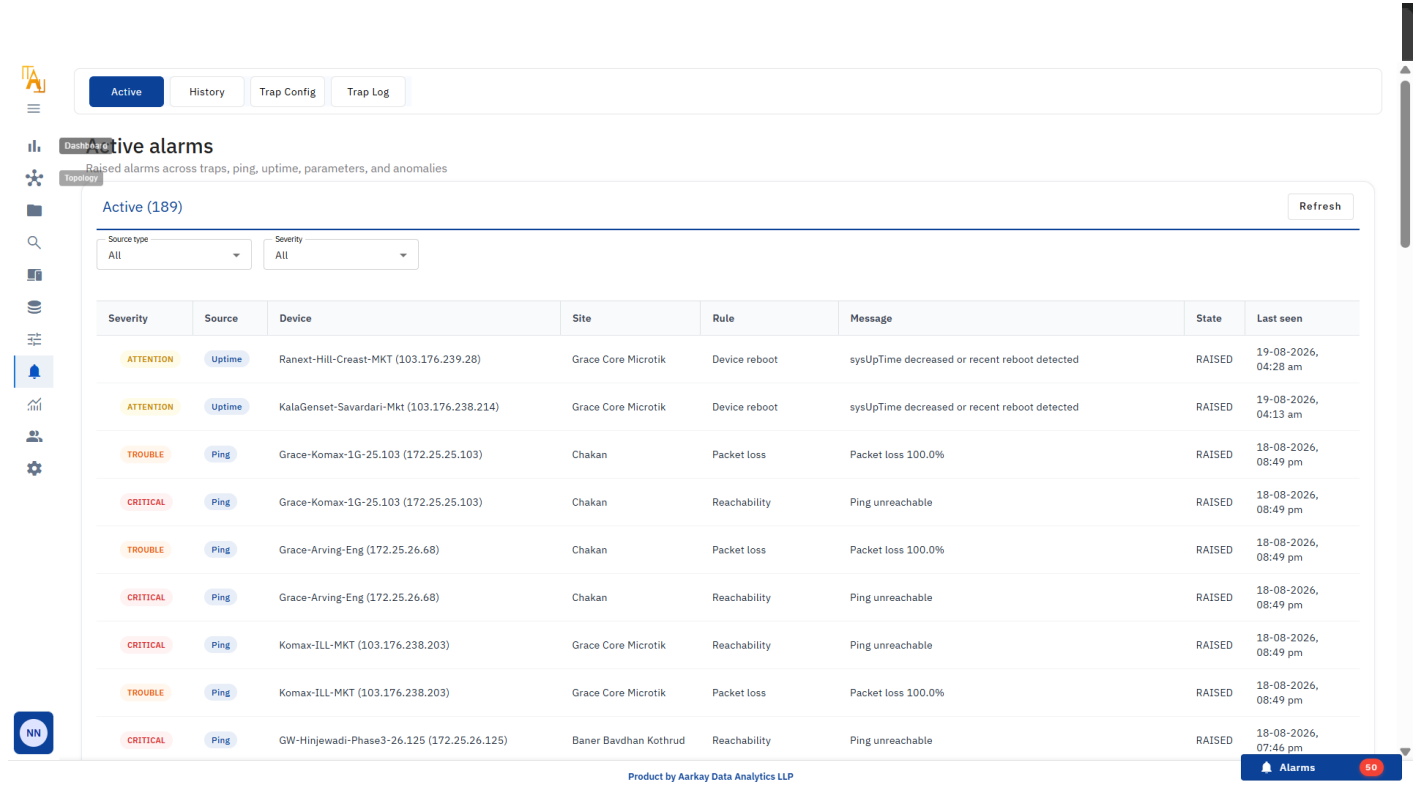
- 1 Open RouteInsight and create a Probe with name, site, location label and source IP.
- 2 When the probe is remote, install the probe command on the branch/remote host.
- 3 Create a Service with destination host, port, interval and probe.
- 4 Open the service snapshot and inspect max hop latency, max hop loss, discovered paths and critical hops.

06 Alerts & Alarms

Turn telemetry into incidents that operators can act on.

Unified alarm model

ArkayNMS brings incidents from SNMP parameters, traps, ping, uptime, syslog, NetFlow, anomaly rules and configuration-backup events into one alarm view.



Active Alarms

Raised alarms across traps, ping, uptime, parameters, and anomalies

Active (189)

Source type: All Severity: All

Severity	Source	Device	Site	Rule	Message	State	Last seen
ATTENTION	Uptime	Ranext-Hill-Creast-MKT (103.176.239.28)	Grace Core Microtik	Device reboot	sysUpTime decreased or recent reboot detected	RAISED	19-08-2026, 04:28 am
ATTENTION	Uptime	KalaGenset-Savardari-Mkt (103.176.238.214)	Grace Core Microtik	Device reboot	sysUpTime decreased or recent reboot detected	RAISED	19-08-2026, 04:13 am
TROUBLE	Ping	Grace-Komax-1G-25.103 (172.25.25.103)	Chakan	Packet loss	Packet loss 100.0%	RAISED	18-08-2026, 08:49 pm
CRITICAL	Ping	Grace-Komax-1G-25.103 (172.25.25.103)	Chakan	Reachability	Ping unreachable	RAISED	18-08-2026, 08:49 pm
TROUBLE	Ping	Grace-Arving-Eng (172.25.26.68)	Chakan	Packet loss	Packet loss 100.0%	RAISED	18-08-2026, 08:49 pm
CRITICAL	Ping	Grace-Arving-Eng (172.25.26.68)	Chakan	Reachability	Ping unreachable	RAISED	18-08-2026, 08:49 pm
CRITICAL	Ping	Komax-ILL-MKT (103.176.238.203)	Grace Core Microtik	Reachability	Ping unreachable	RAISED	18-08-2026, 08:49 pm
TROUBLE	Ping	Komax-ILL-MKT (103.176.238.203)	Grace Core Microtik	Packet loss	Packet loss 100.0%	RAISED	18-08-2026, 08:49 pm
CRITICAL	Ping	GW-Hinjewadi-Phase3-26.125 (172.25.26.125)	Baner Bavdhan Kothrud	Reachability	Ping unreachable	RAISED	18-08-2026, 07:46 pm

Product by Arkay Data Analytics LLP

Alarms 50

Active Alarms: one filterable queue across multiple event sources.

Severity	Operator meaning
Critical	Immediate attention. Treat as an urgent service or infrastructure risk.
Trouble	A significant fault requiring investigation.
Attention	A warning condition or lower-severity issue worth reviewing.
Clear	The condition has recovered/cleared.

Active alarms

Investigate an active alarm

- 1 Open Alarms; the Active view is the starting point.
- 2 Filter by Source type if you already know the origin (Trap, Parameter, Ping, Uptime, Syslog, NetFlow, Anomaly).
- 3 Filter by Severity to narrow the queue.
- 4 Expand related alarms when a root incident has children.
- 5 Open Alarm detail to review the summary, related alarms and timeline.

History and acknowledgement

Use History to review incidents over a From/To range and filter by source, severity and state. Trap-driven alarms can also be acknowledged from the relevant trap workflow.

Notifications

- Notification profiles can send Email, SMS or Web alarm notifications based on devices, conditions and severity. Email/SMS requires Notification Provider Settings to be configured and enabled.
- You can Configure the SMTP
- Add web hooks.
- Supports the following notifications
 - a) MS Teams
 - b) WhatsApp
 - c) Telegram
 - d) Gmail Integration

NOISE CONTROL Good alerting is not the same as maximum alerting. Start with meaningful thresholds and critical/core-device notifications, then expand based on observed signal quality.

• 07 Events

Understand the lower-level activity behind alarms and state changes.

Events versus alarms

An event is a recorded observation or message from a monitoring source. An alarm is the operator-facing incident state produced when configured rules or health conditions warrant attention. The two should be related, but not treated as interchangeable.

Key event sources

Source	Typical evidence
Parameter	Threshold crossings or monitoring-state changes.
Trap	Asynchronous device-generated SNMP notification.
Ping	Reachability, loss or latency conditions.
Uptime	Device restart / uptime state information.
Syslog	Device log records and patterns.
NetFlow	Flow-derived rules and traffic conditions.
Config backup	Backup failure, change or baseline drift.

Trap Log

Review trap history

- 1 Open Alarms and select Trap Log when permitted.
- 2 Choose All Devices or a specific Device Name.
- 3 Set From Date and To Date.
- 4 Click Show Data.
- 5 Use source IP, parameter name, received time and value to identify the triggering device event.

Correlating an event with an alarm

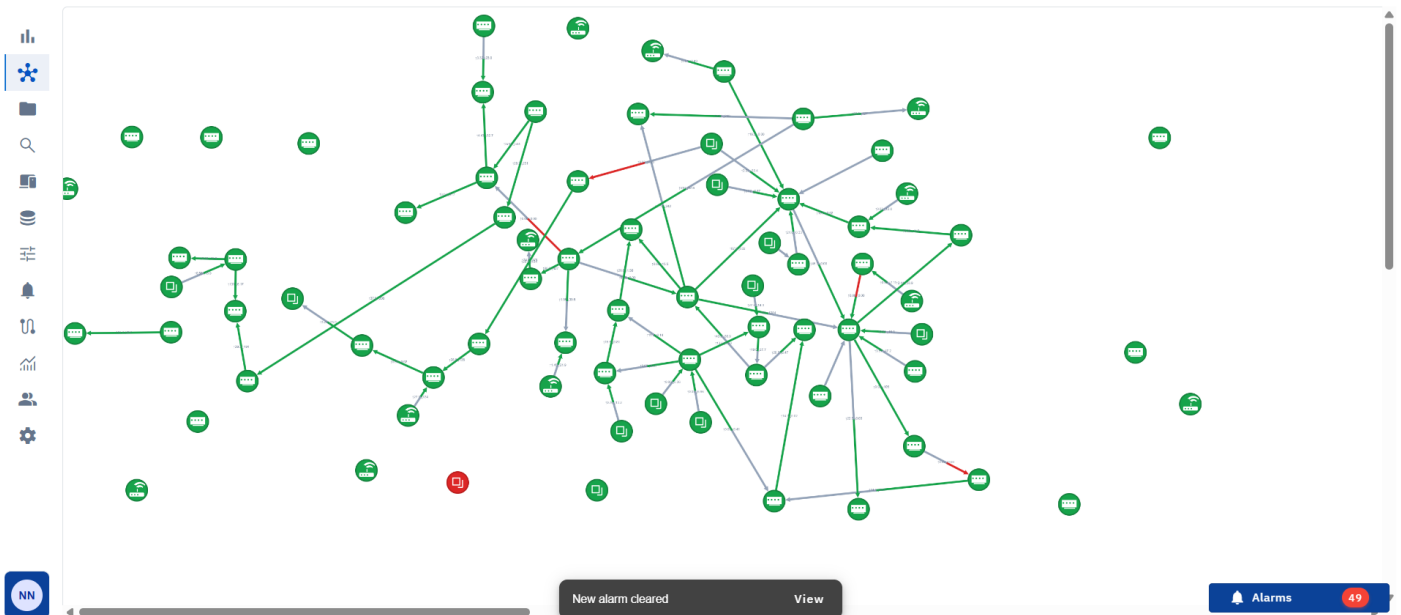
- Start from the alarm source and drill to the related event record.
- Use device and site context to distinguish a local fault from a dependency problem.
- Use timestamps consistently; Settings -> Display & Time controls the platform timezone.

• 08 Network Topology

See relationships, verify links and use the map for dependency analysis.

Topology views

Map view	How it behaves
Automatic	Verified SNMP discovery only.
Semi-automatic	Verified map plus overrides, hints and hidden auto-links.
Fully manual	Only links explicitly drawn by an operator; discovery is ignored.



Network Topology: live device relationship map.

Load a map

Topology workflow

- 1 Open Topology and choose a Site. Prefer one site for normal operation; loading all sites can be slow on large fleets.
- 2 Select Automatic, Semi-automatic or Fully manual.
- 3 Use Search device to highlight a node and Fit to frame the graph.
- 4 Use Refresh when the underlying inventory or discovery state has changed.

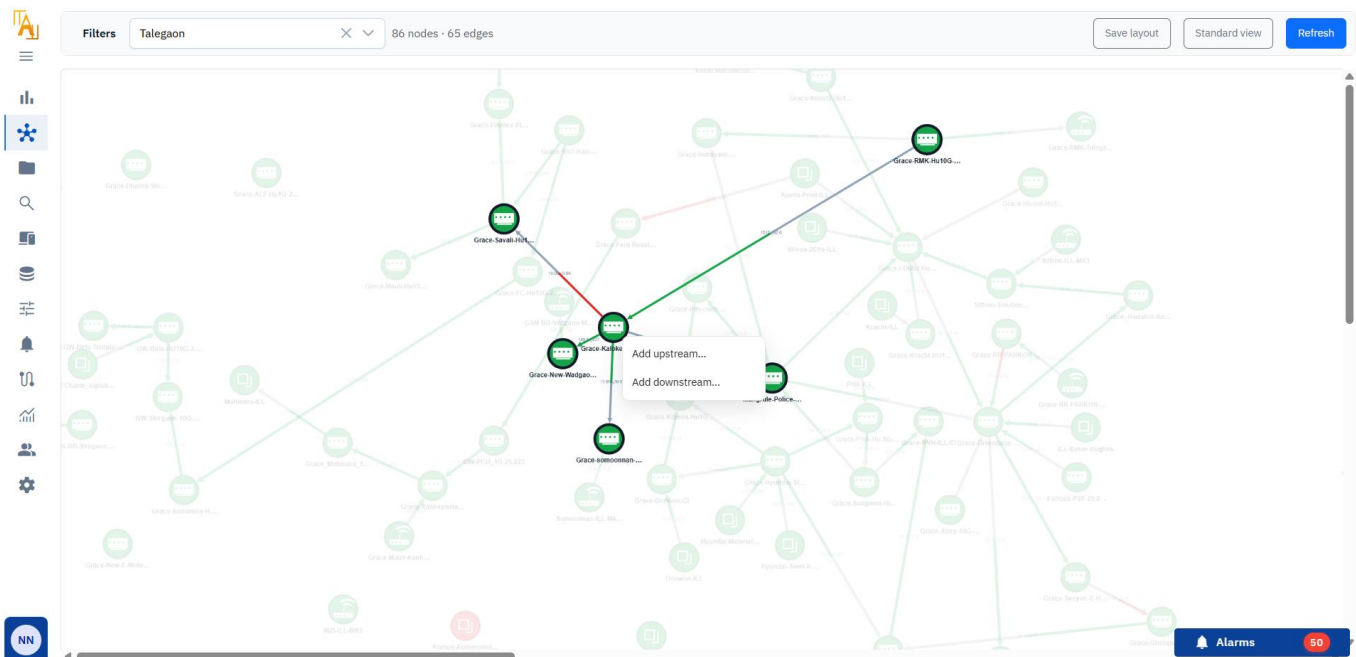
Discovery sources and incomplete maps

Automatic topology relies on polled relationship data such as LLDP, with CDP, FDB/Q-BRIDGE and ARP contributing depending on the environment. An empty map can indicate missing polling, missing neighbor advertisements or the wrong site/view selection.

Fixing or drawing links

Manual / semi-automatic link correction

- 1 Right-click a node and choose Add upstream or Add downstream.
- 2 Select one or more peers and continue.
- 3 Select the interface on the current device; map the optional peer port when known.
- 4 Verify and save the links.
- 5 Use the edge menu later to delete a manual link, hide an auto link or replace an auto link with a manual one.



Path and focus tools

- Focus a device and choose 1, 2 or 3 hops to isolate a local neighborhood.
- Use Tools -> Path from / Path to -> Show path for a targeted relationship view.
- Use Advanced filters for border display, node labels, edge speeds and live link traffic.

Topology export

- Save layout positions per site and map view.
- Export CSV for manual and semi/automatic data views.
- Export PNG for sharing a map snapshot.

09 Reports

Turn monitoring data into evidence, history and shareable output.

❖ Parameter reports

From a device, View Params supports historical analysis and exports in PDF or Excel when the account has View Reports permission. Vertical, Horizontal and Chart presentation modes can be used depending on what needs to be compared.

❖ Inventory and operational reporting

The product feature set includes device, monitor, multi-parameter, inventory and grouped/scalar reporting, plus inventory export. Use reporting when you need a static record rather than a live dashboard.

❖ Grafana analytics

Grafana is opened from the sidebar or directly at the configured Grafana URL. The NMS dashboards include application health, alarms, syslog, NetFlow, executive network views, availability and device/vendor-specific dashboards when those devices are polled.

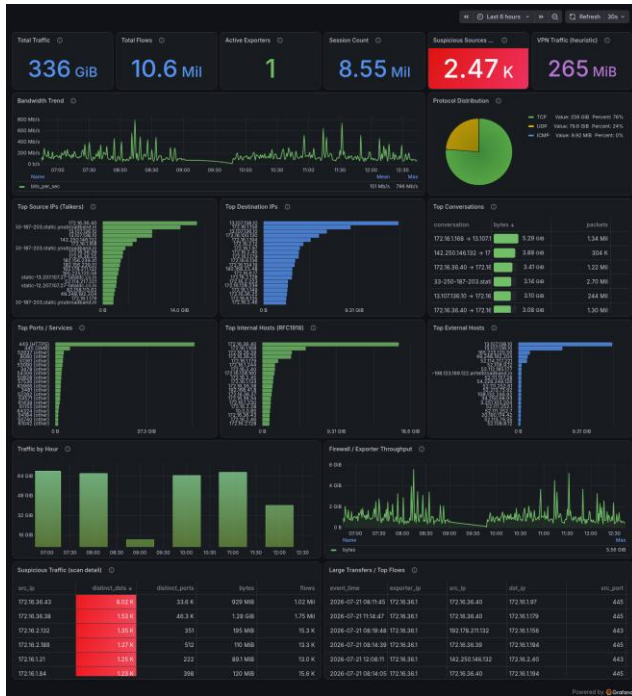
THE Dashboards can be created as per user requirement

Following are the sample dashboards provided.



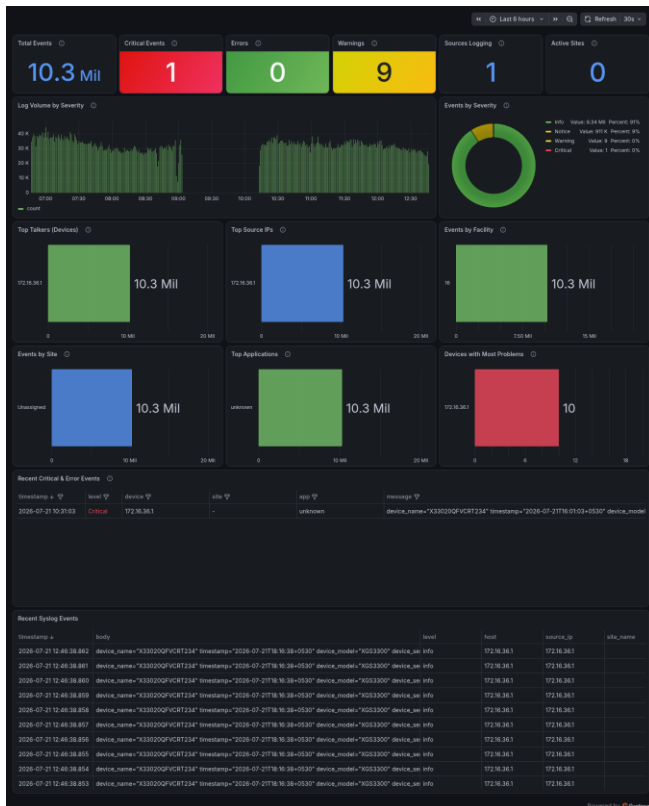
System Uptime & Availability

- Availability percentage over time.
- ICMP latency, packet loss and SNMP response time.
- Recent unexpected reboot indication.



Syslog - Log & Security Overview

- Real-time event volume by severity.
- Top sources generating log traffic.
- Critical and recent events for focused review.



NetFlow - Network & Security Overview

- Top source/destination conversations and talkers.
- Protocol and port mix.
- Traffic patterns and anomaly-oriented views.

DATA DEPENDENCY Syslog and NetFlow dashboards remain empty until devices are configured to export the corresponding data to the NMS ports.

• 10 Search & Filtering

Find the right device, event or time window without hunting.

Search patterns

Need to find...	Best starting point
A device	Inventory search or Topology -> Search device.
A site	Sites search or the site tree in Inventory.
A current alarm	Alarms -> Active, then source/severity filters.
A historical alarm	Alarms -> History with From/To and state filters.
A trap	Alarms -> Trap Log with Device Name and date range.
A parameter	Device -> View Params / Configure Params and search by name or OID.
A flow conversation	Grafana -> NetFlow Dashboard.
A log source	Grafana -> Syslog Dashboard.
A WAN path	RouteInsight -> service snapshot / Compare.

Filtering by time

Use From Date / To Date for alarms, trap logs, parameter history and other historical views. Keep the platform timezone aligned with the environment so that timestamps and "today" boundaries match operator expectations.

Search discipline

- Start with the narrowest stable identifier: IP address, device name, site or source type.
- Add severity or time filters only after the correct data set is selected.
- When investigating a red topology node, compare the node state with Device Summary ping and SNMP availability.

• 11 Troubleshooting

Use a repeatable evidence chain instead of guessing.

A practical troubleshooting flow

Step	Question	Next action
1. Reachability	Does ping respond?	If no, check path, ACL, routing and device availability.
2. SNMP	Does the SNMP agent respond?	If ping works but SNMP fails, validate version, community/v3 keys and ACL.
3. Device health	Are CPU, memory and interfaces healthy?	Open View Params and review live/history values.
4. Alarms	What changed and when?	Check Active/History and related incidents.
5. Topology	What depends on this device/link?	Use site topology, focus and path tools.
6. Flow/log context	Is traffic or logging abnormal?	Review NetFlow / Syslog in Grafana.
7. Config state	Did the configuration change?	Open Config Backup and compare snapshots or golden baseline.
8. Path probe	Is WAN or internet performance abnormal?	Use RouteInsight hop latency/loss to isolate a critical hop.

❖ Scenario: device is down

Investigation

1. Open Dashboard or Inventory and identify the device/site.
2. Open Device Summary and review ICMP status, packet loss, RTT and SNMP availability.
3. If ping is down, validate network path and device state before changing NMS settings.
4. If ping is up but SNMP is down, validate SNMP version, credentials and access controls.
5. Review recent alarms and history around the first failure time.
6. Use topology to see whether an upstream device or link explains the symptom.

❖ Scenario: ping is healthy but users report slowness

Do not stop at ICMP. Review interface utilization and errors, device CPU/memory, WAN circuits, flow behavior, syslog events, and hop-by-hop path performance. A low ping value only proves that the specific ICMP test is responsive.

❖ Scenario: topology is incomplete

1. Select the correct site and verify devices are registered in Inventory.
2. Check that LLDP/CDP/FDB relationship data is actually being polled.
3. Try Semi-automatic or Fully manual modes when discovery data is incomplete.
4. Use manual upstream/downstream links when the network relationship is known but not advertised.

❖ Scenario: Grafana is empty

1. Confirm the device is exporting syslog/flow data to the NMS server IP and expected port.
2. Check firewall and transport settings.
3. Confirm the corresponding ingest service is operational.
4. After a correction, allow a few minutes for data to land before re-evaluating the dashboard.

EVIDENCE FIRST Record the device, site, timestamp, alarm/event, screenshot and checks already performed before escalating. This shortens the handoff dramatically.

• 12 Administration

Control users, permissions, settings, notifications, licenses and backup infrastructure.

Users and permissions

The Users area contains Users and Permissions tabs. Administrator accounts have full access; Operator accounts can be tuned with fine-grained privileges.

Privilege area	Examples
Dashboard / alarms	View Dashboard, View Alarms, View All Alarms, export alarms
Sites	View / Add / Update / Delete / Manage Site
Devices	View / Add / Update / Delete Device, Manage Device Details
Monitoring	Monitor CRUD, parameter groups, log intervals, reports
Traps	Configure Trap, Trap Viewer and trap processor controls
MIB / types	MIB operations and Device Type CRUD
Users	User and permission administration
Settings	Groups, notifications, forwarding, retention, providers, web alarm
Display	View and update display settings

Create an operator

User creation

- 1 Open Users -> Add User.
- 2 Enter first name, last name, username, email and location.
- 3 Choose Administrator or Operator.
- 4 Add the user.
- 5 Open Permissions and enable only the privileges the operator requires.

Settings

Tab	Purpose
Configuration	Parameter groups and trap groups.
Notifications	Email, SMS and web-alarm profiles.
Forward Traps	Relay traps to another NMS/SIEM/parent platform.
Data Retention	ClickHouse TTLs for monitored data and history.
Display & Time	Platform timezone.
Notification Provider Settings	SMTP and SMS gateway configuration.
Web Alarm Settings	Browser alarm sound assets.
License Management	Entitlement and device/user count.
Config Backup Credentials	SSH/Telnet credential vault.
Config Backup Vendors	Vendor CLI command sets.

Retention and licensing

Retention is configured with selectable TTL windows. Licensing is per managed device, with features included rather than sold as separate modules. Use License Management to review status, entitlement, validity and pending requests.

Config backup administration

- Create SSH/Telnet credential profiles and test them before assigning them to devices.
- Maintain vendor collectors and do not deactivate system vendors still referenced by devices.

• 13 Best Practices

Keep the platform useful, quiet enough to trust, and easy to operate.

1. Inventory hygiene

- Maintain site hierarchy before onboarding devices.
- Use clear device names and consistent device types.
- Review inventory regularly for stale devices and incorrect site assignments.

2. Monitoring hygiene

- Use reusable Parameter Groups instead of building every device independently.
- Configure thresholds that represent actionable conditions, not normal variation.
- Use history and trends before changing polling intervals.

3. Alarm hygiene

- Start with meaningful Critical notifications and expand only when the signal proves useful.
- Review unresolved alarms on a routine cadence.
- Use related alarms and root-cause context instead of treating every child alarm as a separate outage.

4. Topology hygiene

- Keep the selected site scope correct.
- Use Automatic discovery as the baseline, then correct known gaps with Semi-automatic or Fully manual links.
- Save layouts so the map remains recognizable to the next operator.

5. Access and security

- Give operators only the permissions they need.
- Use SNMPv3 with authentication and privacy for production where supported.
- Protect configuration-backup credentials and treat restore as a controlled change.

6. Documentation habit

- When escalating, provide device, site, timestamp, symptom, relevant alarm/event and evidence.

● 14 FAQ

Quick answers to the questions operators ask most often.

Why can I ping a device but SNMP still fail?

Ping and SNMP test different things. Check the SNMP version, community string or SNMPv3 keys, device ACLs and the SNMP agent.

Why is the topology empty?

Confirm the site, registration and relationship polling. Check LLDP/CDP/FDB data and try Semi-automatic or Fully manual mode.

Why is Grafana NetFlow empty?

The device must export flow records to the NMS IP/port and the corresponding ingest service/firewall path must be working.

Why is Syslog empty?

The device must send syslog to the NMS on the configured port. Validate device forwarding, firewall and ingest service.

Why is a menu missing?

Menu visibility follows the signed-in user permissions.

How do I find a device quickly?

Use Inventory search, or Topology -> Search device.

How do I review a link-down event?

Use Alarms with source Trap or open Trap Log.

How do I see historical CPU/interface data?

Open the device -> View Params and select the required history range.

How do I compare configurations?

Open Config Backup and use Diff or vs Golden.

How do I probe a WAN path?

Use RouteInsight to create a probe and service, then inspect hop latency/loss.

• 15 Glossary

The vocabulary behind everyday ArkayNMS operation.

Term	Meaning
Alarm	Operator-facing incident state raised by configured monitoring conditions or event rules.
CDP	Cisco Discovery Protocol, used as a fallback relationship source for topology where available.
FDB	Forwarding Database information used as one of the relationship sources for topology discovery.
Grafana	Analytics and visualization layer used for time-series dashboards.
ICMP	Internet Control Message Protocol; used here for reachability and latency/loss checks.
IPFIX	IP Flow Information Export, a flow telemetry format supported by the platform.
LLDP	Link Layer Discovery Protocol; a primary source of neighbor information for topology discovery.
MIB	Management Information Base; a dictionary of SNMP OIDs and their meaning.
NetFlow	Flow telemetry technology used to collect network traffic records.
OID	Object Identifier used to address an SNMP parameter.
Parameter Group	Reusable collection of SNMP OIDs, intervals and threshold definitions.
RBAC	Role-based access control; ArkayNMS permissions determine what a user can see or change.
RTT	Round-trip time measured by an ICMP ping or similar path test.
sFlow	Flow sampling/telemetry format supported by ArkayNMS.
SNMP	Simple Network Management Protocol used to poll and manage network devices.
SNMPv3	SNMP version with authentication/privacy security options.
Syslog	Network event/log transport and message format used for centralized logging.
Topology	Graph representation of device relationships and links.
Trap	Asynchronous SNMP notification sent by a device to the NMS.
TTL	Time-to-live retention setting controlling how long a class of data remains stored.

• 16 Support

Make issues easy to reproduce, route and resolve.

How to report an issue

A good support report starts with the smallest reproducible description and enough evidence for someone else to continue the investigation without repeating basic checks.

Include	Example of useful detail
Environment	NMS host/site and affected site.
Device	Device name, IP, type and site.
Time	First observed time and timezone.
Symptom	What the operator expected vs what happened.
Alarm/Event	Alarm severity, source, message or trap details.
Evidence	Screenshot, parameter trend, topology state or Grafana panel.
Checks already done	Ping, SNMP, credentials, firewall, export test, etc.
Recent changes	Device change, threshold change, topology correction, license/settings change.

Support boundaries

- For deployment issues such as services, upgrades or server access, contact Aarkay Data Analytics LLP.
- For day-to-day platform usage, contact the organization's ArkayNMS administrator.

Protocols and ports quick reference

Data	Direction	Default port
SNMP poll	NMS -> device	UDP 161
SNMP traps	Device -> NMS	UDP 162
Syslog	Device -> NMS	UDP/TCP 1514
NetFlow v5/v9	Device -> NMS	UDP 2055 or 9995
IPFIX	Device -> NMS	UDP/TCP 4739
sFlow	Device -> NMS	UDP 6343
ICMP	NMS -> device	ICMP
Config backup	NMS -> device	TCP 22 / 23
Web UI	Browser -> NMS	80
Web API	Browser -> NMS	8080
Grafana	Browser -> NMS	3000

FINAL CHECK Before escalating: verify site scope, device state, ping vs SNMP, recent alarms, topology context and relevant Grafana/log/flow evidence.

ArkayNMS - Operator Quick Reference

You want to...	Go to...
See if the network is up	Dashboard, then Alarms -> Active
Find a device	Inventory search, or Topology -> Search device
Understand a red topology node	Hover on Topology; compare Device Summary ping vs SNMP
See how devices connect	Topology -> Automatic or Fully manual
Watch CPU / interface counters	Device -> View Params / Configure Params
Export parameter history	Device -> View Params -> Export PDF/Excel
See a link-down trap	Alarms (source Trap) or Trap Log
See who is using bandwidth	Grafana -> NetFlow Dashboard
Search logs	Grafana -> Syslog Dashboard
Backup / change / drift	Device -> Config Backup
Probe a WAN path	RouteInsight -> probe + service
Stop email from sending	Settings -> Notification Provider Settings, then Notifications toggle
Hide a menu from an operator	Users -> Permissions
Change timestamps / today boundaries	Settings -> Display & Time
Check license / device count	Settings -> License Management
Fix an empty map	Select a Site; try Semi-automatic or Fully manual; confirm LLDP

End of guide.