

Enhancing ITA's Network Reliability with PRTG Network Monitoring

Presented By:

Sidrah Hashmi, Aysha Bilai, Al Nowshin Rahman

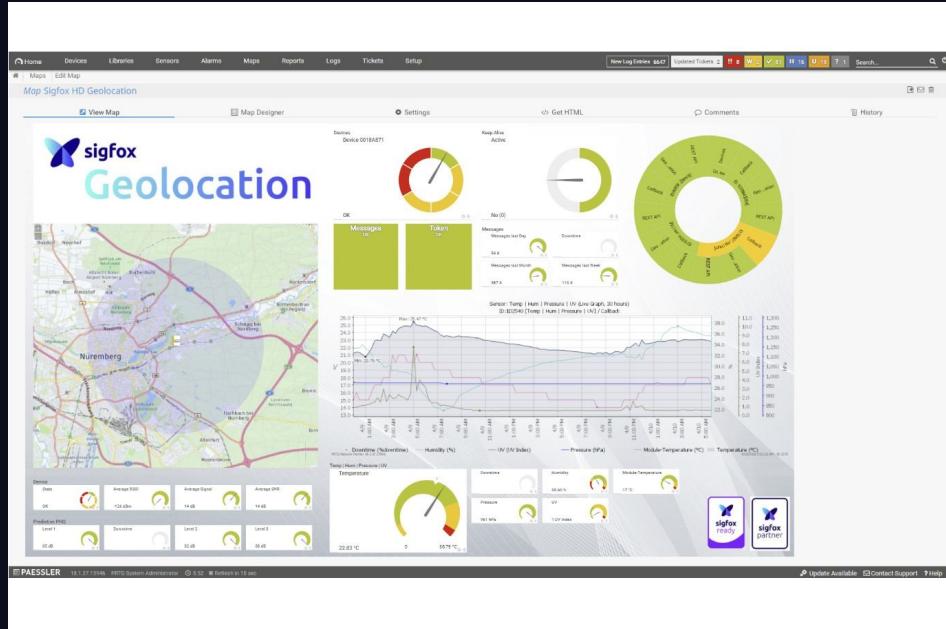


ITA's Problem:

- Rapidly company growth
- Complaints:
 - laggy
 - unstable
 - hard to troubleshoot
- No centralized visibility
- Hard to determine what is online, down or configured



Why PRTG?



PRTG offers:

- Centralized monitoring
 - Auto-discovery
 - Topology maps
 - Basic IP address management
 - Alerts and notifications
 - Easy to deploy and use

PRTG Installation & Monitoring

PRTG Core Server:

- Installed in Head Office Data Centre
- Monitors WAN links and remote branches
- Uses sensors to pull data from routers, switches, servers and firewalls

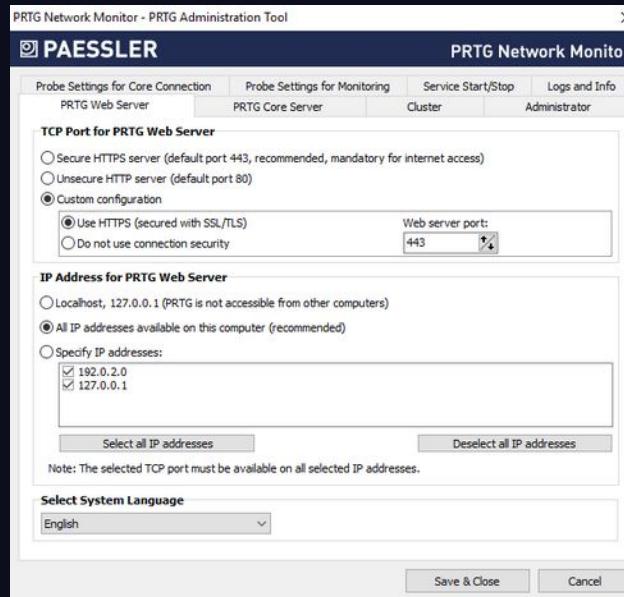
PRTG monitors using:

- Sensors = individual checks (interface load, ping, CPU, VLAN traffic)
- Device groups
- Dashboards: real-time health status (green/yellow/red)

IP Address Management

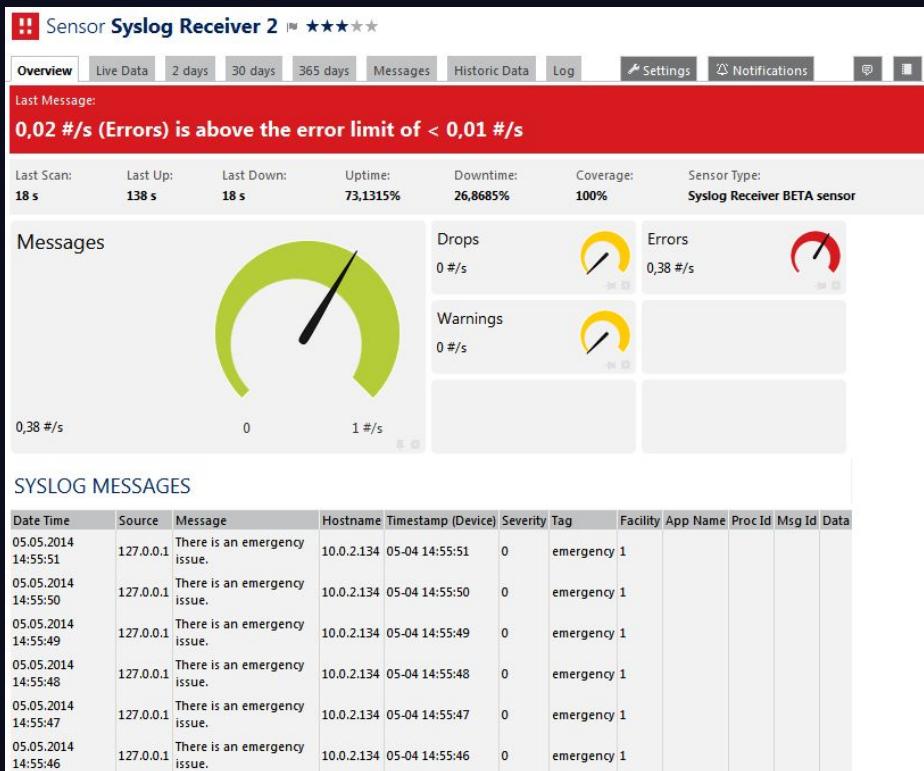
PRTG helps ITA with:

- Auto-discovery of IP ranges
- Tracking used/unused IPs
- Detecting duplicate IPs
- Seeing devices online/offline
- Preventing IP conflicts



What is Syslog?

- Standard **system logging protocol**
- Used to **transfer log information** from network devices to a **central server**
- Uses a **specific message format** for consistency
- Helps track the **overall health** of network devices by simplifying log management



How Syslog Works

- Devices **send event messages** using the syslog protocol
- Messages are sent to a **logging / syslog server**
- **Each message can include:**
 - **Timestamp**
 - **Device ID & IP address**
 - **Severity level**
 - **Event details**

Syslog servers

Syslog Listener

- Listens on the network to **receive syslog messages**

Database/Storage

- Stores large volumes of log data
- Needs **fast read/write** for searching and reporting

Monitoring & Alerts With Syslog

- Use **monitoring tools** to watch syslog messages
Set up **alerts** for important events (e.g., email to admins)
- Can trigger **automated scripts** for certain events
- Helps **respond faster**, reduce damage, and **improve application availability** during peak hours

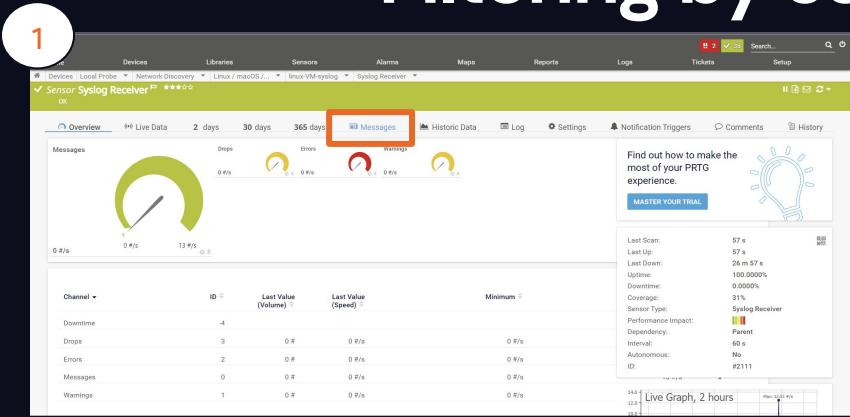
Sensors With Status Down												
Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	Perf. Impact				
Ping v2	Local Probe (Local Probe) » Linux / macOS / Unix » 10.0.0.14	Down		Error caused by lookup value 'Unre...'								
DNS v2	Local Probe (Local Probe) » Network Infrastructure » DNS: 64.71.255.204	Down		Error 4 occurred: Domain name not...								
DNS v2	Local Probe (Local Probe) » Network Infrastructure » DNS: 64.71.255.198	Down		Error 4 occurred: Domain name not...								

<< < 1 to 3 of 3 > >>

Play demo vid

Setting up and sending a syslog message

Filtering by severity, device, or keyword



Syslog Messages

2

The screenshot shows a search interface for syslog messages. It includes a 'Select Range' dropdown, a 'Filter By Date' section with a date range from '2025-08-06 01:31' to '2025-11-14 01:31', and a 'Filter' section with dropdowns for Source, Message, Hostname, Severity (set to Any), Tag, Facility (set to Any), Appname, and Procid. Below this is a table of log entries. The table has columns for Source, Message, Hostname, Severity, Tag, Facility, Appname, Procid, and several columns that are mostly cut off. The first log entry is: 'Source: 2025-11-14 1:31:32 AM 172.20.225. 136 Message: PRTG TEST MESSAGE FROM Aysha-VM Hostname: Aysha Severity: 6 Tag: aysha Facility: 16 App Name: Proc Id: Msg Id: 1'.

Source	Message	Hostname	Severity	Tag	Facility	Appname	Proc Id	Msg Id	I
2025-11-14 1:31:32 AM 172.20.225. 136	PRTG TEST MESSAGE FROM Aysha-VM	Aysha	6	aysha	16				

Aysha Bilai

Centralized Logging

1

element, or contains, a parameter, and a value (comma separated) to match on a structured data value (RFC 5424)

Fixed Include Filter This sensor runs on a specific device, so the sensor filters incoming syslogs for the source IP address of this device and shows matching messages only. If you want to see all messages that are sent to a probe system, create this sensor on the probe device.

Include Filter severity[0-6]

Exclude Filter

Warning Filter severity[4]

Error Filter severity[0-3]

Save

2

Notification Triggers

Type	Rule	Actions
State Trigger	When sensor state is Down for at least 60 seconds, perform @ > Email and push notification to admin When sensor state is Down for at least 300 seconds, perform Ticket Notification and repeat every 5 minutes When sensor state is no longer Down, perform no notification	<input checked="" type="checkbox"/> <input type="checkbox"/>

Configuration Management in PRTG

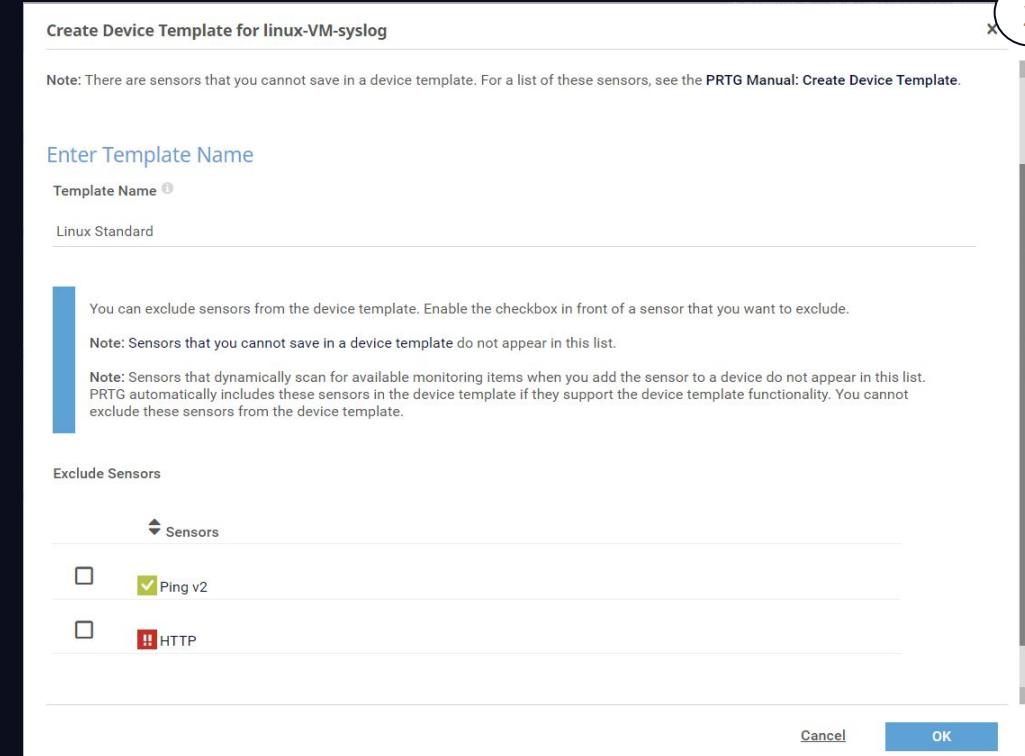
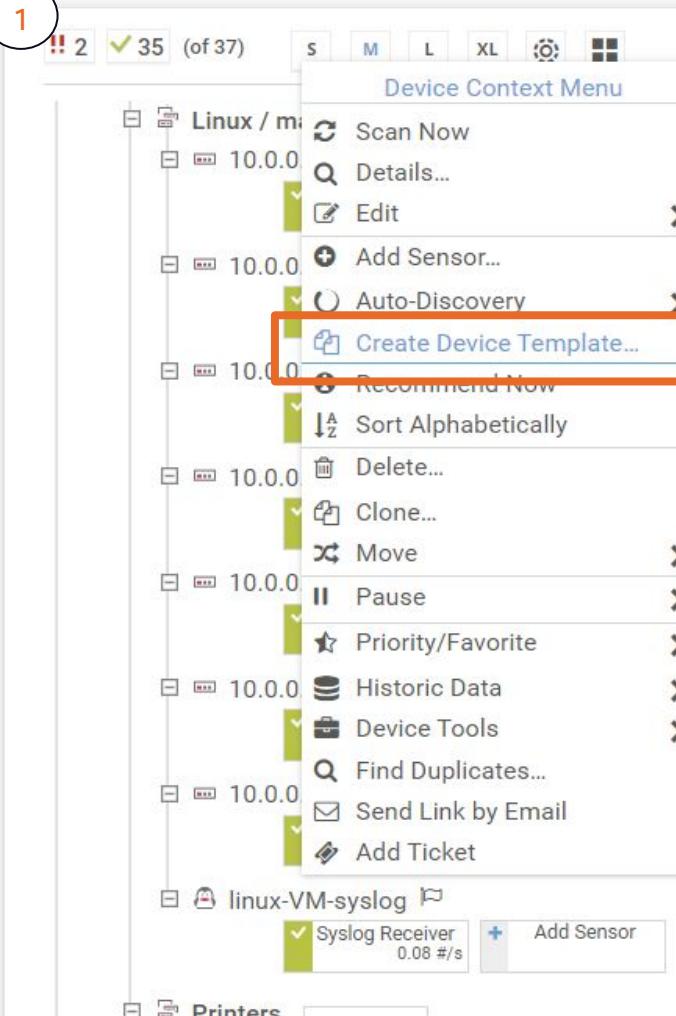
Many branches → lots of repeated device types

- Linux servers, firewalls, switches at each site

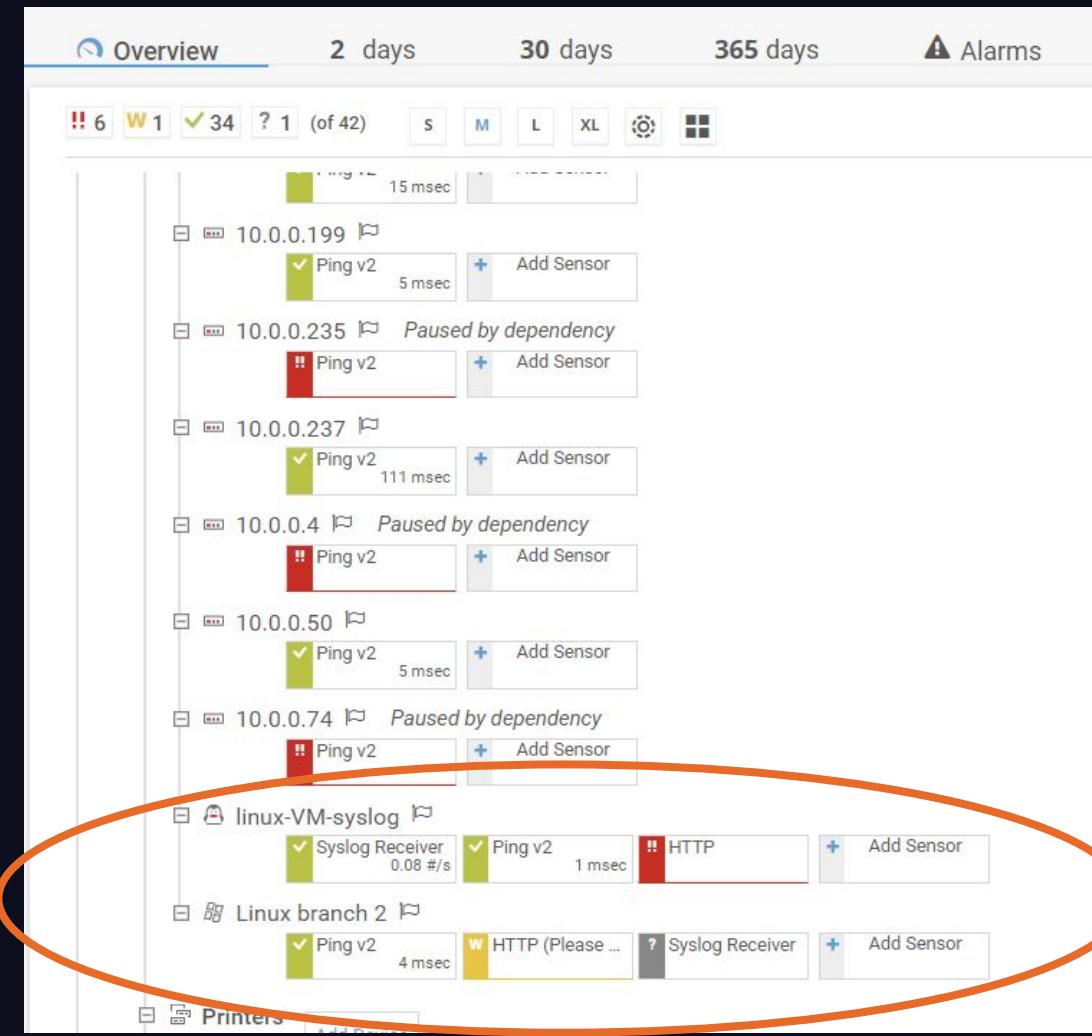
Goal: **same monitoring config everywhere, minimal manual work**

PRTG tools we can use:

- Device templates → standard monitoring pack we can re-use
- Groups & tags → organize devices, share common settings
- SSH / custom script sensors → optionally watch for config changes



Play video



Performance Monitoring in PRTG

Historical Reports and Trends

Date Time	User	Message
2025-11-14 7:54:58 PM	PRTG System Administrator	Subnode Created. Change Trigger ID:4/On Notification: Ticket Notification (ID: 302)
2025-11-14 7:54:42 PM	PRTG System Administrator	Subnode Edited. Threshold Trigger ID:3/Off Notification: Networking Assignment (ID: 2088)
2025-11-14 7:54:34 PM	PRTG System Administrator	Subnode Created. Threshold Trigger ID:3/channel: Primary Threshold Trigger ID:3/condition: above Threshold Trigger ID:3/latency: 60 Threshold Trigger ID:3/Latency: 60 Threshold Trigger ID:3/On Notification: no notification (-1) Threshold Trigger ID:3/Off Notification: no notification (0;-1)
2025-11-14 7:53:52 PM	PRTG System Administrator	Subnode Created. Speed Trigger ID:2/Channel: Traffic in Speed Trigger ID:2/Value: 10 Speed Trigger ID:2/Unit: Mbit Speed Trigger ID:2/Time minute Speed Trigger ID:2/On Notification: Networking Assignment (ID: 2088) Speed Trigger ID:2/Off Notification: Networking Assignment (ID: 2088)
2025-11-14 7:52:36 PM	PRTG System Administrator	Subnode Edited. State Trigger ID:1/On Notification: Networking Assignment (ID: 2088) State Trigger ID:1/Off Notification: Networking Assignment (ID: 2088) State Trigger ID:1/Escalation Notification: Networking Assignment (ID: 2088)
2025-11-14 2:25:05 PM	PRTG System Administrator	Up to date 25.4.112.2189

- Monitors CPU, RAM, Disk, and Bandwidth
- Real-time and historical tracking
- Detects overloaded or failing devices
- Key for diagnosing ITA's "laggy" performance issues

Historical Reports and Trends

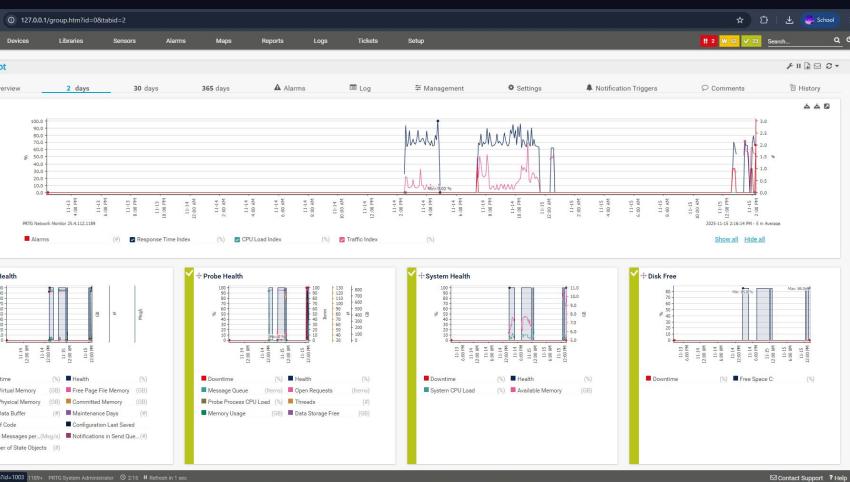
- Stores long-term Graphs
- Useful for capacity planning
- Shows recurring problem times

Monitoring CPU and Memory Health

CPU Monitoring

- Shows real-time processor usage
- Detects overloaded servers/routers
- CPU spikes = slow apps and lags

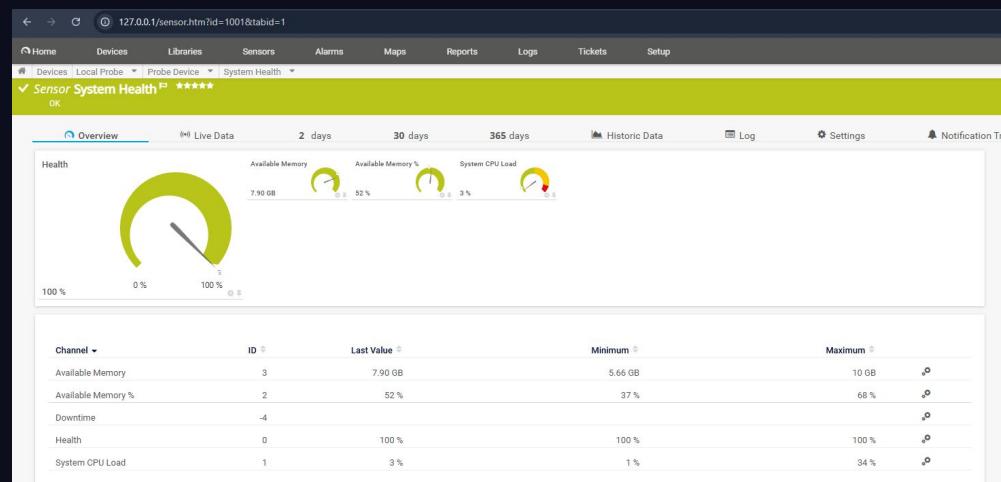
CPU Monitoring



Memory Monitoring

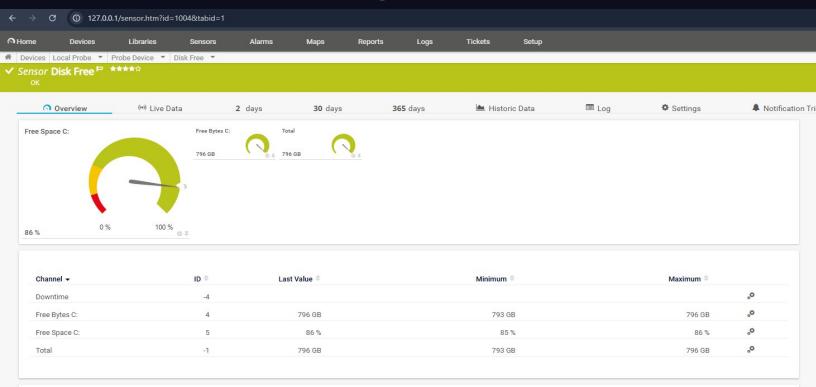
- Tracks RAM usage
- High memory means there's freezing and slowness
- Helps detect stressed equipment

Memory Monitoring



Storage and Network Traffic Monitoring

Disk Space



Traffic Index



Disk Monitoring

- Monitors free disk space
- If disks are full there are service failures
- Important for servers storing logs, apps, backups

Bandwidth Monitoring

- Measures WAN/LAN traffic
- Detects congestion on branch links
- Helps explain slow connections

Alert and Threshold Triggers

Alerts and Thresholds →

- Thresholds for CPU, RAM, Disk, Traffic
- Sends email, SMS, push alerts
- Notifies IT before users complain



Live Alert Example →

- Alert triggers automatically
- Sensor turns yellow/red
- Incident is logged



2025-11-15 4:29:27 PM | Probe Device

WMI Free Disk Space (Multi Disk)

Disk Free

Subnode Created

| Threshold Trigger ID:2/Channel: Total | Threshold Trigger ID:2/Condition: above | Threshold Trigger ID:2/Value: 90 | Threshold Trigger ID:2/Latency: 60 | Threshold Trigger ID:2/On Notification: no notification (ID: -1) | Threshold Trigger ID:2/Off Notification: no notification (ID: -1)

Play video

Conclusion and Recommendation

- PRTG centralized monitoring and logging for all ITA devices
- Maps and dashboards allow IT to quickly identify network issues
- Alerts and notifications reduce downtime and speed up incident response
- Templates, device groups, and IPAM support standardized configurations and up-to-date inventories
- Helps ITA's "laggy, unstable" network providing visibility, proactive alerts, and trend analysis
- Recommendation: implement PRTG to improve network reliability, reduce outages, and support future growth.

