

PLATFORM EXTENSION · RELEASE 10.2

SNMP Management

Polled, trapped and logged like every other element on your network — from the management system you already run.

The **SNMP Management** extension presents the Universal Service Node to your network management system as a managed element: a standard SNMP agent answers SNMPv1 and SNMPv3 queries, watches the platform's own daemons and raises a trap when one stops, and every system event can be forwarded to remote syslog collectors or a SIEM.

2

SNMP versions — v1 communities and authenticated, encrypted v3

4

platform processes watched for traps — media, web, voice and web monitors

15 s

process check interval behind the traps

514

default UDP port for syslog forwarding; any number of collectors

What it does

On the Platform Extensions > SNMP page a system administrator switches the local SNMP agent on, defines read-only community strings each tied to one manager address and, optionally, an SNMPv3 user with MD5 or SHA authentication and DES or AES privacy. A trap destination turns on process monitoring: every 15 seconds the agent checks that the media engine, web server, voice monitor and web monitor are running, and sends a trap naming the process when one is not.

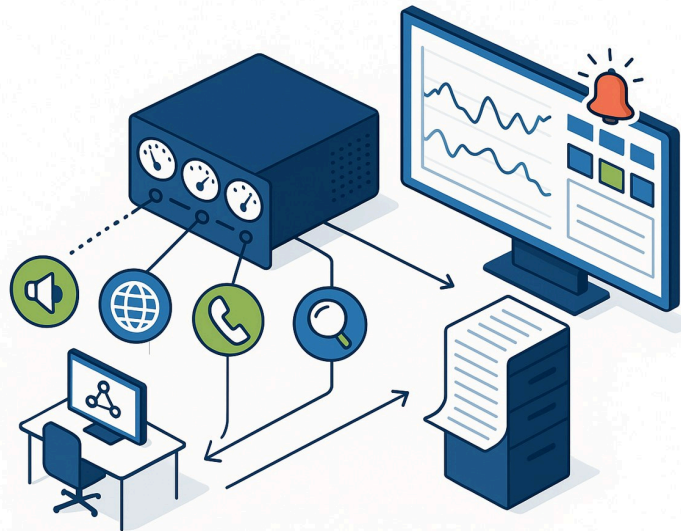
The same page configures syslog: system events written also to syslog, a host nickname on every message, and any number of remote servers by host and port. Settings are validated in full before anything is written.

Why it matters

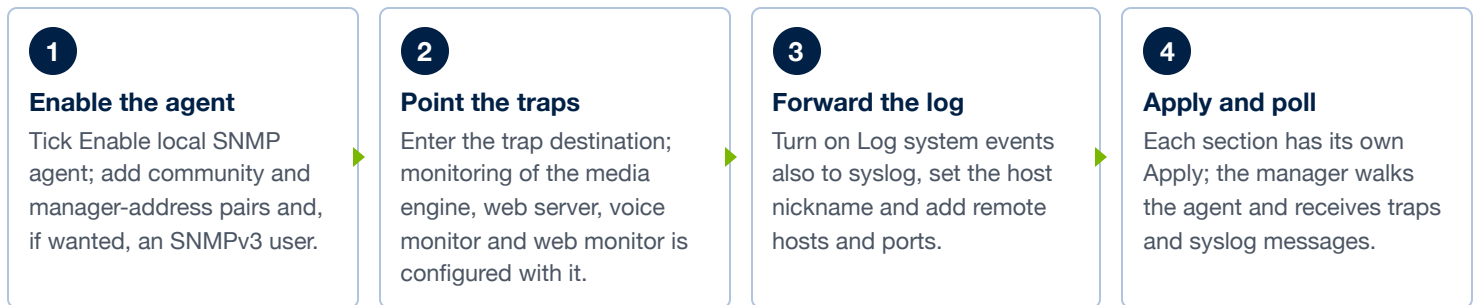
- ✓ Polled like any other element: standard MIBs, v1 or authenticated and encrypted v3.
- ✓ A trap the moment a platform daemon dies — not at the next poll.
- ✓ Sign-ons, failed sign-ons, configuration changes, calls and alarms streamed to your syslog or SIEM.
- ✓ Several collectors at once, each with its own port.
- ✓ Every change validated before it is applied; the agent restarts with the new configuration.
- ✓ Nothing to install: net-snmp and rsyslog are part of the appliance.

How it works

Configured by a system administrator on the Platform Extensions > SNMP page; each section is applied on its own.



The manager polls the agent, the process monitor raises a trap when a daemon goes missing, and the event trail streams to the syslog collectors.



WHAT IS WATCHED

UNIVERSAL SERVICE NODE

WHERE IT GOES



The agent answers the manager's polls, the process monitor raises a trap when a daemon is missing, and rsyslog carries the event trail to any number of collectors.

Features and benefits

FEATURE	HOW IT WORKS	BENEFIT
Local SNMP agent	The appliance's net-snmp daemon is enabled, configured and restarted from the portal; the configuration written by the page becomes the agent's <code>snmpd.conf</code> , and the agent can be disabled again with one tick.	Monitoring switched on without a shell session.
SNMPv1 read-only access	Any number of community and manager-address pairs; each community is read-only and valid only from its manager address. Communities are letters, digits, dots and underscores and act as passwords.	Each management host gets its own credential.
SNMPv3 user	One user of at least 8 characters with MD5 or SHA authentication and DES or AES privacy, each passphrase at least 8 characters, read-only to the whole tree. Optional — leave the block empty for a v1-only setup.	Authenticated and encrypted where v1 is not allowed.
Traps on process failure	With a trap destination set, the agent monitors the media engine (matrix), the web server (nginx), the voice monitor (vmon) and the web monitor (webmon) every 15 seconds, and sends a trap carrying the process name and error message when one is missing.	The NOC knows before the first user calls.
Standard MIBs	What net-snmp exposes by default — MIB-II system and interfaces, HOST-RESOURCES-MIB (processors, memory, storage, running software) and the UCD-SNMP-MIB process table the monitor uses.	Works with the MIB browser the NMS already has.
Syslog forwarding	System events are written to syslog and forwarded by rsyslog to any number of remote servers by host and port (UDP, 514 by default), stamped with a local host nickname; rsyslog is restarted on Apply.	The audit trail lives off the appliance.
Richer event trail	Log additional call info in system events adds per-call detail to the trail; the System Events report in the portal shows the same events with filters and download.	One trail — on the box and at the SIEM.
Validated, atomic apply	Communities, manager addresses, SNMPv3 fields, hostnames and ports are checked in full before a file is written; a rejected Apply names the field and leaves the running configuration untouched.	A typo cannot silence monitoring.

Technical specifications

SNMP agent

Agent	net-snmp <code>snmpd</code> on the appliance, enabled and disabled from the portal
Versions	SNMPv1 (community) and SNMPv3 (user); read-only access
v1 access	One read-only community per manager address; several pairs
v3 security	MD5 or SHA authentication with DES or AES privacy; user and passphrases of 8+ characters

Traps and monitoring

Trap destination	One host name or IP address
Monitored processes	matrix (media engine), nginx (web server), vmon (voice monitor), webmon (web monitor)
Check interval	Every 15 s, DISMAN-EVENT-MIB monitor over the UCD-SNMP-MIB process table
Trap content	Process name and error message, raised when a process count leaves its range



Restart Agent restarted with the new configuration on Apply

Syslog

Transport rsyslog forwarding over UDP; port 1–65535, default 514

Destinations Any number of remote hosts, each with its own port

Identity Local host nickname stamped on every message

Content System events — sign-ons, configuration changes, calls, alarms, security events; optional additional call info

Shared settings The same logging switches and hosts appear on the Enhanced Security page

Administration and licensing

Location Account Portal > Platform Extensions > SNMP; System Administrator

Validation Every field checked before any file is written; a specific error per field

Boot service The same page selects one conference to start automatically at system boot

Licence SNMP feature on the system licence

Managers Any SNMP-capable NMS, including XOP Networks' own Network Management System

Sample use cases**Network operations centre**

The NOC adds the appliance to its NMS with an SNMPv3 user; processors, memory, storage and interfaces appear on the same dashboard as the switches, and a trap fires if the media engine stops.

Security operations

Every sign-on, failed sign-on and configuration change is forwarded to the SIEM within seconds, tagged with the appliance nickname, so a brute-force attempt is correlated with the rest of the estate.

Carrier and multi-site

A service provider running several appliances forwards all of them to one collector and polls each with its own community — no agent to deploy or patch.

One platform, connected to yours

SNMP Management is one of the platform extensions of the Universal Service Node — options that connect the platform to the infrastructure around it. Each is licensed on its own, so a system carries only what its deployment requires.

Call 972-590-0200
www.xopnetworks.com