

# How to configure SNMP on your firewall

# How to configure SNMP on your firewall

This menu allows the administrator to configure the firewall to send relevant information notification events as SNMP traps to the configured host(s). You will need software which can catch these traps and create relevant reports.

## Configure the agent information

Information like name, location of the firewall, contact information and a test description.

Configure

Access Policy

SNMP Trap Settings

Start Service

Add SNMP Configure

Name (For SNMP v2/v3)

Gajshield

Location (For SNMP v2/v3)

Mumbai

Contact (For SNMP v2/v3)

hanif@gajshield.com

Username (For SNMP v3)

gajshield

Security Level (For SNMP v3)

No Authentication and No Privacy

Authentication Algorithm (For SNMP v3)

MD5

Authentication Password (For SNMP v3)

\*\*\*\*\*

Privacy Algorithm (For SNMP v3)

DES

Privacy Password (For SNMP v3)

Description

test

Save

## SYSTEM - SNMP - Access Policy

This shows different SNMP communities which have been configured. SNMP Access policy menu allows you to define the community's name, IP address/network which would be able to query the SNMP server running on your firewall. The access is always read-only. In SNMP access policies' IP field, you need to specify the IP address of machine on which you are configuring PRTG.

**NOTE: To Enable Polling port 161 should be opened from the logging IP to the firewall IP.**

GAJSHIELD

Definitions

Configuration

Management

License

Administration

Shut down

SNMP

CMS

NTP

Settings

Backup

Updates

Syslog

Get logs

Reports via Email

Configure

Access Policy

SNMP Trap Settings

Start Service

Add SNMP Community

Community Name

snmpserver

IP Address

snmpserver

Enable Community

☒

Save

Cancel

Configure			
Access Policy			
SNMP Trap Settings			
Start Service			
Search in All for			
<input type="checkbox"/>	Community Name	IP Address	Enable Community
<input type="checkbox"/>	snmpserver	snmpserver	yes
Delete			

## SNMP - SNMP Trap Settings

In this section you can add the community names and corresponding IPs on which the traps would be configured by those communities. The static traps configured currently are:

1. **Authorization Failure Trap:** Unauthorized SNMP Command Notifications.
2. **Cold Start Trap:** SNMP Agent Start/Stop Notifications
3. **Link Up/Down Trap:** Ethernet Link Up/Down Notifications.
4. **Process Check Trap:** Specific Process MIN/MAX values and currently running Notifications.

Configuration window titled "Add SNMP Trap Setting". It includes tabs for "Configure", "Access Policy", "SNMP Trap Settings", and "Start Service". The form contains the following fields:

- Community String: snmpserver
- Trap Destination IP: fwip-LAN
- Process Monitoring: A list of processes to monitor, currently showing sshd, httpd, sendmail, pptpd, and l2tpd.

Buttons: Save, Cancel.

Configure

Access Policy

SNMP Trap Settings

Start Service

Search in

All

for

Community String

↓

snmpserver

Delete

Trap Destination IP

↓

fwip-LAN

Tasks

## System - SNMP - Start Service

Show whether the SNMP server is running, and you can start and stop the SNMP server.

SNMP Service			
Service			Stopped

Now you can add a rule for SNMP in firewall.

IPV4	Any to Any	snmpserver	fwip-LAN	snmp	-	*	accept	AllTime	-	-			
------	------------	------------	----------	------	---	---	--------	---------	---	---	--	--	--

You have successfully configured SNMP in your firewall.