GAJSHIELD

Data Security Firewall

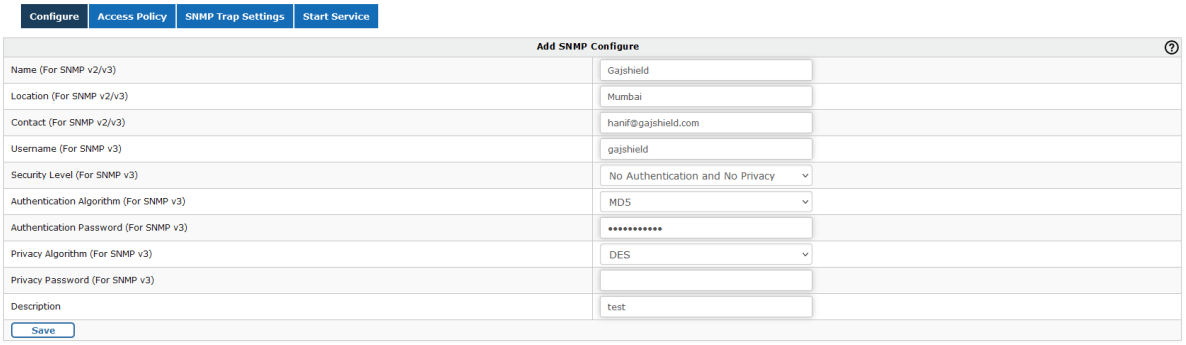
How to configure SNMP on your firewall

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

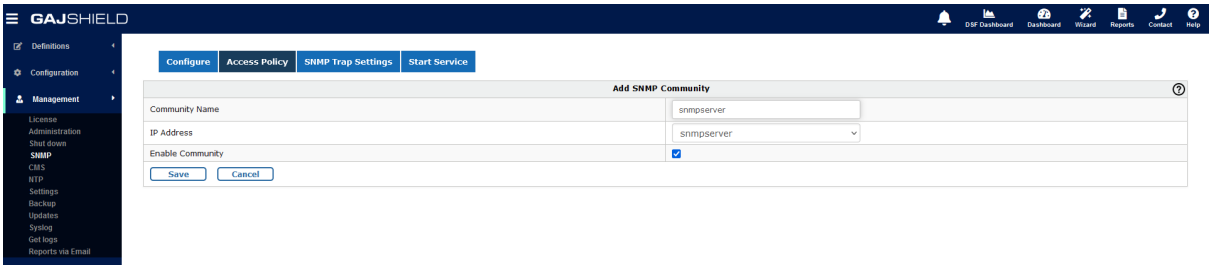
Information like name, location of the firewall, contact information and a test description.

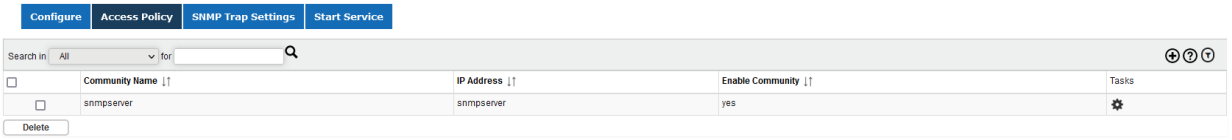


SYSTEM - SNMP - Access Policy

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.





SNMP - SNMP Trap Settings

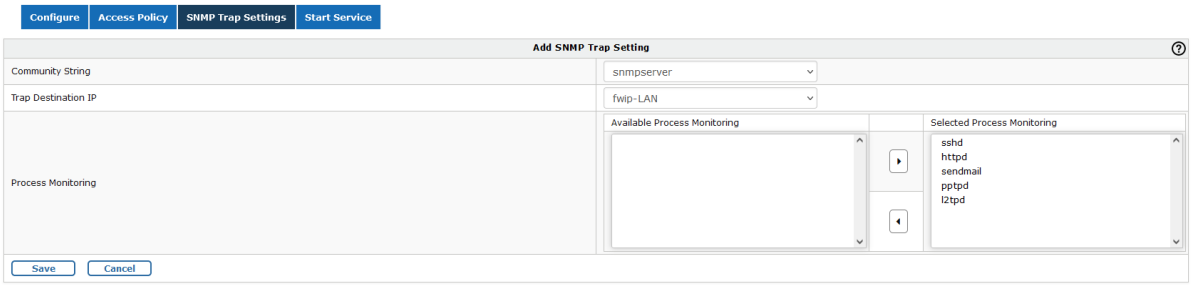
In this section you can add the community names and corresponding IPs on which the traps would be configured by those communities. The static traps configured currently are:

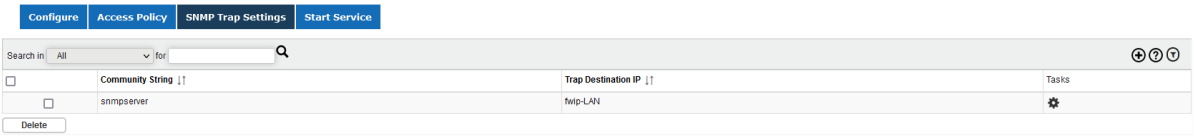
1. **Authorization Failure Trap:** Unauthorized SNMP Command Notifications.

2. **Cold Start Trap:** SNMP Agent Start/Stop Notifications

3. **Link Up/Down Trap:** Ethernet Link Up/Down Notifications.

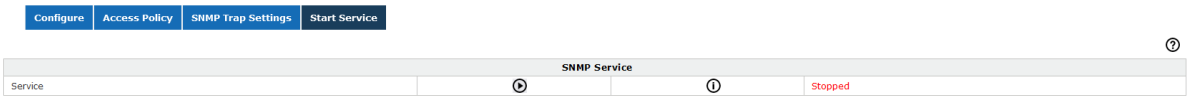
4. **Process Check Trap:** Specific Process MIN/MAX values and currently running Notifications.





System - SNMP - Start Service

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



Now you can add a rule for SNMP in firewall.

You have successfully configured SNMP in your firewall.