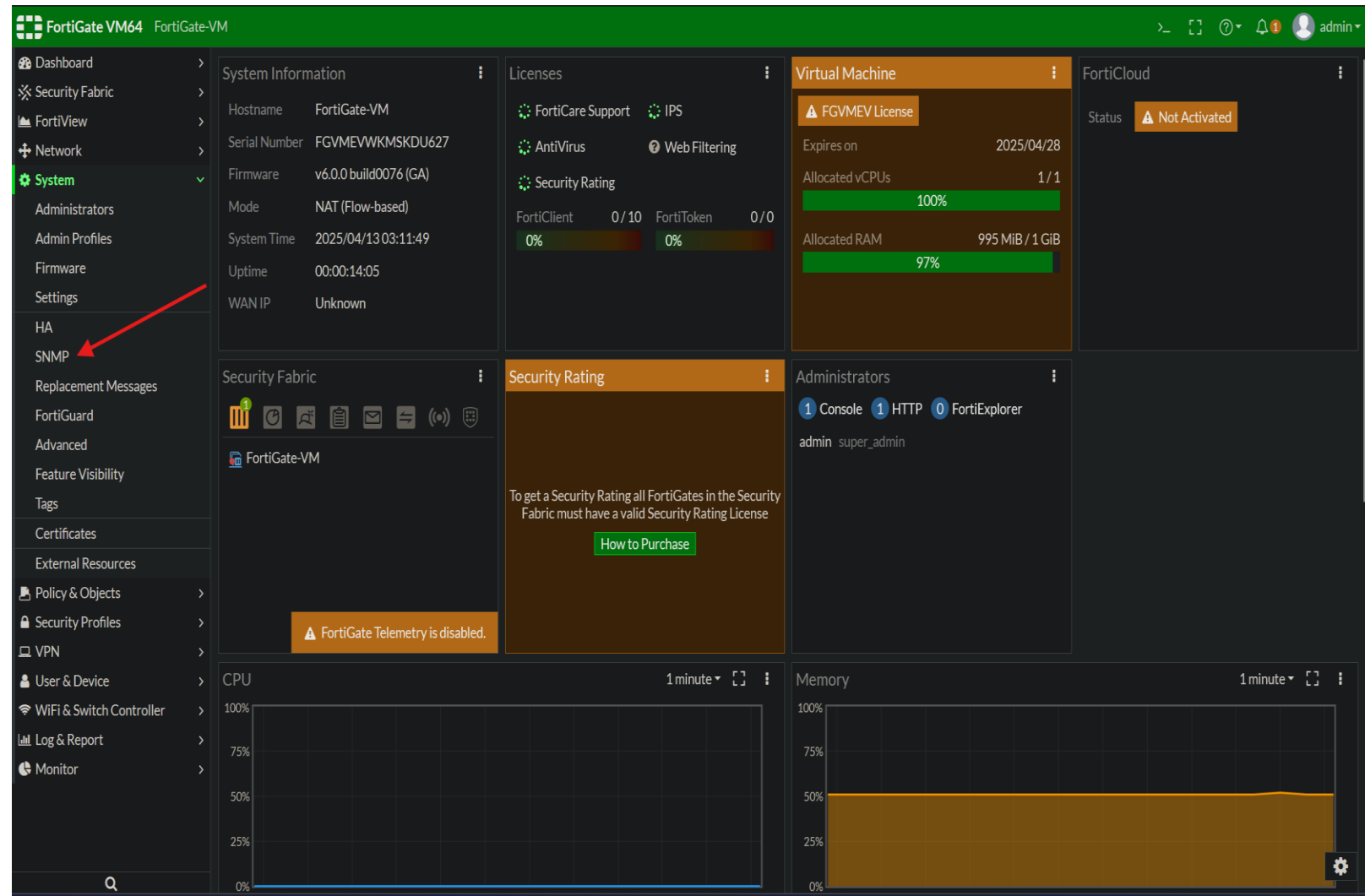


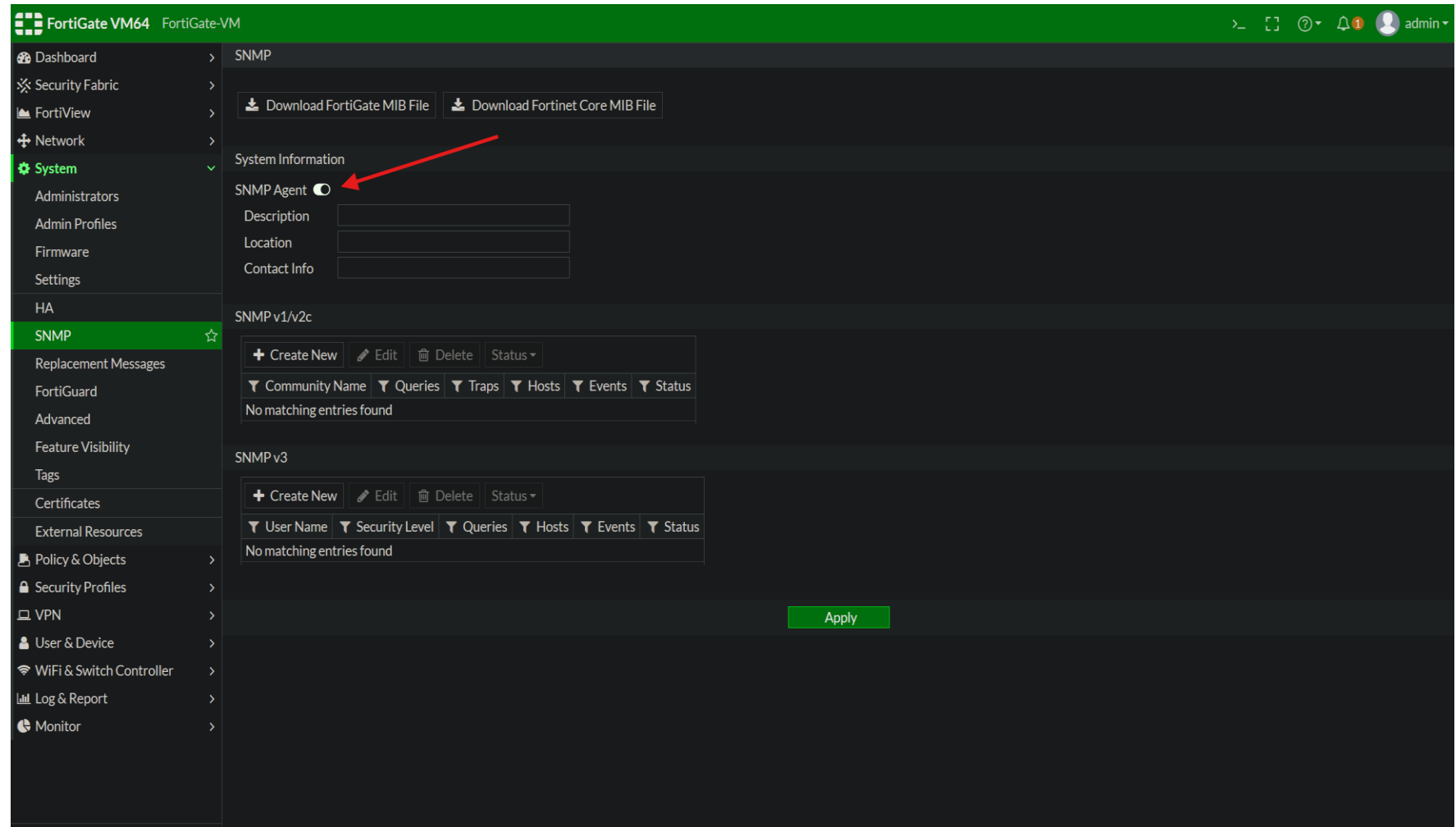


# **Integrating Fortinet Firewall with PRTG: Step-by-Step Guide + Ping Sensor Setup**

1. Log in to the Fortinet firewall and navigate to the SNMP tab



## 2. Enable SNMP agent



The screenshot displays the FortiGate VM64 configuration interface. The left sidebar shows the navigation menu with 'System' expanded and 'SNMP' selected. The main content area shows the SNMP configuration page. A red arrow points to the 'SNMP Agent' toggle, which is currently disabled. Below the toggle are fields for 'Description', 'Location', and 'Contact Info'. The 'SNMP v1/v2c' section shows a table with columns for 'Community Name', 'Queries', 'Traps', 'Hosts', 'Events', and 'Status', and a message 'No matching entries found'. The 'SNMP v3' section also shows a table with columns for 'User Name', 'Security Level', 'Queries', 'Hosts', 'Events', and 'Status', and a message 'No matching entries found'. An 'Apply' button is visible at the bottom right.

FortiGate VM64 FortiGate-VM

Dashboard > Security Fabric > FortiView > Network > **System** > Administrators > Admin Profiles > Firmware > Settings > HA > **SNMP** > Replacement Messages > FortiGuard > Advanced > Feature Visibility > Tags > Certificates > External Resources > Policy & Objects > Security Profiles > VPN > User & Device > WiFi & Switch Controller > Log & Report > Monitor >

SNMP

Download FortiGate MIB File Download Fortinet Core MIB File

System Information

SNMP Agent ☐ Description Location Contact Info

SNMP v1/v2c

+ Create New Edit Delete Status

Community Name Queries Traps Hosts Events Status

No matching entries found

SNMP v3

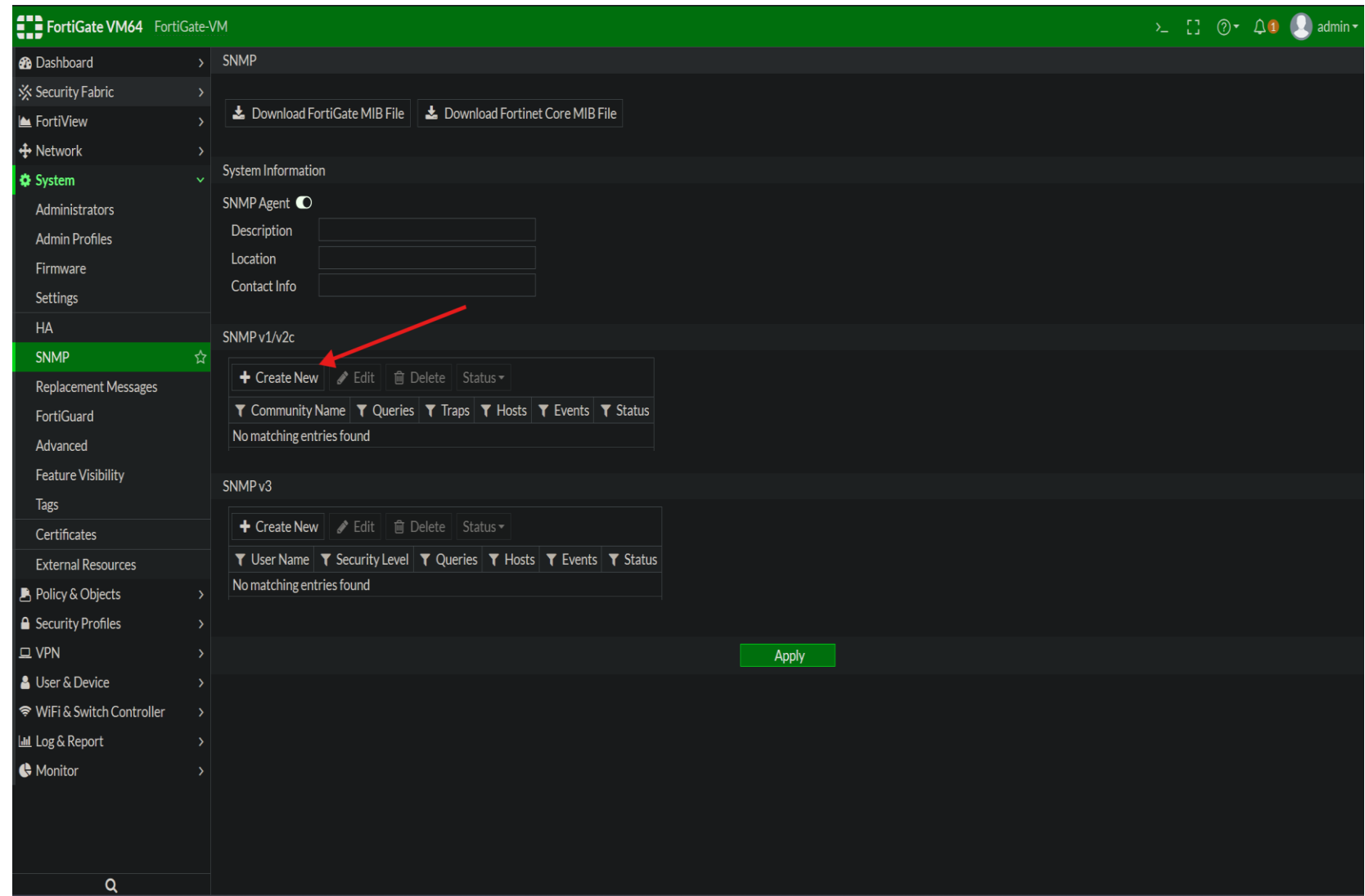
+ Create New Edit Delete Status

User Name Security Level Queries Hosts Events Status

No matching entries found

Apply

### 3. Click on 'Create New' button



The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'System' selected and 'SNMP' highlighted. The main content area is titled 'SNMP' and includes a green header bar. Below the header, there are two download buttons: 'Download FortiGate MIB File' and 'Download Fortinet Core MIB File'. The 'System Information' section contains fields for 'SNMP Agent' (a toggle switch), 'Description', 'Location', and 'Contact Info'. The 'SNMP v1/v2c' section features a '+ Create New' button, which is pointed to by a red arrow, along with 'Edit', 'Delete', and 'Status' buttons. Below these buttons are tabs for 'Community Name', 'Queries', 'Traps', 'Hosts', 'Events', and 'Status'. The 'Community Name' tab is active, showing 'No matching entries found'. The 'SNMP v3' section also has a '+ Create New' button and tabs for 'User Name', 'Security Level', 'Queries', 'Hosts', 'Events', and 'Status', also showing 'No matching entries found'. An 'Apply' button is located at the bottom right of the page.

4. Type the community name and PRTG server IP address

FortiGate VM64 FortiGate-VM

Dashboard > Security Fabric > FortiView > Network > System > Administrators > Admin Profiles > Firmware > Settings > HA > **SNMP** > Replacement Messages > FortiGuard > Advanced > Feature Visibility > Tags > Certificates > External Resources > Policy & Objects > Security Profiles > VPN > User & Device > WiFi & Switch Controller > Log & Report > Monitor >

SNMP

Download FortiGate MIB File Download Fortinet Core

System Information

SNMP Agent ☐

Description

Location

Contact Info

SNMP v1/v2c

+ Create New Edit Delete Status

Community Name Queries Traps Hosts Events

No matching entries found

SNMP v3

+ Create New Edit Delete Status

User Name Security Level Queries Hosts Events

No matching entries found

New SNMP Community

Community Name

Enabled ☐

Hosts

IP Address

Host Type

Queries

v1 Enabled ☐

Port

v2c Enabled ☐

Port

Traps

v1 Enabled ☐

Local Port

Remote Port

v2c Enabled ☐

Local Port

Remote Port

SNMP Events

CPU usage too high ☐

Available memory is low ☐

Available log space is low ☐

Interface IP address changed ☐

VPN tunnel is up ☐

OK Cancel

5. Click OK

FortiGate VM64 FortiGate-VM

Dashboard > Security Fabric > FortiView > Network > **System** > Administrators > Admin Profiles > Firmware > Settings > HA > **SNMP** > Replacement Messages > FortiGuard > Advanced > Feature Visibility > Tags > Certificates > External Resources > Policy & Objects > Security Profiles > VPN > User & Device > WiFi & Switch Controller > Log & Report > Monitor >

SNMP

Download FortiGate MIB File Download Fortinet Core

System Information

SNMP Agent ☐

Description

Location

Contact Info

SNMP v1/v2c

+ Create New Edit Delete Status

Community Name Queries Traps Hosts Events

No matching entries found

SNMP v3

+ Create New Edit Delete Status

User Name Security Level Queries Hosts Events

No matching entries found

New SNMP Community

Community Name

Enabled ☒

Hosts

IP Address

Host Type

Queries

v1 Enabled ☒

Port

v2c Enabled ☒

Port

Traps

v1 Enabled ☒

Local Port

Remote Port

v2c Enabled ☒

Local Port

Remote Port

SNMP Events

CPU usage too high ☒

Available memory is low ☒

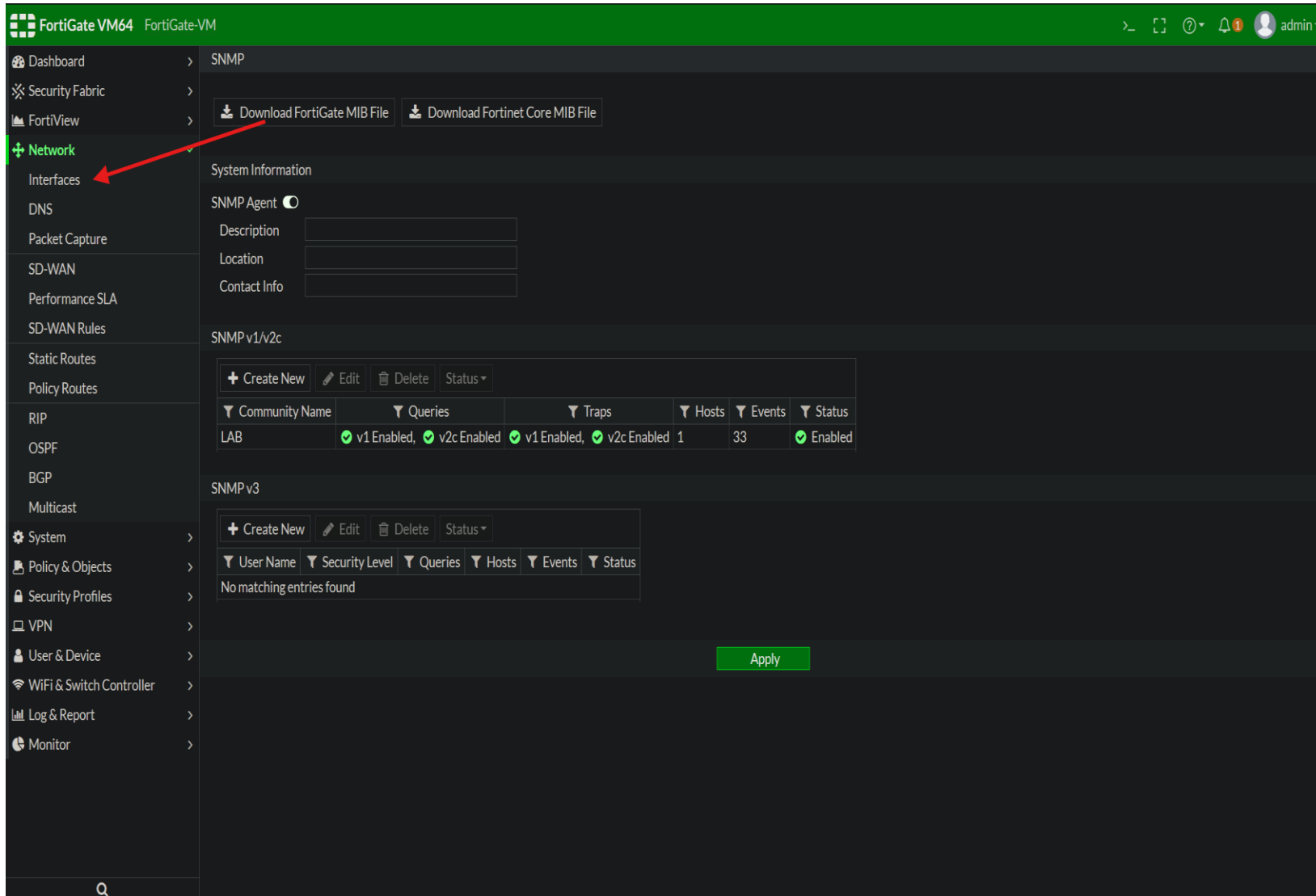
Available log space is low ☒

Interface IP address changed ☒

VPN tunnel is up ☒

OK Cancel

## 6. Navigate to the *Interface* tab



The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with the 'Network' section expanded. A red arrow points to the 'Interfaces' tab. The main content area shows the 'SNMP' configuration page. The 'System Information' section includes fields for 'Description', 'Location', and 'Contact Info'. The 'SNMP v1/v2c' section shows a table with one entry for 'LAB'. The 'SNMP v3' section shows no matching entries found. An 'Apply' button is visible at the bottom right.

FortiGate VM64 FortiGate-VM

Dashboard > Security Fabric > FortiView > **Network** > Interfaces > DNS > Packet Capture > SD-WAN > Performance SLA > SD-WAN Rules > Static Routes > Policy Routes > RIP > OSPF > BGP > Multicast > System > Policy & Objects > Security Profiles > VPN > User & Device > WiFi & Switch Controller > Log & Report > Monitor >

SNMP

Download FortiGate MIB File Download Fortinet Core MIB File

System Information

SNMP Agent ☐

Description

Location

Contact Info

SNMP v1/v2c

+ Create New Edit Delete Status

Community Name	Queries	Traps	Hosts	Events	Status
LAB	✓ v1 Enabled, ✓ v2c Enabled	✓ v1 Enabled, ✓ v2c Enabled	1	33	✓ Enabled

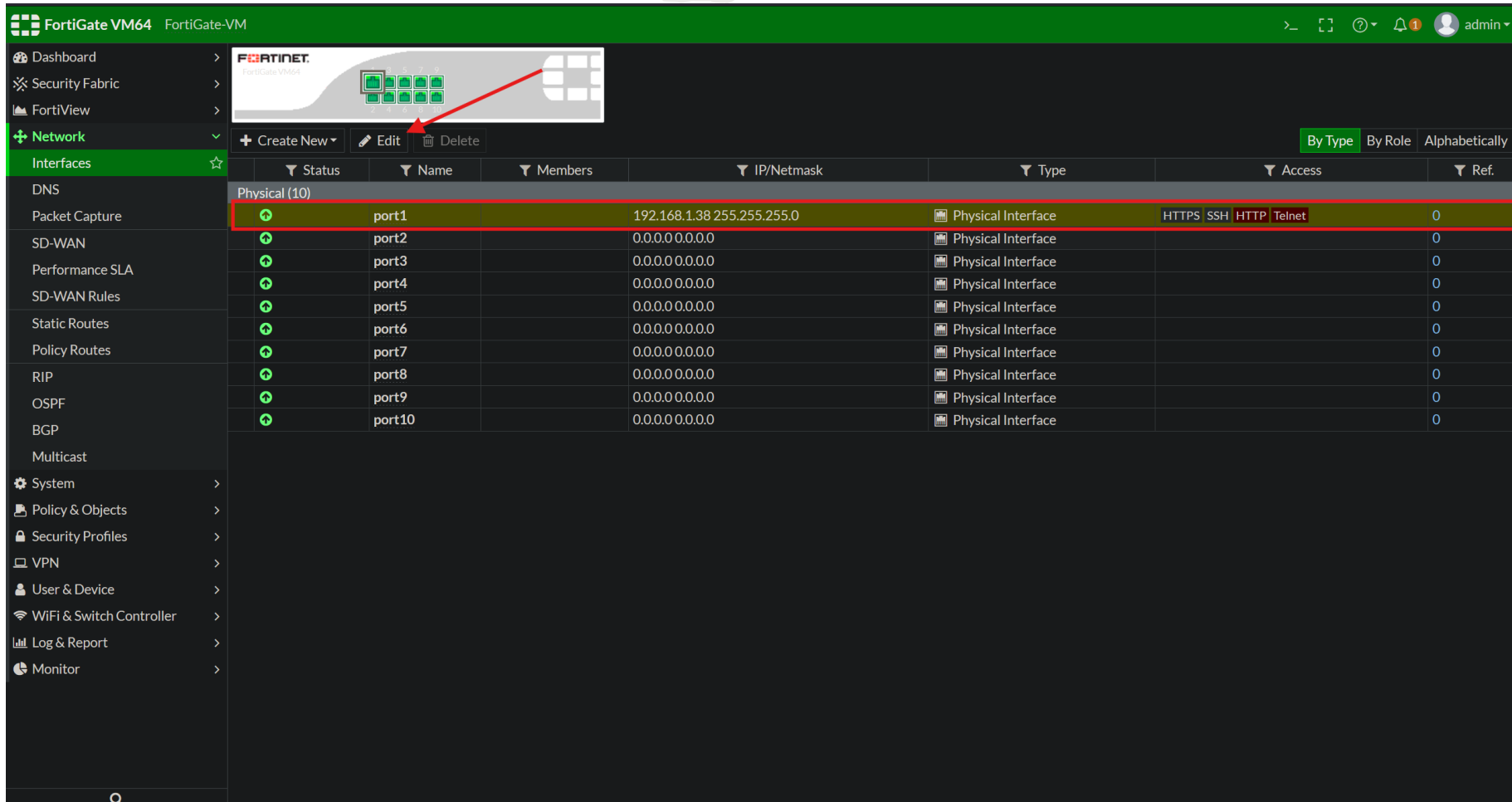
SNMP v3

+ Create New Edit Delete Status

User Name	Security Level	Queries	Hosts	Events	Status
No matching entries found					

Apply

## 7. Select Port 1 on the firewall, then click on the *Edit* button

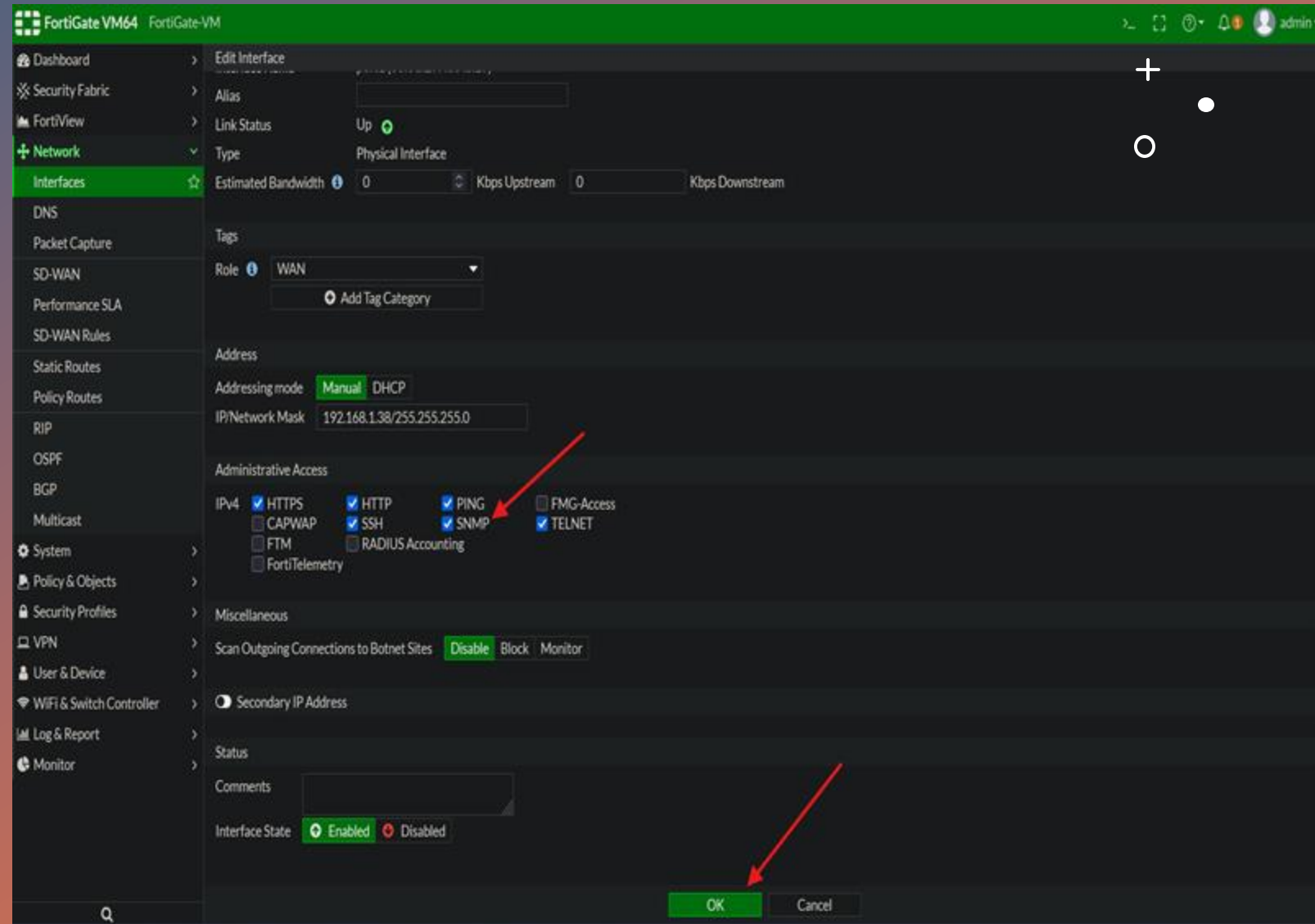


The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'Network' expanded and 'Interfaces' selected. The main content area shows a table of physical interfaces. The first row, 'port1', is highlighted with a red box. Above the table, the 'Edit' button is highlighted with a red arrow.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
+	port1		192.168.1.38 255.255.255.0	Physical Interface	HTTPS SSH HTTP Telnet	0
+	port2		0.0.0.0 0.0.0.0	Physical Interface		0
+	port3		0.0.0.0 0.0.0.0	Physical Interface		0
+	port4		0.0.0.0 0.0.0.0	Physical Interface		0
+	port5		0.0.0.0 0.0.0.0	Physical Interface		0
+	port6		0.0.0.0 0.0.0.0	Physical Interface		0
+	port7		0.0.0.0 0.0.0.0	Physical Interface		0
+	port8		0.0.0.0 0.0.0.0	Physical Interface		0
+	port9		0.0.0.0 0.0.0.0	Physical Interface		0
+	port10		0.0.0.0 0.0.0.0	Physical Interface		0



8. Enable  
SNMP, then  
click the  
*OK* button.



9. Log in to the PRTG tool, go to the *Devices* tab, and click on *Add Device*.

The screenshot displays the PRTG Network Monitor web interface. The top navigation bar includes tabs for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. The 'Devices' tab is active, showing a tree view of the network hierarchy under 'Group Root'. The tree includes categories like Local Probe, Network Discovery, Network Infrastructure, Internet, Firewall, Router, Windows, Servers, and Monitoring SVR. A red arrow points to the 'Add Device' link next to the 'Firewall' category. The right sidebar contains a 'Find out how to make the most of your PRTG experience.' section with a 'MASTER YOUR TRIAL' button, a status summary (Status: OK, Default Interval: 60 seconds, ID: #0), an 'Add Sensor' button, a world map, and a 2-day performance graph. The bottom status bar shows the user 'PAESSLER' with IP '25.1.104.1961+' and the role 'PRTG System Administrator'. The system clock indicates 2:24 PM on 4/13/2025.

10. Enter the device name and the IP address of the firewall.

← → ↻ Not secure https://127.0.0.1/group.htm?id=0&tabid=1

Home Devices Libraries

Devices

Group Root

Overview 2 days 30 days

10 W 5 ✓ 52 (of 67) S M L XL

Root

- Local Probe
  - Probe Device IP
- Network Discovery
  - Network Infrastructure
    - DNS/Gateway/DHCP mysgon IP
    - Internet IP
    - Firewall Add Device
  - Network Infrastructure
    - DNS/Gateway/DHCP mysgon IP
    - Router
      - Microsoft router IP
  - Windows
    - Clients Add Device
    - Servers
      - SRV-SOLARWIND IP
      - Monitoring SVR IP
  - Windows
    - Clients Add Device

PAESSLER 25.1.104.1961+ PRTG System Administrator 2:33 Refresh in 22 sec

### Add Device to Group Firewall

**Add a New Device**  
Define a device name and IP address, options for auto-discovery, and credential settings for Windows, Linux, VMware/XenServer, SNMP, and specific vendors, if necessary.  
PRTG Manual: Add a Device

**Basic Device Settings**

Device Name ⓘ  
Fortinet

IP Version ⓘ  
☒ IPv4 (default)  
☐ IPv6

IPv4 Address/DNS Name ⓘ  
192.168.1.38

Tags ⓘ  
+

**Additional Device Information**

Device Icon ⓘ

Cancel OK

11. Enter the community string and Click on ok button.

← → ↻ Not secure https://127.0.0.1/group.htm?id=0&tabid=1

Home Devices Libraries

Devices

Group Root

Overview 2 days 30 days

10 W 5 ✓ 52 (of 67) 3 M L XL

Root

- Local Probe
  - Probe Device
- Network Discovery
  - Network Infrastructure
    - DNS/Gateway/DHCP/mysgon
  - Internet
  - Firewall
- Network Infrastructures
  - DNS/Gateway/DHCP/mysgon
- Router
  - Microtik router
- Windows
  - Clients
- Servers
  - SRV/SOLARWIND
  - Monitoring SVR
- Windows
  - Clients

Add Device

### Add Device to Group Firewall

☐ inherit from Firewall (SNMP Version: V2, SNMP Port: 161, Timeout (Se...)

SNMP Version ⓘ

☐ SNMP v1

☒ SNMP v2c (default)

☐ SNMP v3

Community String (SNMP v2c) ⓘ

LAB

SNMP Port ⓘ

161

Timeout (Sec.) ⓘ

5

Credentials for Database Management Systems

☒ inherit from Firewall (Timeout (Sec.): 60 seconds)

Credentials for AWS

☒ inherit from Firewall

Cancel OK

PAFSSI ER

2 days

Max: 25.21

Min: 1.11

11. Click on  
the *Add  
Sensor*  
button.

← → ↻ Not secure https://127.0.0.1/group.htm?id=0&tabid=1

New Alarms 1 New Log Entries 24 !! 10 W 5 ✓ 52 Search...

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

Devices

Group Root

Overview 2 days 30 days 365 days Alarms Log Management Settings Notification Triggers Comments History

!! 10 W 5 ✓ 52 (of 67) S M L XL Search...

Root

- Local Probe
  - Probe Device ✓ 5 Sens...
- Network Discovery
  - Network Infrastructure
    - DNS/Gateway/DHCP: mygpon !! DNS v2 W SSL Ce... ✓ 2 Sens...
    - Internet ✓ HTTP
    - Firewall Fortinet Add Sensor Run Auto-Discovery
  - Network Infrastructure
    - DNS/Gateway/DHCP: mygpon !! DNS v2 W SSL Ce... ✓ 2 Sens...
    - Router Mikrotik router !! SNMP ...
  - Windows
    - Clients Add Device
    - Servers
      - SRV-SOLARWIND !! HTTP (... ✓ 4 Sens...
      - Monitoring SVR !! Windo... !! SNMP ... W 2 Sens... ✓ 17 Sens...
    - Windows Clients Add Device

We feel like there is a right license waiting just for you.

CONTINUE PRTG JOURNEY

Status: OK  
Default Interval: 60 seconds  
ID: #0

Add Sensor

2 days

PAESSLER 25.1.104.1961+ PRTG System Administrator 2:35 Refresh in 19 sec Contact Support ? Help

13. Select 'PING' as the technology used, and choose the Ping sensor.

The screenshot shows the PRTG Network Manager web interface for adding a new sensor. The breadcrumb trail indicates the path: Home > Devices > Local Probe > Network Discovery > Network Infrastr... > Firewall > Fortinet > Add Sensor (Step 1 of 2). The main heading is "Add Sensor to Device Fortinet [192.168.1.38] (Step 1 of 2)".

The configuration is divided into three columns:

- Monitor What?**
  - ☐ Availability/Uptime
  - ☐ Bandwidth/Traffic
  - ☐ Speed/Performance
  - ☐ CPU Usage
  - ☐ Disk Usage
  - ☐ Memory Usage
  - ☐ Hardware Parameters
  - ☐ Network Infrastructure
  - ☐ Custom Sensors
- Target System Type?**
  - ☐ Windows
  - ☐ Linux/macOS
  - ☐ Virtualization OS
  - ☐ Storage and File Server
  - ☐ Email Server
  - ☐ Database
  - ☐ Cloud Services
- Technology Used?**
  - ☒ Ping (highlighted with a red box)
  - ☐ Packet Sniffing
  - ☐ Flow Protocols
  - ☐ PowerShell
  - ☐ Push Message Receiver
  - ☐ PRTG Cloud
  - ☐ SNMP
  - ☐ WMI
  - ☐ Performance Counters
  - ☐ HTTP
  - ☐ SSH

Below the configuration section, there is a search bar with the text "Search Type to search for a name or description" and "9 Matching Sensor Types". Under "Most Used Sensor Types", the "Ping" sensor is listed with a description: "Monitors connectivity using ping" and "Shows if a device is reachable through the network using ping requests." A red arrow points to the "+" icon next to the "Ping" sensor card.

The footer of the interface shows the user "PAESSLER" with IP "25.1.104.1961+", role "PRTG System Administrator", and a refresh timer of "2:45". There are also links for "Contact Support" and "Help".

14. Click the  
*Create* button

← → ↻ Not secure https://127.0.0.1/addsensor4.htm?id=2172&tmpid=10 ☆ ⓘ ⋮

New Alarms 3 New Log Entries 194 !! 10 W 7 ✓ 50 Search... 🔍 ⏻

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

Devices Local Probe ▾ Network Discovery ▾ Network Infrast... ▾ Firewall ▾ Fortinet Add Sensor (Step 2 of 2)

### Add Sensor to Device Fortinet [192.168.1.38] (Step 2 of 2)

< Cancel

#### Basic Sensor Settings

Sensor Name ⓘ Ping

Parent Tags ⓘ

Tags ⓘ pingsensor x +

Priority ⓘ ★★☆☆☆

Create 📄

#### Ping Settings

Timeout (Sec.) ⓘ 5

Packet Size (Bytes) ⓘ 32

Ping Method ⓘ  
☐ Send one single ping  
☒ Send multiple ping requests (default)

Ping Count ⓘ 5

Ping Delay (ms) ⓘ 5

Acknowledge Automatically ⓘ  
☒ Show down status on error (default)  
☐ Show down (acknowledged) status on error

PAESSLER 25.1.104.1961+ PRTG System Administrator 2:46 || Refresh in 26 sec Contact Support ? Help

# 15. The Ping sensor is now successfully added

← → ↻ Not secure https://127.0.0.1/device.htm?id=2172&tabid=1#

New Alarms 3 New Log Entries 202 !! 10 W 7 ✓ 51 Search...

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

Devices Local Probe Network Discovery Network Infrast... Firewall Fortinet

Device Fortinet ★★★★★

Overview 2 days 30 days 365 days Alarms System Information Log Settings Notification Triggers Comments History

✓ Ping OK

Ping Time 0 msec 0 msec 1 msec

Find out how to make the most of your PRTG experience.

MASTER YOUR TRIAL

Status: OK

Sensors: ✓ 1 (of 1)

DNS Name/IP Address: 192.168.1.38

Dependency: Parent

Default Interval: 60 seconds

Last Auto-Discovery: (never)

Last Recommendation: 7 minutes ago

ID: #2172

Add Sensor

Recommended Sensors

Priority	Sensors	Total Sensors	Links
★★★★★	1×Ping	1	Add These Sensors

PAESSLER 25.1.104.1961+ PRTG System Administrator 2:47 Refresh in 27 sec Contact Support ? Help



Thanks for  
your time  
and  
attention!