



# **Network Passive Sensor**

## Physical Appliance User Guide

November 24, 2023

Copyright 2022-23 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.  
919 E Hillsdale Blvd  
4th Floor  
Foster City, CA 94404  
1 (650) 801 6100



# Table of Contents

<b>About this Guide .....</b>	<b>4</b>
<b>Welcome to Qualys Network Passive Sensor .....</b>	<b>5</b>
Get Started .....	8
Configuring Appliance and Registering to Qualys Cloud Platform .....	8
Manage Sensors .....	18
Configure Assets .....	20
<b>Intranet Scanner Tour .....</b>	<b>27</b>
A Quick Look at the Appliance (1Gbps (QPS-01G-0100-A0) .....	28
Navigating the Appliance UI .....	29
System Reboot and Shutdown .....	34
Configure Static IP Address .....	34
Proxy Configuration .....	37
<b>Troubleshooting .....</b>	<b>43</b>
How can I test network connectivity? .....	43
Need the model number or serial number for your appliance? .....	43
Communication Failure message .....	44
Appliance Configuration Errors .....	44
<b>Appendix A- Product Specifications.....</b>	<b>46</b>
<b>Appendix B - Software Credits.....</b>	<b>55</b>
<b>Appendix C - Safety Notices.....</b>	<b>56</b>
<b>Appendix D- Extending the Network Feature .....</b>	<b>57</b>
<b>Appendix E- Classification of Assets in Passive Sensor .....</b>	<b>59</b>
<b>Best Practices .....</b>	<b>65</b>

# About this Guide

This user guide introduces the Qualys Network Passive Sensor and will help you with setting up the physical sensor to detect known and unknown devices on your network.

Note: Your use of the Qualys Network Passive Sensor physical sensor appliance is subject to the terms and conditions of the Qualys Service User Agreement.

## About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the [Cloud Security Alliance \(CSA\)](#).

For more information, please visit [www.qualys.com](http://www.qualys.com).

## Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at [www.qualys.com/support/](http://www.qualys.com/support/).

# Welcome to Qualys Network Passive Sensor

With Qualys Network Passive Sensor (PS), you can automatically detect, and profile devices connected to your network, eliminating blind spots across your IT environment. Network Passive Sensor monitors network activity without any active probing of devices in order to detect active assets in your network.

Network Passive Sensor is available in five models - 1 Gbps (QPS-01G-0100-A0), 4Gbps (QPS-04G- 0402-B0), 10 Gbps (QPS-10G-0404-B1), 100 Mbps (QPS-01M-0500-D1), 100 Mbps QPS-01M-0600-B2

It's easy to set up a Network Passive Sensor appliance within your network. Let's get started!

## Check Package Accessories

Depending on the appliance variant you choose, starter kit package contains components. If any components are missing or damaged, please contact Qualys Support.

The following are the Passive Sensor appliance models along with packing lists:

### 1Gbps (QPS-01G-0100-A0)

---

AC Power Cord

---

CAT6 Cable

---

Rack Screws (quantity 4) - 10-32 x 3/4"

---

USB-to-RS232 Converter Cable

---

**Important:** For the 1Gbps (QPS-01G-0100-A0) appliance, use only the USB-RS232 converter cable shipped with the appliance.

### 4Gbps (QPS-04G- 0402-B0)

---

Rack Mount Slide Rail Set

---

2 x Power Cords

---

Accessory box which contains:

- 1x USB-RJ45 console cable
  - 1x DB9-RJ45 console cable
  - 1x rack mount screw set/ ear bracket screw set/SSD screw set
  - 1x slide rail screw pack
  - 1x SATA cable and SATA power cable set
  - 1x crossover LAN cable (red)
  - 1x SFP+ transceiver
-

**10Gbps (QPS-10G-0404-B1)**


---

QPS-10G-0404-B1(10Gbps Hardware Appliance)

---



---

Rack Mount Slide Rail Set

---



---

2 x Power Cords

---



---

Accessory box which contains:

- 1x USB-RJ45 console cable
  - 1x DB9-RJ45 console cable
  - 1x rack mount screw set/ ear bracket screw set/SSD screw set
  - 1x slide rail screw pack
  - 1x SATA cable and SATA power cable set
  - 1x crossover LAN cable (red)
  - 1x straight LAN cable (gray)
  - 1x SFP+ transceiver
- 

**100Mbps (QPS-01M-0500-D1)**


---

QPS-01M-0500-D1(100Mbps Hardware Appliance)

---



---

USB-RJ45 Console Cable

---



---

Power Adapter

---



---

Power Cord

---



---

Rack Mount Kit

---



---

Wall Mount Kit

---



---

Mounting Screws

---

**Note:** The following are supported SFP's for PS appliance Models -- QPS-04G- 0402-B0, QPS-10G-0404-B1.

- Finisar FTLX1475D3BCL (Single Mode Long range (10km))
- Finisar FTLX8574D3BCL (Multimode Short range)

**100Mbps (QPS-01M-0600-B2)**


---

QPS-01M-0600-B2 (100Mbps Hardware Appliance)

---



---

USB-DB9(F) Console Cable

---



---

1 x Ear Bracket

---



---

4 x Ear Bracket Screws

---



---

1 x Power Terminal Block Plug

---

The following are supported SFP's for PS appliance Model QPS-01M-0600-B2.

Brand	MPN	Speed	Type	Operation/Temperature	Type
FINISAR	FTLF1318P3BTL	1Gb Longwave	Single mode(10km)	-40°C to 85°C	SFP
FORMERICA	TSD-S2CA1-F11	1Gb Longwave	Single mode(10km)	-40°C to 85°C	SFP
FINISAR	FTLF8519P3BNL	1Gb Shortwave	Multi mode	-40°C to 85°C	SFP
FORMERICA	TSD-S2CH1-C11	1Gb Shortwave	Multi mode	-40°C to 85°C	SFP
FINISAR	FCLF8522P2BTL	1Gb Optic to RJ-45	N/A	-40°C to 85°C	SFP to RJ-45
FORMERICA	TCP-S2BC1-A1M	1Gb Optic to RJ-45	N/A	-40°C to 85°C	SFP to RJ-45

**Note:** SFPs are not **hot** swappable for PS appliance Model QPS-01M-0600-B2.

## Network Prerequisites

Make sure that your network follows the prerequisites mentioned in the below table:

Bandwidth	Minimum recommended bandwidth connection of 1 Megabits per second (Mbps) to the Qualys Cloud Platform for a network containing around 10,000 assets.
Appliance Access	The Network Passive Sensor must be able to reach certain infrastructure located on the Qualys Cloud Platform where your Qualys account is located. The local network must be configured to allow outbound HTTPS and WebSocket (port 443) access to the Internet, so that the Network Passive Sensor can communicate with the Qualys Cloud Platform. <b>Tip - Log into your account and go to Help &gt; About to see the Qualys Cloud Platform URLs.</b>
DHCP or Static IP	By default the Intranet Scanner is pre-configured with DHCP. If configured with a static IP address, be sure you have the IP address, netmask, default gateway and primary DNS.
Proxy Support	The Intranet Scanner includes Proxy support with or without authentication. Proxy-level termination (as implemented in SSL bridging, for example) is not supported. SOCKS proxies are not supported.

## Get Started

Once you complete the setup, the Network Passive Sensor will start discovering assets on your network. It takes just a couple of minutes. It's important that you complete the steps in the order shown. As per your appliance variant, you can configure your appliance using LCD or using dialogue menu.

### Before you Begin - Mirror the Traffic

You need to feed traffic to the sensor by mirroring the traffic (using physical tap or mirror port). Connect the mirrored port to the sniffing interface of the sensor. This step is required in order to see discovered assets.

Network Passive Sensor supports mirror traffic of SPAN, RSPAN, and ERSPAN methods. For more information, refer to the [Deployment Guide](#).

## Configuring Appliance and Registering to Qualys Cloud Platform

### Step 1 - Generate the Personalization Code

You'll get a personalization code from the Network Passive Sensor application.

- 1) Log in to the Qualys UI and select **Network Passive Sensor** from the app picker.
- 2) On the **Sensors** tab, go to **New Sensor > Physical Sensor**. (Similarly, you can go to the registration step directly from **Home > Deploy Network Sensor > Physical Sensor > Deploy**).
- 3) Provide information in the Sensor Details section and then click the **Generate Code** button in the Personalization Code section. **Copy the code and keep it handy. You'll need it later.** Steps on how to personalize the sensor will appear on the screen.



**Qualys Express**

← New Physical Sensor

STEPS 1/3

- 1 Register Sensor
- 2 Network
- 3 General Settings

### Register Sensor

To register your sensor with the Qualys Cloud Platform, provide the Sensor details and generate a Personalization Code. You'll enter this code in the physical sensor console to personalize the sensor.

**Sensor Details**

Sensor Name \*  
TB\_N

Deployment Location  
Pune

**Personalization Code**

Generate a unique personalization code used to activate your sensor. Please note, every time you generate a code one of your license is consumed.

Generate Code 70192264604618 Copy

Would you like to start sensing as soon as license is registered? ☐ YES ☒ NO

Follow these steps to register your sensor device using the personalization code. This is a one-time mandatory step that must be done before using the passive sensor device.

**Personalize this sensor**

Enter the generated code into the sensor dialog box and click submit.

**Personalize This Sensor**

Enter the 14 digit Personalization Code:

12345678912345

Submit Cancel

You will get a message once the appliance is successfully registered with Qualys Cloud Platform.

**Appliance registration completed successfully.**

OK

Cancel Next

4) Click **Next** to go to the **Network** screen.

Here, you can define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges or use customized IP ranges. Select **Do you want to Inventory the assets?** check box for marking inventoried assets. You can able to apply existing tags to these assets.

**Note:** To view the detailed explanation on the **Network Feature**, refer to the [Appendix D- Extending the Network Feature](#) section.

To configure internal, external and excluded type of assets, refer to the [Configure Assets](#) section.

The screenshot shows the 'New Physical Sensor' configuration page in Qualys Express, specifically the 'Network' step (Step 2/3). The left sidebar shows the progress: 1. Register Sensor, 2. Network (current), and 3. General Settings. The main content area is titled 'Network' and includes instructions: 'Associate the sensor with the Network in which it is deployed. You will need to specify the Network to Sensor association if you want the sensor to uniquely identify assets in overlapping IP address space. [Learn More](#)'. The configuration fields include: 'Internal Asset Group/Network' with a name input field containing 'PS\_06\_group'; a question 'Do you want to inventory the assets?' with radio buttons for 'Yes' and 'No' (selected); 'Internal Asset IP Range' with a dropdown menu set to 'Default IP Ranges'; a list of selected IP ranges: '192.168.0.0/16', '172.16.0.0/12', and '10.0.0.0/8'; and a 'Type' dropdown menu set to 'DHCP'. At the bottom, there is a '+ Add Another' link and three buttons: 'Cancel', 'Previous', and 'Next'.

5) Click **Next** to go to the **General Settings** screen.

Follow on-screen instructions for your module activation and enable Qualys to collect support logs for troubleshooting.

6) Click **Save** to complete the registration.

The screenshot shows the 'New Physical Sensor' configuration page in Qualys Express, specifically the 'General Settings' step (Step 3/3). The left sidebar shows the progress: 1. Register Sensor, 2. Network, and 3. General Settings (current). The main content area is titled 'General Settings' and includes instructions: 'Configure General settings for your sensor on the virtual sensor console. Scroll through the instructions on the screen for help.' The configuration fields include: 'Module Activation' with a toggle switch for 'VMDR OT' (labeled 'Enable sensor for VMDR OT' and 'Discover OT Devices and add them to your inventory') which is currently turned off; and 'Enable Qualys to collect support logs for troubleshooting' with a toggle switch which is currently turned off. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Save'.

## Step 2 - Connect the Appliance to the Network

The Network Passive Sensor connects like any other computer to a switch on your network. To set up the network connection, follow these steps:

- 1) Connect one end of an Ethernet cable to the Ethernet LAN port on the Intranet Scanner (back panel).
- 2) Connect the other end of the Ethernet cable to a 10BASE-T or 100BASE-TX or 1 Gigabit switch on your network.

### Step 3 - Power On the Appliance

To power on the appliance, follow these steps:

- 1) Connect the AC power cord into the Power Supply Socket.

**Note** - Qualys strongly recommends the appliance be plugged into a Managed Power Supply. On the rare occasion where the appliance may need to be rebooted, utilizing the MPS will allow for remote rebooting in unmanned or high security areas.

- 2) Press the power button on the back panel. Be sure that the power indicator has turned green.

### Step 4 - Complete the Network Configuration Using LCD Keypad (Applicable for QPS-01G-0100-A0)

- 3) The **Welcome to Qualys** message appears in the LCD interface followed by other informational messages during the boot process which takes approximately two minutes.

We recommend having a quick look at how to navigate the appliance UI before making configuration settings. Refer to the [Navigating the Appliance UI](#) section.

Enable network configuration settings for the appliance, as appropriate.

- If the appliance is installed on a network with Static IP and without a Proxy server, you need to configure Static IP. Refer to the [Configure Static IP Address](#) section.
- If the appliance is installed on a network with DHCP and a Proxy server, you need to configure Proxy. Refer to the [Proxy Configuration](#) section.
- If the appliance is installed on a network with Static IP and a Proxy server, you need to configure Static IP and Proxy.
- Keep default configurations if the appliance is installed on a network with DHCP and without proxy.

Any errors must be resolved before continuing to Step 5. Refer to [Troubleshooting](#) for help with resolving any errors.

### Step 5 - Activate the Appliance Using LCD Keypad (Applicable for QPS-01G-0100-A0)

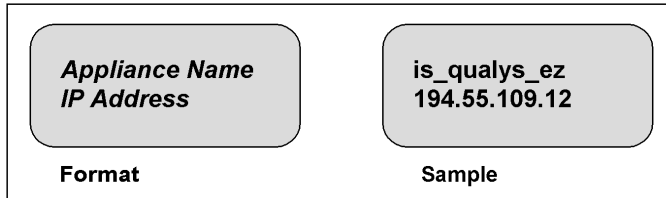
To activate the appliance, follow these steps:

- 1) Select the **REGISTER WITH QUALYS PLATFORM** option on the LCD interface.
- 2) Enter the 14-digit **PERS CODE** which you generated in [Step 1 - Generate the Personalization Code](#). Press **Enter** when prompted **PERS CODE IS CORRECT?**

3) Once activation completes, you'll be prompted to set a 4-digit PASSWORD. Please remember this PASSWORD. You will need to enter it to unlock the configuration menu. If activation fails, you'll see an error message on the LCD interface.

4) The **APPLIANCE NAME-IP ADDRESS** message appears after the appliance successfully connects to the Qualys Cloud Platform. Do you see another message instead? Refer to the [Troubleshooting](#) section for assistance.

The name and IP address appear as shown below.



The name can be changed using the Qualys user interface.

The IP address is available for information purposes only. The Intranet Scanner is remote controlled by the Qualys Cloud Platform, and it does not allow incoming logins or connections from the network.

The Qualys Cloud Platform indicator for your account appears in the lower right corner.

## Step 6 - Setting Remote Console Interface to Configure Appliance Using Serial Port

This section helps user to configure an appliance using dialogue menu. Following are the steps to set up appliance using dialogue menu:

**Prerequisites** - Install latest version of PuTTY.

This step is an alternative method for remote configuration and management of the Intranet Scanner using serial option using Putty on Windows machine.



a) For 4G(QPS-04G-0402-B0), 10G(QPS-10G-0404-B1) & 100 Mbps (QPS-01M-0500-D1) models: Use USB-RJ45 serial console cable provided for console connectivity. Connect the RJ45 end of the cable to the console port (RJ45) on the appliance and the other end to the USB port of the laptop/PC.

b) For 100 Mbps (QPS-01M-0600-B2): Use the USB-RS232(DB9-F) serial console cable provided for console connectivity. Connect the DB9-F end to the com1 port(DB9-M) on the appliance and the other end to the USB port of the laptop/PC.

c) For 1Gbps (QPS-01G-0100-A0): Use USB-RS232(DB9F) converter provided by Qualys. A separate DB9(F) - USB/RJ45 cable is also required (not provided by Qualys). Connect the USB port of the cable to the USB port on the rear side of the appliance, and connect the RS232(DB9F) to the DB9(F) end of the cable. The other end of the cable, USB/RJ45, should be connected to the laptop or terminal server.

Qualys recommends the following USB-to-RS232 converter cable:

IOGEAR USB-Serial Model GUC232A

Full specifications: <http://www.iogear.com/product/GUC232A/>

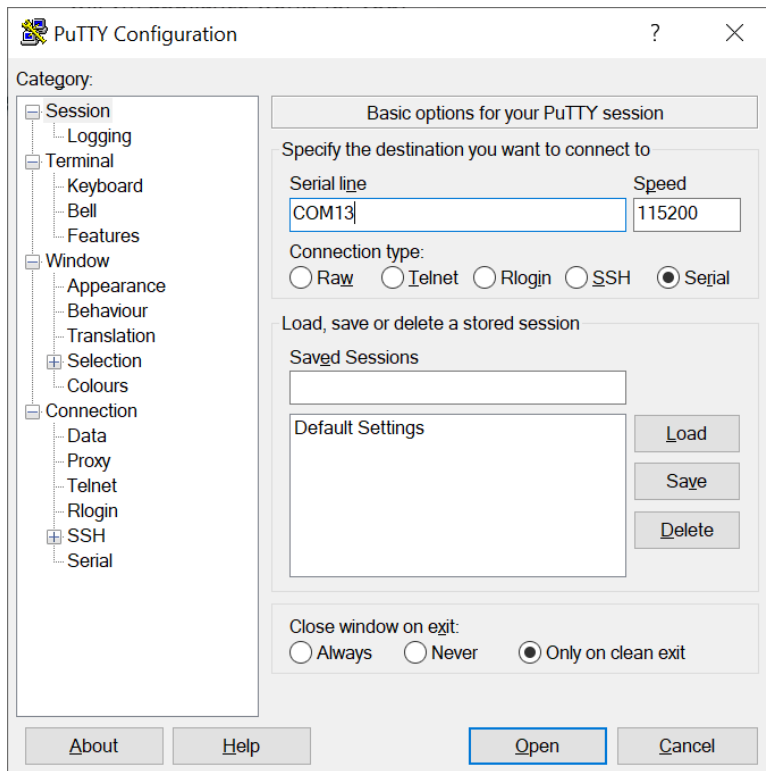
Keystroke File Not Supported: The Remote Console interface is not intended for uploading the whole sensor configuration by means of a pre-defined “keystroke file.” Uploading such a file will result in lost characters and incorrect configuration.

To set up the Remote Console interface, follow these steps:

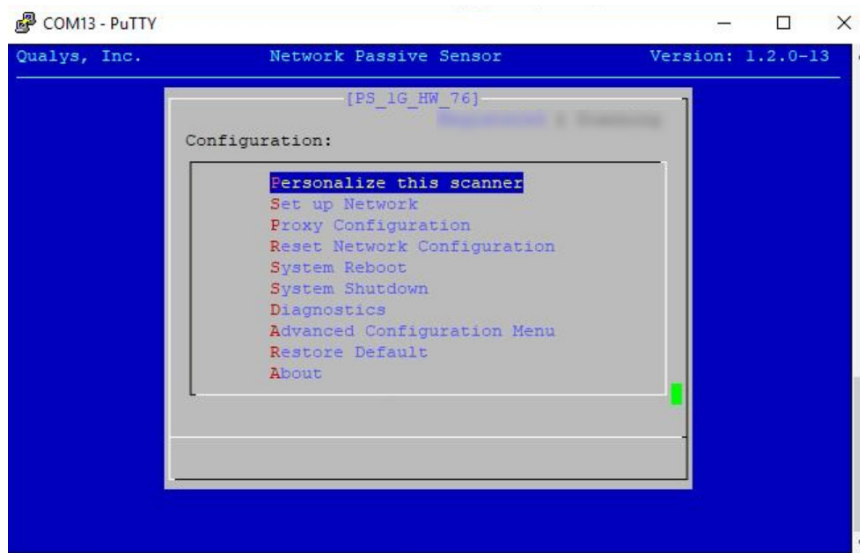
1) Be sure the terminal server is up and running. Also check the terminal server settings. The following settings are required.

Port Setting	Value
Bits per second (Baud rate)	115200
Data Bits	8
Parity	None
Flow Control	None

2) Run PuTTY on your windows machine and mention the Connection type as “Serial”. Provide COM Port Number in the Serial line field and 115200 in the Speed. Click Open to display remote console.



3) On successful connection, you'll see Network Passive Sensor console as shown below.



### Step 7 - Setting up Network Using Remote Console Interface

To enable a static IP address, follow these steps:

- 1) Go to the **Set up Network** menu option and press **Enter** to continue.
- 2) Select **Static IP** option and choose **OK**.
- 3) Provide parameters for Static IP configuration:
  - **IP address** - Enter the static IP address.
  - **Netmask** - Enter the desired netmask value.
  - **Gateway** - Enter the gateway IP address.
  - **DNS1** - Enter the IP address for the primary DNS server.
  - **DNS2** - Enter the IP address for the secondary DNS server. This entry is optional.
- 4) Choose **Submit** and press **Enter**. Wait for some time and you'll see a confirmation message for successful configuration of network settings.

### Step 8 - Proxy Configuration Using Remote Console Interface

If the Intranet Scanner is behind a Proxy server, you need to enable a Proxy configuration using the **Proxy Configuration** menu option. Authentication (Basic) of the Intranet Scanner connection to your Proxy server can be enabled by configuring the Proxy user and password fields.

The Intranet Scanner uses Secure Sockets Layer (SSL) protocol (HTTPS and WebSocket) to secure its connection to the Qualys web application, in a similar way that a web browser does to a secure web server. If the Qualys connection must pass through a Proxy server, then you must enable the Proxy option on the Intranet Scanner. This configuration re-directs Qualys outbound connections through the Proxy server.

Your Proxy server must be configured to tunnel or pass through the SSL session to the Qualys web application. This ensures a secured end-to-end connection. SSL bridging or tunnel termination must not be configured in your Proxy server when supporting the Intranet Scanner.

To configure Proxy support, follow these steps:

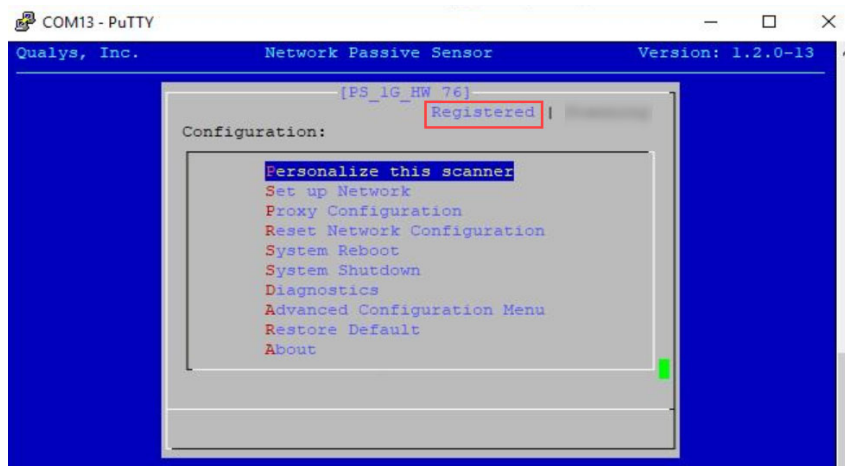
- 1) Go to the **Proxy Configuration** menu option and press **Enter** to continue.
- 2) Select **Enable Proxy** and click **OK**.
- 3) When the **Enter the proxy server details** prompt appears, provide the proxy server parameters:
  - **Proxy IP Address** - Enter the Proxy server's IP address.
  - **Proxy Port** - Enter the port number assigned to the Proxy server.
- 4) Click **Next** to select the authentication type from **NoAuth**, **BasicAuth** and **NTLMAuth**. If you select authentication type as **BasicAuth** or **NTLMAuth**, you need to provide user name and password.
  - **Proxy User** - Enter the user name for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.
  - **Proxy Password** - Enter the password for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.

## Step 9 - Register the Physical Appliance Using Remote Console Interface

- 1) Go to the **Personalize this scanner** menu option and press **Enter** to continue.
- 2) Enter your 14 digit personalization code which you generated in [Step 1 - Generate the Personalization Code](#).



3) Click **Submit** and wait for the confirmation message **Appliance registration completed successfully**. Check that the status on the console is Registered. Once your appliance successfully registers to the Qualys Cloud Platform, you'll start seeing appliance with status as paused.



## Step 10 - Check the Status on UI

Log in to the Qualys UI and select **Network Passive Sensor** from the application picker. The Sensors tab appears with the list of sensors in your account and their status.

Sensors						
4 Active Assets (7days)		0 New Discoveries (24hrs)				
Filters	New Sensor	1 - 3 of 3				
SENSOR	DEPLOY LOCATION	ACTIVE ASSETS (1 HOUR)	NETWORK UTILIZATION	CPU	RAM	HDD
PS-AutoPhysical Unregistered	Pune	0	0	0	0	0
PS-AutoVirtual QPS-01G-0100-VM 1.3.2-12 Sensing	Pune 10.113.231.61 / fe80:20c:29ff:febb:fd03 00:0c:29:bb:fd:03	73	0.0 Gbps/1.0 Gbps	20%	22%	4%
PS-Virtual_deploy QPS-01G-0100-VM 1.3.2-12 Deregistered	wifi 10.113.231.61 / fe80:20c:29ff:febb:fd03 00:0c:29:bb:fd:03	0	0/1.0 Gbps	0	0	0

You'll see the status for each sensor in the list: Unregistered, Sensing and Deregistered.

- If the status is **Unregistered**, you can view details for the sensor and deregister.
- If the status is **Sensing**, you can view details and pause the sensing.
- If the status is **Deregistered**, you can view details for the sensor and delete Sensor.

## Step 11 - Check the Status on Appliance

Checking the status on appliance, only applicable to models 1G (QPS-01G-0100-A0) and 4G (QPS-04G-0402-B0) appliance with LCD).

The status of the sensing and error messages are indicated using LEDs and LCD interface. Appliance has 3 LEDs on front panel - 2 green and 1 amber (red for 4G appliance) colored. Depending on the appliance sensing state, LEDs and LCD interface will have different indications:

State	LCD Indicator (Applicable for Model QPS-01G-0100-A0)	LED Indicator (Applicable for Models QPS-01G-0100-A0 & QPS-04G-0402-B0)
Sensing	S letter	Steady Green LED
Paused	P letter	Blinking Green LED
ECO	NA	Blinking Amber LED for model QPS-01G-0100-A0 Blinking Red LED for model QPS-04G-0402-B0
Communication error	NA	Steady Amber LED for model QPS-01G-0100-A0 Steady Red LED for model QPS-04G-0402-B0

## Manage Sensors

You can easily manage your physical or virtual sensors from the Sensors tab.

Simply, navigate to the **Sensors** tab and from the Quick Actions menu you can perform actions like view details, deregister sensor, delete assets discovered by the sensor, delete sensor, etc.

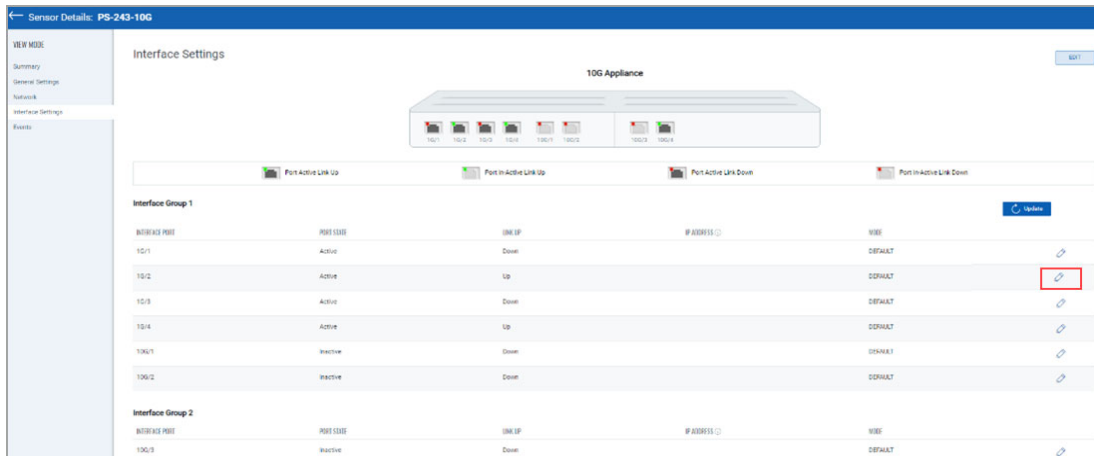
PS-Automation Unregistered	Quick Actions	wifi	0	0	0	0	0
PS-AutoPhysical Unregistered	View Details	Pune	0	0	0	0	0
PS-AutoVirtual QPS-01G-0100-VM 1 Sensing	Start Sensing	Pune	75	0.0 Gbps/1.0 Gbps	19%	22%	4%
PS-Virtual_deploy QPS-01G-0100-VM 1 Deregistered	Reboot						
	Delete Assets						
	Deregister	wifi	0	0/1.0 Gbps	0	0	0

For more detailed information about the **Sensors** tab, refer to [online help](#).

## Assigning/Removing IP Addresses to the Appliance Sniffing Interfaces

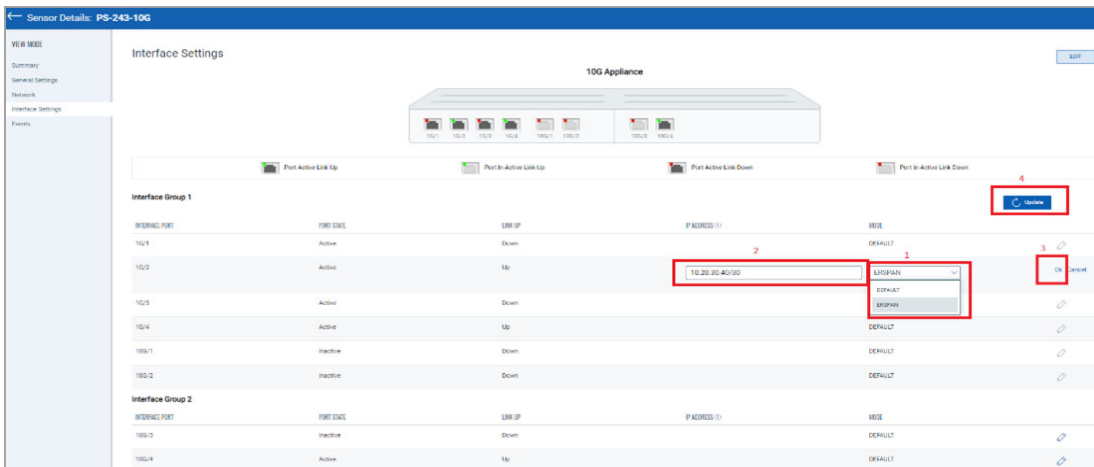
To assign or remove the IP address from the appliance sniffing interface, go to the **Sensors** tab and from the Quick Actions menu of a sensor, click **View Details > Interface Settings**. Alternatively, you can click on the sensor to go directly to the sensor view details page.

Click the **edit** icon of the desired sniffing interface, as shown in the following screenshot.



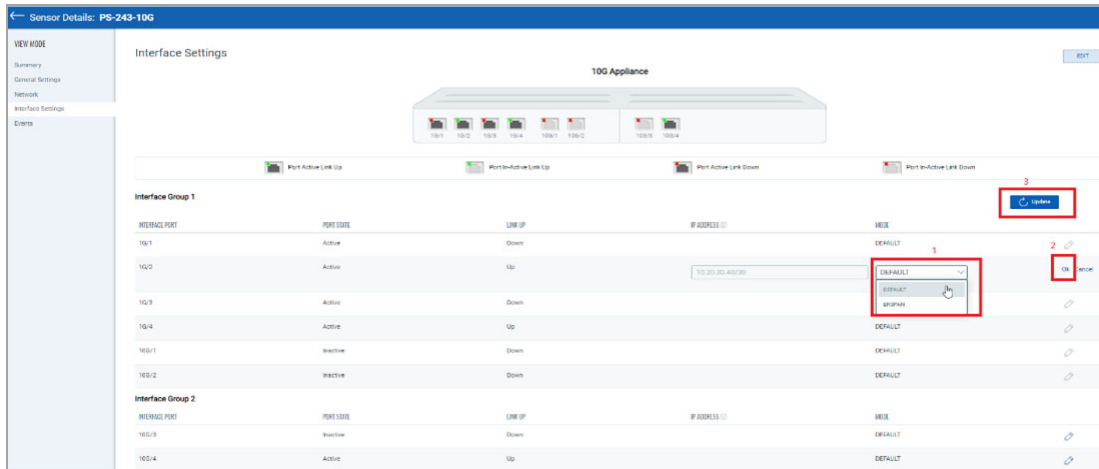
Select **ERSPAN** mode and assign IP to the interface along with subnet mask.

Click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.



To remove the IP Address from the sniffing interface, click the edit icon of the desired sniffing interface.

Select **DEFAULT** mode, click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.



### Important:

- For the 10G appliance model (QPS-10G-0404-B1), the interface needs to be active before assigning an IP address to the sniffing interface.
- The Network Passive Sensor (NPS) appliance will reboot once after adding/editing/deleting the IP address of the sniffing interface.

**Note:** The Network Passive Sensor (NPS) appliance version 1.3.6-12 supports assigning IP addresses on the sniffing interface. So before assigning an IP address to the sniffing interface, ensure that the NPS appliance version is 1.3.6-12 or above.

## Configure Assets

Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

You can configure how you want to categorize your assets discovered by the sensors while monitoring traffic flow. All these assets are listed in the Assets tab of Global AssetView/CyberSecurity Asset Management.

Assets can be defined as Internal Assets, Excluded Assets, and External Assets.

## Internal Assets

To add internal assets, simply go to **Configuration > Internal Assets > Add**.

← Internal Assets

### Internal Assets

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name \*

ICS\_test\_group

Include the Following Sensors [Select Sensors](#)

1 SENSOR SELECTED [Remove All](#)

Test\_Sensor

Do you want to inventory the assets? [?](#)

☒ Yes ☐ No

Internal Asset IP Range

Default IP Ranges

- 192.168.0.0/16
- 172.16.0.0/12
- 10.0.0.0/8

Type

DHCP

[Cancel](#) [Save](#)

Here, you'll define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use Default IP Ranges, IP range Tags and Custom IP Ranges options to define range of internal assets. NPS will inventory assets for the IP ranges configured in the Internal Asset IP Range when default option under **Do you want to Inventory the assets?** is set to **Yes**.

Select **No** if you want to just monitor the traffic flows to/from the configured IP ranges but do not want to track them in asset inventory. You can always edit the sensor configuration later to add assets for the IP ranges to the inventory if you have selected No while registering virtual or physical sensors.

To complete the sensor setup and to start sensing assets you must define Internal Asset ranges. The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

## 1 - Default IP Ranges

This option defines internal assets discovered within default internal ranges for your network. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors

Select Sensors

1 SENSOR SELECTED

Remove All

Test\_Sensor

×

Do you want to inventory the assets? ?

☒ Yes
 ☐ No

Internal Asset IP Range

Default IP Ranges

☒ 192.168.0.0/16
 ☒ 172.16.0.0/12
 ☒ 10.0.0.0/8

Type

DHCP

Cancel

Save

## 2 -IP Range Tags

This option defines internal assets discovered with IP range tags. These are the dynamic tags created with 'IP Address In Range(s)' rule engine. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset. Click **Select IP Ranges** to select IP tags from the list of tags for which you want to define internal asset.

Include the Following Sensors

Select Sensors

1 SENSOR SELECTED

Remove All

PS-Automation

×

Do you want to inventory the assets? ?

☒ Yes
 ☐ No

Internal Asset IP Range

IP Range Tags

Include the Following IP Tags

Select IP Ranges

TAGS	IP RANGES	
IP_tag1	1 192.168.16.0/24 192.168.17.0/24 192.168.18.0/24	×

Type

DHCP

### 3- Custom IP Ranges

This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors Select Sensors

1 SENSOR SELECTED Remove All

PS-Automation ×

Do you want to inventory the assets? ?

☒ Yes ☐ No

Internal Asset IP Range

Custom IP Ranges ▼

IP Ranges \*

10.10.10.0/12 +

Type

DHCP ▼

### Excluded Assets

Here, you can define the IP ranges or MAC addresses to be excluded from the inventory. The assets discovered for these addresses will be masked as Excluded in the traffic summary.

To add excluded assets, simply go to **Configuration > Excluded Assets > Add**.

← Excluded Assets

**Excluded Assets**

Define the IP or MAC addresses to be excluded from the inventory. The assets discovered for these addresses will be masked as "Excluded" in traffic summary.

Name \*

Asset Type \*

☒ IP Ranges ☐ MAC Address

Enter an IP Range... +

Cancel Save

### Monitor External Assets

Here, you can define the external sites you want to monitor. These sites will be reported individually for traffic summary however these will not be inventoried like the internal assets.

To add external assets, simply go to **Configuration > Monitor External Assets > Add**.

## General Settings

General Settings tab consists of two sub tabs: General Configuration and Exclusion.

### General Configuration

- You can help Qualys NPS to enhance the operating system and device prediction of the asset by providing fingerprint data.
- You can set up notifications for events like Driver Change Required, Reboot Required, and Asset Reporting Stopped to be sent to your email address.

You can see the latest events generated in the events section of the sensor details page.

EVENTS	COUNT	MESSAGE	TYPE	TIMESTAMP RANGE
Driver Change Required	1	All	Moderate	07 Sep 2022 08:56 am
Reboot Required	1	All	Moderate	07 Sep 2022 08:52 am

## Exclusion

You can exclude specific hostnames when merging unmanaged assets or merging them.

### General Configuration



Qualys NPS service utilizes the data gathered from traffic flows to predict the OS and hardware. NPS does not collect any user-specific sensitive data. It collects the protocolspecific data gathered from packet headers, which are transparently displayed to the customer in the asset's Raw Discovery Data (in the CSAM/GAV > Asset Details > System Information > View Raw Information Data section).into managed assets.

NPS service identifies patterns in this data to predict OS and device models. There is always a scope for improving pattern recognition to detect more OS and device models. Once consent is given, Qualys can collect the asset's metadata and utilize it to enhance predictions of OS and device models in future releases.

Follow these steps to configure the general settings.

- Navigate to **Configuration > General Settings > General configuration.**
- To give consent to Qualys to access the metadata, toggle Access to Fingerprint Data to allow access.

Go to the recipient's text box and add the e-mail or you can add multiple e-mails using comma separated. Click **Save**.

Network Passive Sensor

HOME SENSORS **CONFIGURATION**

**Configuration** Internal Assets Excluded Assets Monitor External Assets General Settings

General Configuration

Exclusion

**General Configuration**

**Access to Fingerprint Data** ☐

Allow Qualys to collect asset fingerprint data

*By enabling this option you permit Qualys to collect fingerprints of assets. This will help improve Operating System and Device prediction of the assets. Please note that fingerprints do not include any sensitive data. They consist of metadata related to the assets, which can be viewed in the CSAM/GAV -> Asset Details -> System Information -> View Raw Information section.*

**Mail ID Recipients**

Add recipients to receive email notifications for specific events

Recipients

Separate emails using commas (,) between addresses

**Save**

## Exclusion

You can configure hostnames that need to be excluded while merging unmanaged assets or merging unmanaged assets into managed assets. The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer the following screenshot for configuring excluded hostnames.

Also, you can configure hostnames that need to be excluded while de-duplicating unmanaged assets or de-duplicating unmanaged assets into managed assets. The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer to the following screenshot for configuring excluded hostnames.

Network Passive Sensor

HOMESENSORSCONFIGURATION

Configuration

Internal AssetsExcluded AssetsMonitor External AssetsGeneral Settings

General Configuration

Exclusion

Exclusions

Configure names that Qualys should exclude from hostname based asset de-duplication

Add Hostnames ⓘ

Enter Hostname

Add

Clear Selection

Remove Selected

☐ HOSTNAMES

ASD

QWE

example

Save

# Intranet Scanner Tour

This section gives you a tour of the QualysGuard Intranet Scanner physical appliance, its features, basic operation and configuration options.

[A Quick Look at the Appliance \(1Gbps \(QPS-01G-0100-A0\)\)](#)

[Navigating the Appliance UI](#)

[System Reboot and Shutdown](#)

[Configure Static IP Address](#)

[Proxy Configuration](#)

## A Quick Look at the Appliance (1Gbps (QPS-01G-0100-A0))



### Front Panel

You'll see **Welcome to Qualys** in the LCD display when you connect the appliance to the network for the first time. After you've successfully completed the Quick Start steps you'll see the appliance name and IP address.

The appliance has a user interface for configuration and management. You can choose to use the LCD display and keypad on the front panel. LCD display offers the functionality to select menus and navigation (ENTER and arrow keys) for a consistent user experience.

Use the keypad to enter information and respond to prompts.

- Left and Right arrow buttons: move the cursor to left/right in an entry field.
- Up and Down arrow buttons: scroll through menu options, and scroll through characters in an entry field.
- ENTER button: confirm entries and move to the next screen.

### Back Panel

The appliance's back panel includes: the power socket, the Ethernet LAN port, the Ethernet WAN port, two USB 2.0 ports and two USB 3.0 ports.



**Power socket** - Use to connect the power connector to the appliance.

**Power button** - Use to power on the appliance. A green light indicates the appliance is on.

**LAN port** - Use to connect the appliance to a hub or switch on your network using a straight through CAT6 twisted pair Ethernet cable. The LAN port is required for management connectivity to the Qualys Cloud Platform.

**WAN port** - Use to connect the appliance to access or distribution or core switch or core router on your network using a straight through CAT6 twisted pair Ethernet cable. The WAN port is used for incoming mirrored traffic.

**USB ports** - Connect a USB-to-RS232 converter cable (For 4G(QPS-04G-0402-B0)- RJ45 to USB or RJ45 to D-type 9 pin) to a USB port if you want to use the optional Remote Console interface (any port may be used).

## Navigating the Appliance UI

### Main Menu

To access the main menu, press ENTER when the appliance name and IP address are displayed. This shows the Password prompt. Enter the password to display the first menu option **SETUP NETWORK**. A password is required to configure anything on the Physical Passive Sensor Appliance using the LCD panel. This prevents any unauthorized access to the appliance. The default admin password is 0000. After completion of registration process, the admin will be prompted to enter the new admin password which will be used later. If the admin doesn't enter the password within 1 minute, the appliance will continue to use the default password 0000. When the appliance is de-registered, the admin password will be reset to default password(0000).

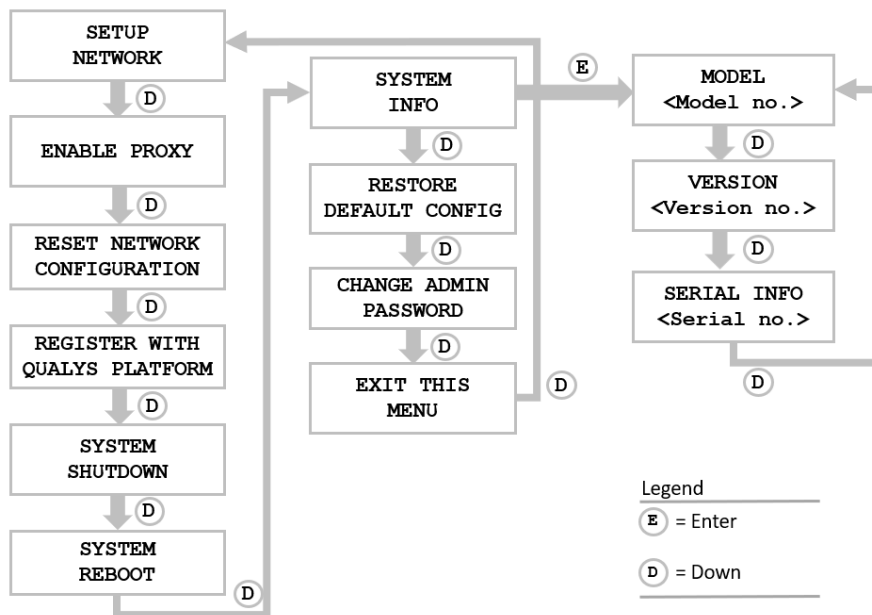







Figure 5-1. Network Passive Sensor Main Menu

To move up through menu options, press the Up arrow. To move down through menu options, press the Down arrow. To select an option, press ENTER. To exit the main menu, press the down arrow button until the **EXIT THIS MENU** option appears, and then press ENTER.

## Navigation Indicators

Each screen displays one or more indicators in the top right corner, indicating the navigation options available from the current screen.

LCD Button	Remote Console Key	Description
	ENTER	Confirm a selection. After you press ENTER, another screen appears.
	RIGHT	Move the cursor to the right in an entry field.
	LEFT	Move the cursor to the left in an entry field. (For 4G(QPS-04G-0402-B0) appliance, this button is not available).
	UP	Used to: — Increase the value in an entry field — Move up through menu options — Cancel a confirmation message
	DOWN	Used to: — Decrease the value in an entry field — Move down through menu options

Note these important guidelines for using buttons: 1) Press one button at a time, 2) Do not hold down an arrow button (except as noted in guideline #3), instead press the arrow multiple times, and 3) When entering a user name or password, you can hold down the Up and Down arrow buttons to scroll through characters quickly.

## Entering Information

The LCD interface allows users to enter information in the fields provided using arrow keys. The Left and Right arrows move the cursor to the left and right and the Up and Down arrows are used to scroll through characters. Some fields allow only certain characters to be entered. The character restrictions are described below.

### Up and Down Arrows

Using the LCD interface use the Up and Down arrows to enter characters in a field. Using the Remote Console interface you have the option to use the Up and Down arrows or to use your keyboard to enter characters.

In numeric entry fields, press the Up and Down arrows to select a value between 0 and 9. When a numeric field is first displayed, a default value appears.

In text entry fields where you enter a username and password, press the Up and Down arrows to select a character (numeric, alphabetic, underscore or special character). In these fields, you can hold the Up/Down arrow to scroll through the available characters. Text fields are blank to start (filled with spaces).

## Scrolling through Characters

Some fields allow you to select characters. Press the Up arrow to scroll through characters in ascending order. Starting from the space character, the characters appear in this order: lowercase letters (a to z), space, numbers (0 to 9), underscore, special characters (for Proxy username and password only), uppercase letters (A to Z).

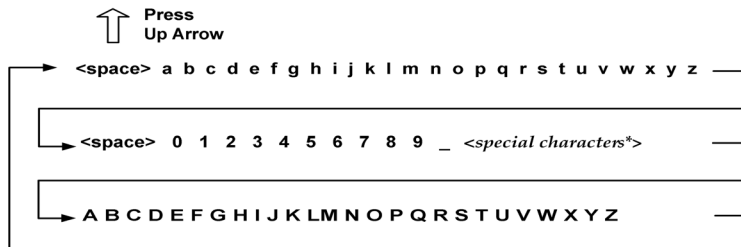


Figure 5-2. Scrolling characters in ascending order

Press the Down arrow to scroll through characters in descending order. Starting from the space character, the characters appear in this order: uppercase letters (Z to A), special characters (for Proxy username and password only), underscore, numbers (9 to 0), space, lowercase letters (z to a).



Figure 5-3. Scrolling characters in descending order

## Space Character

When a text field entry contains fewer characters than the characters displayed on the LCD interface screen, you must select the space character for the unused positions before or after the field entry. Only the characters associated with the field entry and space characters may be included in a text field entry.

Embedded spaces are not permitted in text field entries (except for the Proxy password).

Use the space character to remove characters when editing text fields (except for the Proxy password). To remove a character in an entry field using the LCD interface, move the cursor on the character (using the Left and Right arrows), select the space character (using the Up and Down arrows) and then press ENTER. Any space characters entered appear in the LCD interface screen until the next time you revisit the screen.

## IP Addresses

Entry fields for IP addresses are pre-filled with values in this format: *nnn.nnn.nnn.nnn*

The IP address format displays values for each character position in all octets. When entering an IP address, you replace the three “n” digits for each octet as appropriate. If an octet has less than three digits, then the octet must include leading zeros. For example, to specify the IP address “194.55.176.2”, you need to enter the IP address as “194.055.176.002”.

## Proxy User Name

For the Proxy user name in the **PROXY USER** field you may enter a maximum of 32 characters including lower case letters, upper case letters, numbers and underscore. These special characters can be used: underscore (\_), dash (-), backslash (\), period (.), at sign (@).

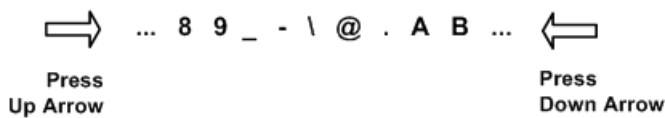


Figure 5-4. Special characters in the Proxy user field

The screen displays 16 characters of the **PROXY USER** field entry, and it scrolls left. For example, the first character of the Proxy username is hidden when the 17th character is entered. As each additional character is entered, the Proxy user name scrolls left. The space character should be used to remove characters.

The format of a Proxy user entry is: “domain\user”. If there is a backslash in the middle of the entry, the appliance interprets the string before the backslash as the domain name. No double backslashes (\\) are needed in front of the “domain\user” format.

## Proxy Password

The **PROXY PASS** allows you to enter a maximum of 16 characters including lowercase letters, uppercase letters, numbers, space, and underscore. Many special characters are allowed. These characters are shown in ascending order in the table below. Using the LCD interface, to scroll through characters 1 to 30, press the Up arrow. To scroll through characters in descending order, press the Down arrow.

Special Characters in the PROXY PASS field

Order (ascending)	Character	Name	Order (ascending)	Character	Name
1	_	underscore	16	+	plus
2	-	hyphen	17	=	equal
3	\	backslash	18	(	parenthesis left
4	/	slash	19	)	parenthesis right
5		bar	20	{	brace left



### Special Characters in the PROXY PASS field

Order (ascending)	Character	Name	Order (ascending)	Character	Name
6	~	tilda	21	}	brace right
7	!	exclamation	22	[	bracket left
8	?	question	23	]	bracket right
9	@	at sign	24	<	less
10	#	number sign	25	>	greater
11	\$	dollar	26	;	semicolon
12	%	percent	27	"	double quote
13	^	caret	28	`	grave
14	&	ampersand	29	,	comma
15	*	asterisk	30	.	period

## System Reboot and Shutdown

It is important to follow the proper system shutdown instructions described below. If you do not follow these instructions, file system corruption may occur.

### How to reboot the system

- 1) With the appliance name and IP address displayed, press ENTER.
- 2) When the **SETUP NETWORK** menu option appears, press the Down arrow to navigate through the menu options.
- 3) When the **SYSTEM REBOOT** menu option appears, press ENTER to select the option.
- 4) When the **REALLY REBOOT SYSTEM?** prompt appears, press ENTER to confirm.

Review the confirmation messages starting with **REBOOTING SYSTEM** message. The **APPLIANCE NAME-IP ADDRESS** is displayed after the Intranet Scanner makes a successful connection to the Qualys Cloud Platform. This message indicates the Intranet Scanner is ready for use. If another message appears you may need to activate the appliance or troubleshoot the issue. Refer to the [Troubleshooting](#) section for resolving errors.

### How to shutdown the system

- 1) With the appliance name and IP address displayed, press ENTER.
- 2) When the **SETUP NETWORK** menu option appears, press the Down arrow to navigate through the menu options.
- 3) When the **SYSTEM SHUTDOWN** menu option appears, press ENTER.
- 4) When the **REALLY SHUTDOWN SYSTEM?** prompt appears, press ENTER to confirm.

**Important!** The appliance should now power down within 60 seconds and then you can safely unplug the appliance.

## Configure Static IP Address

If DHCP is not on your network, you must enable the appliance with a static IP address using the **ENABLE STATIC N/W CONFIG** menu option.

Entry fields for IP addresses used in the static IP address configuration are pre-filled with three digits for all octets, and you must enter a value for each digit. For example, to specify the IP address “176.34.20.5”, you need to enter the IP address as “176.034.020.005”. Refer to the [IP Addresses](#) section for details.

### Tell me the steps

When enabling a static IP address, you must enter network configuration settings for the Intranet Scanner so that the appliance can communicate with the Qualys Cloud Platform. Also, you have the option to enter some network settings for informational purposes.

To enable a static IP address, follow these steps:

- 1) Go to the **SETUP NETWORK** menu option and press ENTER to continue.
- 2) Press the Down arrow until the **ENABLE STATIC N/W CONFIG** menu option appears. Then press ENTER to continue.
- 3) Press the Down arrow to choose **ENABLE IPv4** or **ENABLE IPv6** to enable Internet Protocol and press ENTER to continue.
- 4) When the **CFG STATIC N/W PARAMS?** prompt appears, press ENTER to continue. Or press the Up arrow to quit this procedure and return to the **SETUP NETWORK** menu option.

## Entering parameters on LCD interface

The LCD interface allows users to enter information using the arrow keys. With the Remote Console interface, you enter characters using the VT100 terminal's keyboard.

- 1) When the **IP ADDR** prompt appears, enter the static IP address, and then press ENTER to continue.
- 2) When the **NETMASK** prompt appears, use the Up and Down arrows to scroll to the desired netmask value. For information about netmask values. Refer to the [Tell me about Netmask](#) section. After selecting a netmask value, press ENTER to continue.
- 3) When the **GATEWAY** prompt appears, enter the gateway IP address, and then press ENTER to continue.
- 4) When the **DNS1** prompt appears, enter the IP address for the primary DNS server, and then press ENTER to continue.
- 5) When the **DNS2** prompt appears, enter the IP address for the secondary DNS server. This entry is optional. Press ENTER to continue.
- 6) When the **SAVE AND APPLY?** prompt appears, press ENTER to continue. Or press the Up arrow to quit this procedure and return to the **SETUP NETWORK** menu.
- 7) Review the confirmation messages. The Network Passive Sensor attempts to make a connection to the Qualys Cloud Platform using the new configuration. Upon success the **APPLIANCE NAME-IP ADDRESS** message appears and the static IP address is enabled.

## Confirm the configuration

The message **APPLIANCE NAME-IP ADDRESS** appears when the Intranet Scanner made a successful connection to the Qualys Cloud Platform using the new configuration.

An appliance configuration error appears if it failed to make a connection to the Qualys Cloud Platform. An error may occur because the static IP parameters you entered are incorrect, or they do not match the IP subnet configuration on your network. Refer to the [Troubleshooting](#) section for resolving the issue.

## Tell me about Netmask

When entering static network parameters, you will notice that the cursor does not appear after the **NETMASK** prompt and you cannot enter characters in the entry field. At first, the netmask “255.255.255.000” appears. Use the Up and Down arrows to scroll through valid netmasks. When the appropriate netmask value appears, press ENTER to confirm.

Possible netmask values are listed below. If you press the Down arrow, the values appear in this order: “255.255.255.000”, “255.255.254.000”, “255.255.252.000... If you press the Up arrow, the values appear in this order: “255.255.255.000”, “255.255.255.128”, “255.255.255.192”...

### Scrolling netmask values in the Netmask field

Prefix	Netmask value	Prefix	Netmask value
/24	255.255.255.000	/9	255.128.000.000
/23	255.255.254.000	/8	255.000.000.000
/22	255.255.252.000	/7	254.000.000.000
/21	255.255.248.000	/6	252.000.000.000
/20	255.255.240.000	/5	248.000.000.000
/19	255.255.224.000	/4	255.000.000.000
/18	255.255.192.000	/3	224.000.000.000
/17	255.255.128.000	/2	192.000.000.000
/16	255.255.000.000	/1	128.000.000.000
/15	255.254.000.000	/30	255.255.255.252
/14	255.252.000.000	/29	255.255.255.248
/13	255.248.000.000	/28	255.255.255.240
/12	255.240.000.000	/27	255.255.255.224
/11	255.224.000.000	/26	255.255.255.192
/10	255.192.000.000	/25	255.255.255.128

## Interface - Enable Static IP

Only one option may be enabled: **ENABLE STATIC N/W CONFIG** or **ENABLE DHCP**. After one option is enabled, the other option disappears from the **SETUP NETWORK** menu.

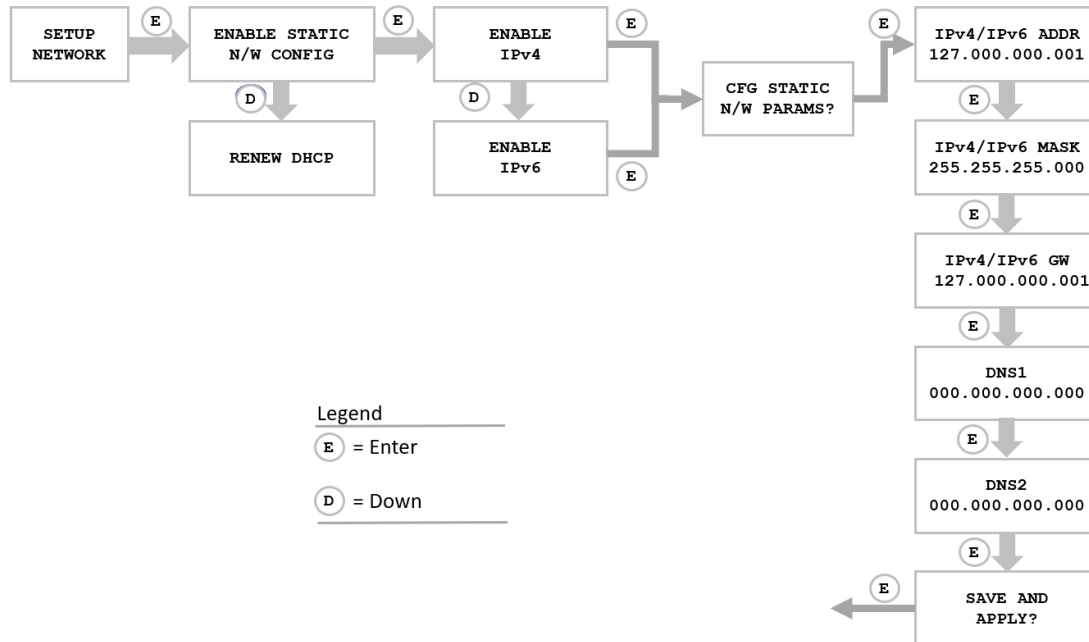


Figure 5-5. Interface to Enable Static IP

Once you configure **ENABLE STATIC N/W CONFIG** the option will change to **CHANGE STATIC N/W CONFIG**. Once you configure **ENABLE DHCP** the option will appear as **RENEW DHCP**.

## Proxy Configuration

If the appliance is behind a Proxy server, you need to enable a Proxy configuration using the **ENABLE PROXY** menu option. Provide details in the Proxy user and password fields to authenticate to your proxy server.

The Intranet Scanner uses Secure Sockets Layer (SSL) protocol (HTTPS and WebSocket) to secure its connection to the Qualys web application, in a similar way that a web browser does to a secure web server. If the Qualys connection must pass through a Proxy server, then you must enable the Proxy option on the appliance. This configuration re-directs Qualys outbound connections through the Proxy server.

Your Proxy server must be configured to tunnel or pass through the SSL session (HTTPS and WebSocket) to the Qualys Cloud Platform. This ensures a secured end-to-end connection. SSL bridging or tunnel termination must not be configured in your Proxy server when supporting the Intranet Scanner.

## Tell me the steps

To configure the appliance with Proxy support, follow these steps:

- 1) Go to the **SETUP NETWORK** menu option.
- 2) Press the Down arrow until the **ENABLE PROXY** menu option appears. Then press ENTER to continue.
- 3) When the **CONFIG PROXY PARAMETERS** prompt appears, press ENTER to continue or press the Up arrow two times to quit this procedure and return to the **SETUP NETWORK** menu option.

## Entering Parameters

Enter Proxy parameters using the Up and Down arrows to scroll through characters.

- 1) When the **PROXY HOST** prompt appears, enter the Proxy server's FQDN/IP address. The gateway IP address appears in the screen by default. Use the LCD interface to enter an FQDN/IP address, and then press ENTER to continue.

IP addresses are allowed in dotted decimal format, e.g. 176.34.20.5

Supported characters for FQDN: Uppercase letters, numbers, dot (.) and hyphen (-)

- 2) When the **PROXY PORT** prompt appears, enter the port number assigned to the Proxy server. Port "0443" appears by default. Confirm that the port number shown is correct or enter a different one, if necessary. When the correct port number appears, press ENTER to continue.

Supported Characters: numbers only

- 3) When the **PROXY USER** prompt appears, enter the username for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank. Press ENTER to continue.

Supported Characters: Lowercase letters, uppercase letters, numbers, and these special characters: \_- \ @.

- 4) When the **PROXY PASS** prompt appears, enter the password for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank. Press ENTER to continue.

Supported Characters: Lowercase letters, uppercase letters, numbers, and these special characters: \_- \ | ~ ! ? @ # \$ % ^ & \* + = ( ) { } [ ] < > ; , " . (including dot).

- 5) When the **REALLY ENABLE PROXY?** prompt appears, press ENTER to continue. Or press the Up arrow two times to quit this procedure and return to the **SETUP NETWORK** menu option.

- 6) Review the confirmation messages. The **ENABLING PROXY SUPPORT** message appears followed by other messages while the Intranet Scanner attempts to make a connection to the Qualys Cloud Platform using the new configuration.

Upon success the **APPLIANCE NAME-IP ADDRESS** message appears and the configured proxy is now confirmed working and being used.

## Interface - Enable Proxy

The LCD interface to enable Proxy support is shown below.

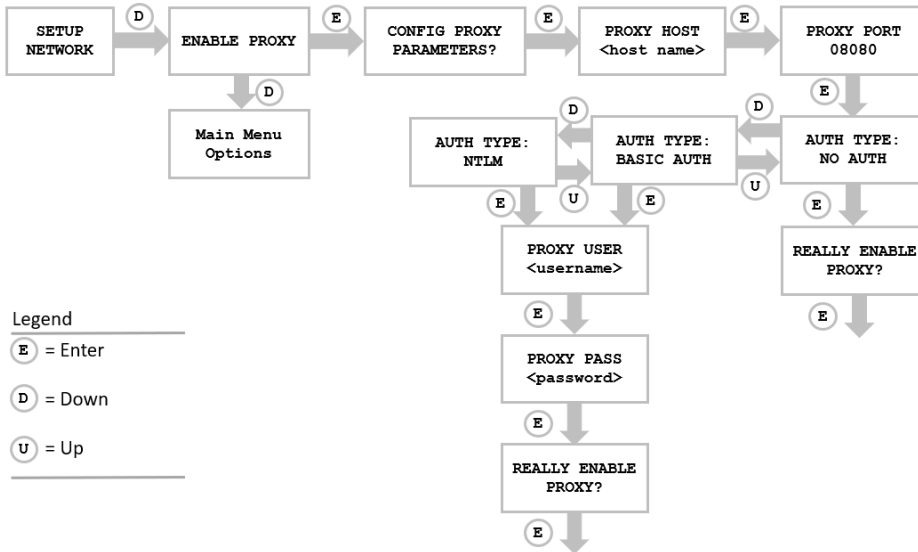


Figure 5-6. Interface to Enable Proxy

## Want to update proxy settings?

Once a Proxy configuration is enabled, the Proxy settings are stored on the appliance. You can change or disable these settings at any time.

To change Proxy parameters, follow these steps:

- 1) Go to the **SETUP NETWORK** menu option.
- 2) Press the Down arrow until the **CHANGE PROXY PARAMS** menu option appears. Then press ENTER to continue.
- 3) Follow the prompts and messages in the LCD interface to change the existing Proxy parameters. Existing parameters are displayed in each screen. Change and confirm each parameter. If a parameter has not changed, press ENTER to view the next parameter.
- 4) When the **REALLY ENABLE PROXY?** prompt appears, press ENTER to continue. Or press the Up arrow two times to quit this procedure and return to the **SETUP NETWORK** menu option.
- 5) Review the confirmation messages. The **ENABLING PROXY SUPPORT** message appears followed by others.

To disable Proxy parameters, follow these steps:

- 1) Go to the **SETUP NETWORK** menu option.
- 2) Press the Down arrow until the **DISABLE PROXY** menu option appears. Then press ENTER to continue.
- 3) When the **REALLY DISABLE PROXY?** prompt appears, press ENTER to continue. Or press the Up arrow two times to quit this procedure and return to the **SETUP NETWORK** menu option.
- 4) Review the confirmation messages.



## Interface - Change Proxy Parameters

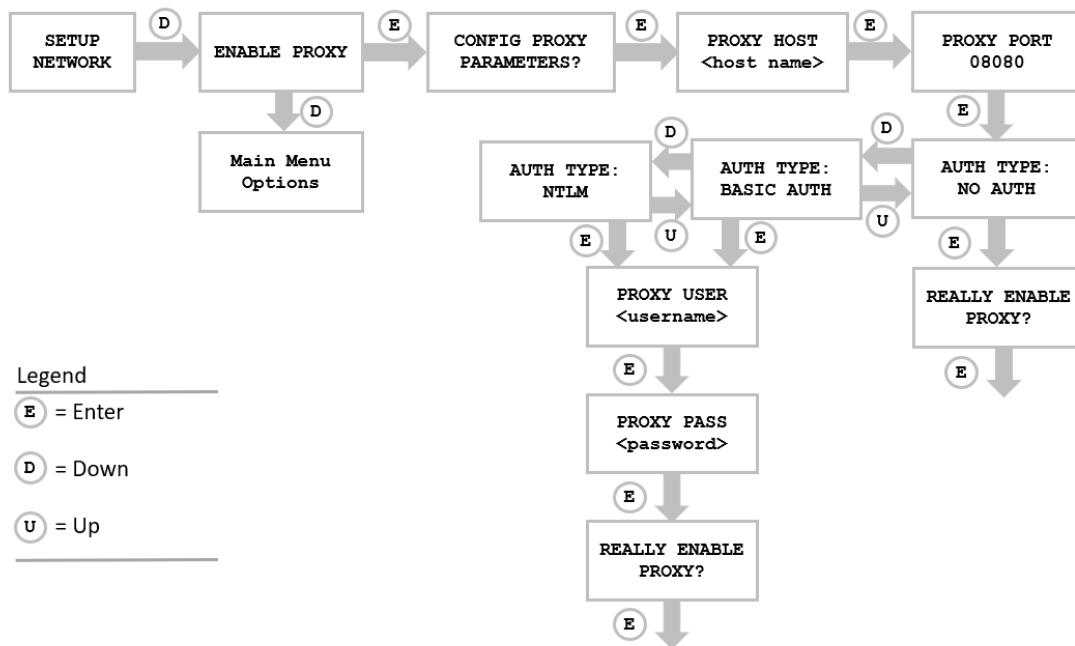


Figure 5-7. Interface to Change Proxy Parameters

## Confirm the configuration

The message **APPLIANCE NAME-IP ADDRESS** appears if the Intranet Scanner made a successful connection to the Qualys Cloud Platform using the new configuration.

The **USER LOGIN** prompt appears if the Intranet Scanner made a successful connection to the Qualys Cloud Platform, however the appliance has not been activated. See Step 1 in the [Get Started](#) section and follow the instructions to activate the appliance.

An appliance configuration error appears if the Intranet Scanner failed to make a connection to the Qualys Cloud Platform. An error may occur because the Proxy parameters you entered are incorrect, or they do not match the Proxy configuration on your network. Refer to the [Troubleshooting](#) section for resolving this issue.



# Troubleshooting

Use the troubleshooting techniques described here to respond to errors and performance conditions when using the Intranet Scanner physical appliance.

[How can I test network connectivity?](#)

[Need the model number or serial number for your appliance?](#)

[Communication Failure message](#)

[Appliance Configuration Errors](#)

## How can I test network connectivity?

### Use a Laptop

It is recommended that you test network connectivity to the Qualys Cloud Platform using your laptop (or other device):

- 1) Take the laptop to the location where the Intranet Scanner will be installed and connect the laptop to the network, using the same network cable and port that will be used for the appliance.
- 2) Configure the laptop with the same network configuration that the Intranet Scanner will use (IP address, gateway, DNS server, etc.).
- 3) If the connection to the Qualys Cloud Platform must pass through a proxy server, configure the laptop's web browser with proxy information.
- 4) Open a browser and try to log into your Qualys account. You'll see the Qualys Log In page after a successful connection is made to the Qualys Cloud Platform.

### Test DNS Name Resolution

You can test DNS name resolution from any machine connected to the same network as your Intranet Scanner. If DNS name resolution is working properly, server information is returned including the server name and IP address (Note that "nslookup" is not available on all systems).

## Need the model number or serial number for your appliance?

You'll find this information on a sticker on your appliance. Depending on the model, it will either be on the side of the appliance or the bottom of the appliance.

## Communication Failure message

You'll see a **COMMUNICATION FAILURE** message if there is a network communications breakdown between the Intranet Scanner and the Qualys Cloud Platform.

### Why does it happen?

The communication failure may be due to one of these reasons: the network cable was unplugged from the appliance, the local network went down, or any of the network devices between the Network Passive Sensor and the Qualys Cloud Platform went down.

### When does the message appear?

If any point of time communication breaks between Network Passive Sensor and Qualys Cloud Platform, then the **COMMUNICATION FAILURE** message appears.

### How do I know the issue is resolved?

After the root cause is resolved, you'll see the **COMMUNICATION FAILURE** message until the next time the appliance makes a successful polling request to the Qualys Cloud Platform. Then you'll see the appliance's name and IP address and you can start using your appliance.

Note - The **COMMUNICATION FAILURE** message may not disappear right away. There may be some lag after the network is restored and before the appliance is back online, depending on when the next polling request is scheduled. Additional time is necessary for communication to be processed by a Proxy server if the appliance has a Proxy configuration.

## Appliance Configuration Errors

An appliance configuration error indicates the Network Passive Sensor attempted to connect to the Qualys Cloud Platform and failed.

Important! The Network Passive Sensor is not functional until the error is resolved. Make sure to resolve the error.

You'll see an error code and short description to help you with troubleshooting. Please refer to the short description provided to help you resolve the issue. If you still need help with the issue, please identify the error code when you contact Qualys Support.

Error Code	Error Description
10	Internal Error
12	DNS Lookup Failed
13	Invalid IP Address
14	Invalid Gateway IP
15	Invalid DNS1 IP
16	Invalid DNS2 IP
17	Loopback IP Error

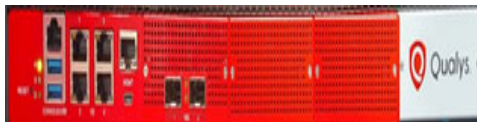
<b>Error Code</b>	<b>Error Description</b>
18	Invalid N/W CFG
19	Invalid Proxy Host
20	Proxy User not Specified
21	Proxy Password not Specified
22	Invalid Prxy CFG
23	Invalid PERS code
24	Registration Failed
25	Gateway Unreachable
26	DNS1 Unreachable
27	DNS2 Unreachable
28	Invalid Password
29	DNS 1 & 2 cannot be same
30	Appliance in ECO state
31	Communication Failed with Cloud
32	Prxy Unreachable
33	NTLM unsupported

## Appendix A- Product Specifications

<b>1Gbps (QPS-01G-0100-A0)</b>	
CPU	Xeon E31275v3, 4C/8T, 3.5GHz
Memory	16GB
Storage	1TB
USB	Two USB 2.0 ports + two USB 3.0 ports
Sensing Interface	1 x RJ45 Ethernet supporting 10/100/1000Mbps
Management Interface	1 x RJ45 Ethernet supporting 10/100/1000Mbps
Power Input	100-240 VAC, 50-60Hz, 4A Single phase
Power Consumption	Max: 91W (310 BTU/hr); Typical: 80W (273 BTU/hr)
Max Throughput	1 Gbps
Dimensions	1.75 (H) x 17 (W) x 14 (D) inches
Weight	12.65 lbs.

### 4 Gbps (QPS-04G- 0402-B0)

#### Front Panel



#### Rear Panel



CPU	Gold 6230, 20C/40T, 2.1GHz
Memory	32GB
Storage	512GB SSD
Sniffing Interface	4 x 1GbE RJ45 and 2 x 10GbE SFP+
Management Interface	1 x GbE RJ45
Power Input	Dual, 120/240 VAC 50/60hz
Power Consumption	Max: 352W

Max Throughput	4 Gbps
Dimensions	650mm x 438mm x 43.5mm
Weight	16.5Kg

#### 10 Gbps (QPS-10G-0404-B1) Front Panel



#### Rear Panel



CPU	2 x Gold 6230, 20C/40T, 2.1GHz
Memory	64GB
Storage	512GB SSD
Sniffing Interface	4 x 1GbE RJ45 + 4 x 10GbE SFP+
Management Interface	1 x GbE RJ45
Power Input	Dual, 120/240 VAC 50/60hz
Power Consumption	Max: 605W
Max Throughput	10 Gbps
Dimensions	610mm x 438mm x 43.5mm
Weight	24Kg

100 Mbps (QPS-01M-0500-D1)    Front Panel



Rear Panel



CPU	Intel Atom (Denverton) 4-Core 2.2GHz
Memory	16GB DDR4-3200Mhz
Storage	256G M.2 SATA
Sniffing Interface	5 x 1GbE ports (RJ45)
Management Interface	1 x 1GbE (RJ45)
Console	1 x RJ45, 1x Mini USB
USB	2 x USB3.0
LED	Power, HDD, Status
Power Button	1x Power Switch
External Power Adapter	Input- AC 100~240V @47~63 Hz, 36W Type- ATX Output-12Vdc,3A Connector-DC Jack lockable



**100 Mbps (QPS-01M-0600-B2) Front Panel****Side Panel**

CPU	Intel Atom , 4 Core, 1.6 GHz
RAM	8GB DDR3L-1866Mhz
Storage	256G mSATA
Networking	4 x 1GbE ports (RJ45) + 2 x 1GbE(SFP)
Management	1 x 1GbE (RJ45)
Console	2 x RS232, DB-9 (M)
USB	2 x USB3.0
LED	Power, HDD, Status
Power Input	Dual 20-54 Vdc Phoenix contact 6-pin connector with lock
Power Button	Standard, HW reset

**Environment Specifications****1 Gbps (QPS-01G-0100-A0)**

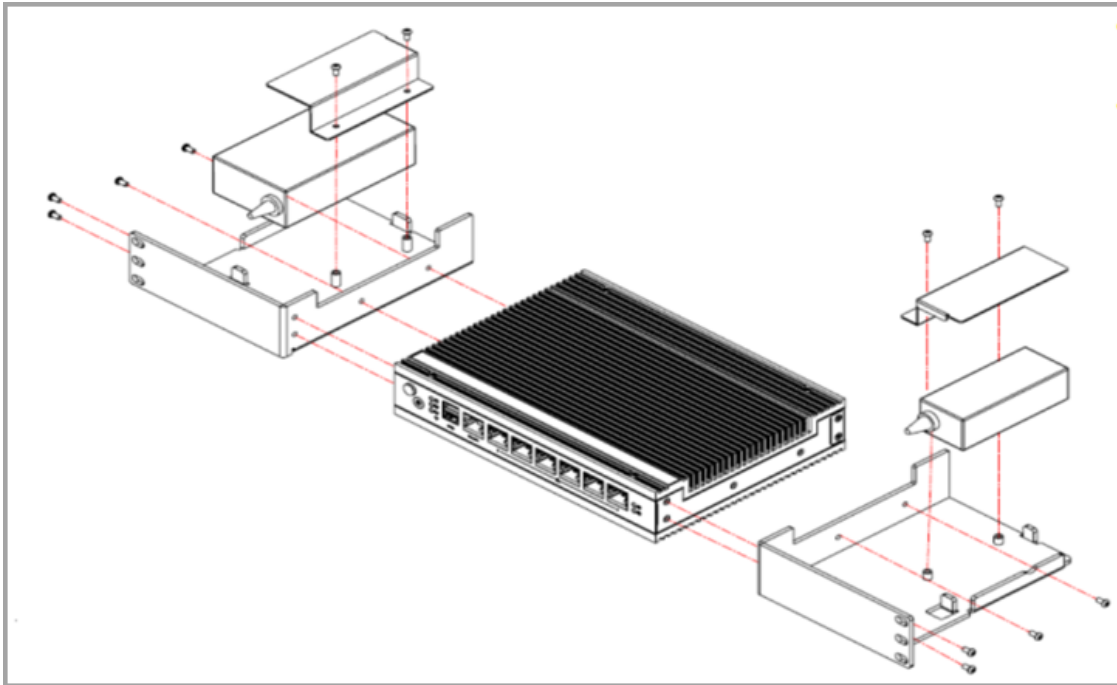
Acoustic Noise	~45 dBA acoustic noise level at 23°C
Operating Conditions	0°C to 35°C, from 0 to 5,000 feet; 20% to 90% RH
Storage Conditions	-10°C to 70°C; 10% to 85% R.H. (non-condensing)
Operating Vibration	0.3 Grms, 10 to 500 Hz, 5 minutes per axis
In-Package Shock	In accordance with ISTA 2A
Regulatory	UL (conforms to UL 60950-1/CSA C22.2 No. 60950/EN 60950-1, 2nd ed.

EMC	FCC Part 15 Class A/ICES-003/EN 55032/EN 55024, CISPR 32
Environmental	RoHS
Other certifications	Per specific requirements
<b>4 Gbps (QPS-04G- 0402-B0)</b>	
Operating Temperature	0°C to 40°C
Non-operating Temperature	-20°C to -70°C
Approvals and Compliance	CE/FCC Class A, UL, RoHS
Humidity	5~90% Operating, 5~95% Non-operating
<b>10 Gbps (QPS-10G-0404-B1)</b>	
Operating Temperature	0°C to 40°C
Non-operating Temperature	-20°C to -70°C
Approvals and Compliance	CE/FCC Class A, UL, RoHS
Humidity	5~90% Operating, 5~95% Non-operating
<b>100 Mbps (QPS-01M-0500-D1)</b>	
System Dimensions(L x W x H) and Weight	220 x 160 x 44 mm (8.7" x 6.3" x 1.7") 2.3Kg
Operating Temperature	-20°C to 70°C
Non Operating Temperature	-40°C to 85°C; 40°C at 95% R.H. non-condensing
Approvals and Compliance	UL 62368, CB 60950/62368, CCC CE EN55032/EN55024 ClassB, FCC ClassB, AS/NZS CISPR32, IEC61000-4-2/61000-4-5, EN 300 386 ROHS, REACH, WEEE
<b>100 Mbps (QPS-01M-0600-B2)</b>	
System Dimensions (L x W x H) and Weight	160 x 166 x 53.5 mm 1.6Kg
Operating Conditions	-40°C to 70°C
Storage Conditions	40°C to 85°C; 5% to 95% R.H. non-condensing
Mounting	DIN rail
Approvals and Compliance	FCC, CE, IEC61850-3, IEEE1613

## Use Case Scenario for Mounting Appliance

Let us take few examples for mounting various appliance.

## Rack Mount 100 Mbps (QPS-01M-0500-D1) Appliance



### Wall Mount 100 Mbps (QPS-01M-0500-D1) Appliance

Follow these steps to wall mount 100 Mbps (QPS-01M-0500-D1) appliance :

1. Remove the screws from the right and left side.



2. Secure the mounting parts by reattaching the screws on both the right and left side.



Your installation is completed.



#### **Mount 100 Mbps (QPS-01M-0600-B2) Appliance using DIN Rail bracket**

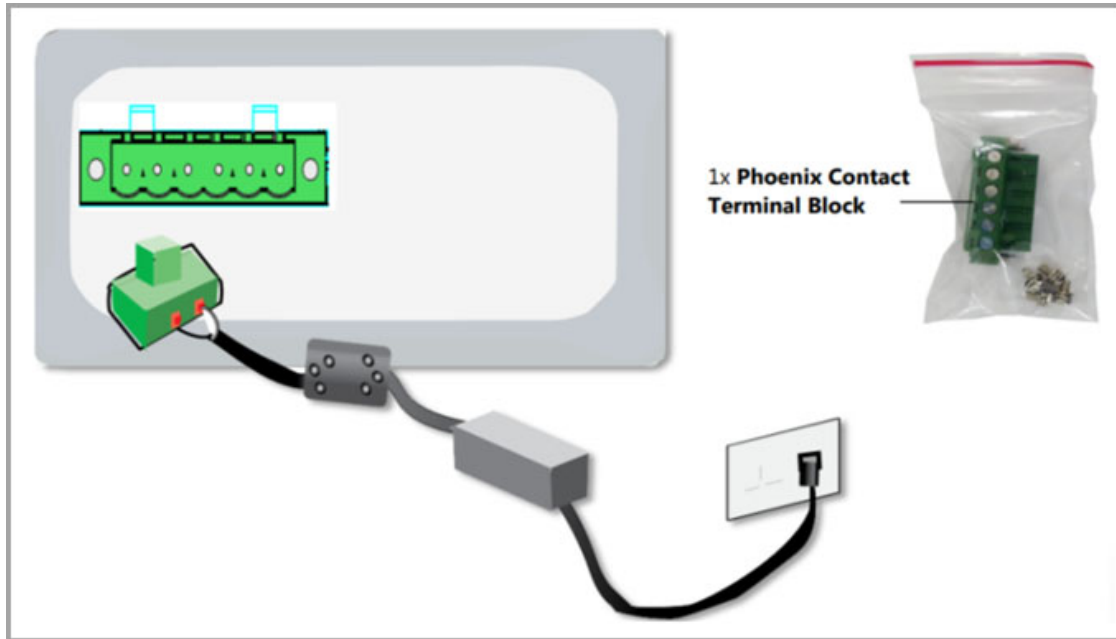
Follow these steps to wall mount 100 Mbps (QPS-01M-0600-B2) Appliance:

1. Attach the bracket to the back of the system using three screws.
2. To securely attach the system, insert the bracket's hook onto the DIN Rail until it is firmly in place..



3. To power the device, connect it to a 20-54 VDC power source supplied by the AC/DC adapter via a Phoenix Contact.

This power socket is especially designed to protect against any power contact faults. So the reverse of the electrical polarity will not damage the system.



## Appendix B - Software Credits

Portions of the software embedded in the Qualys Network Passive Sensor were developed by third parties and are governed by the terms and conditions detailed in the following Qualys document

Qualys Network Passive Sensor Software Credits

<https://qualys-secure.force.com/customers/articles/Knowledge/000006374>

## Appendix C - Safety Notices

**Elevated Operating Ambient** — The ambient temperature of an operating rack environment will be greater than the room's ambient temperature. The unit must be installed in a rack where its operating ambient temperature does not exceed the unit's maximum ambient temperature.

**Reduced Air Flow** — The unit must be installed in a rack which enables adequate air flow for the proper cooling of the unit.

**Adequate Power** — The rack must be set up to ensure that an appropriate level and amount of power is available to the unit. The overall connection of the rack equipment to the supply circuit and the effect that overloading the supply circuit might have on overcurrent protection and supply wiring should also be considered.

**Reliable Grounding** — Reliable grounding of rack equipment must be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (for example, use of power strips).

**Mechanical Loading** — The unit should be installed in a rack in a manner that does not create a hazardous condition due to uneven mechanical overloading.

### Cautionary Notices

The socket-outlet shall be installed near the equipment and shall be easily accessible.

Le socle de prise de courant doit être installé à proximité du matériel et doit être aisément accessible.

CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.  
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

ATTENTION: IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE  
BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGÉES  
CONFORMÉMENT AUX INSTRUCTIONS.

#### WARNING

Hazardous moving parts  
Keep away from moving fan blades



## Appendix D- Extending the Network Feature

The Network feature is also applicable to the PS appliances, which provides these benefits:

- a. It allows PS to maintain two or more passively sensed assets from overlapping IP address space, having the same IP, as separate assets within one subscription, each with its unique identity.
- b. It allows PS to dynamically tag the assets based on the Network and IP.
- c. It allows PS to de-duplicate and merge the passively sensed asset having the same IP as the managed asset, provided both assets belong in the same network. So, asset de-duplication is enhanced to use only-IP in addition to the previously support MAC or hostname as merge criteria. PS uses MAC to merge if available, if not then hostname and lastly only IP.

- The Network feature is available as a subscription on your account, and you should avail this feature subscription only if you have assets in overlapping IP address space that have to be inventoried.

### Use Cases:

1. Your network has overlapping IP addresses of the private RFC-1918 IPs, one existing in you enterprise and another having the same address space coming from an acquisition. You may already have been actively scanning enterprise network using Qualys active scanners and/or passively sensing the same and now you want to extend the same active scan/passively sense operations on the overlapped private IP space of the acquired network. You want to inventory the assets in both the overlapped spaces and also see the assets tagged with a name reflecting the enterprise or the overlapped network. You also want unmanaged assets from enterprise network merge with managed assets from the same network and likewise for the acquired network.

2. The other use case of overlapping IP address space is where you have used routable, non-RFC-1918 IPs in your internal network and want to keep it separate from the routable IPs assigned to load-balancers, external facing servers. You want to deduplicate assets from this internal network with non-RFC1918 IPs actively scanned by internal active scanner with passively sensed assets from internal network.

**Note:** A third use case, arising more misunderstanding of the Network feature, is to use this feature to define networks as per administrative domains rather than for overlapped IP address space. In this case, a single passive sensor may get associated with more than one administrative network whose traffic it may be sensing.

**Note:** For usecase 1 and 2, it is mandatory to have two or more passive sensors, one for each overlapping IP address space. You cannot have a single sensor sensing that is fed with a mirrored traffic from two networks having IP overlapped address space.

## How must you use the Network feature?

1. Subscribe to the Networks feature to see the Network tab in VM DR module. Using the Network tab define two networks one for each overlapping space.

a. Enterprise Network N1

b. Acquired Network N2

2. In VM DR, define asset groups in each of the networks such as

a. Asset group 1: AG1, 192.168.0.0/24, Network N1

b. Asset group 2: AG2, 192.168.0.0/24, Acquired Network N2

3. Have a PS appliance, one for each of the networks and associate it with the corresponding network. To configure the appliance to network association, navigate to Passive Sensor Module, select a sensor, in the details select the “Network” tab and in that edit to select the Network from a list of Networks.

- Deploy PS1 in Network N1. Configure the PS1 to contain 192.168.0.0/24 as internal inventory IP range, associate PS1 with N1.

- Deploy PS2 in Network N2. Configure the PS2 to contain 192.168.0.0/24 as internal inventory IP range, associate PS2 with N2.

- Register both sensors with the same account.

4. Run active scans or install cloud agents on assets in each of the ranges to enable de-duplication with un-managed assets sensed by PS1 and PS2.

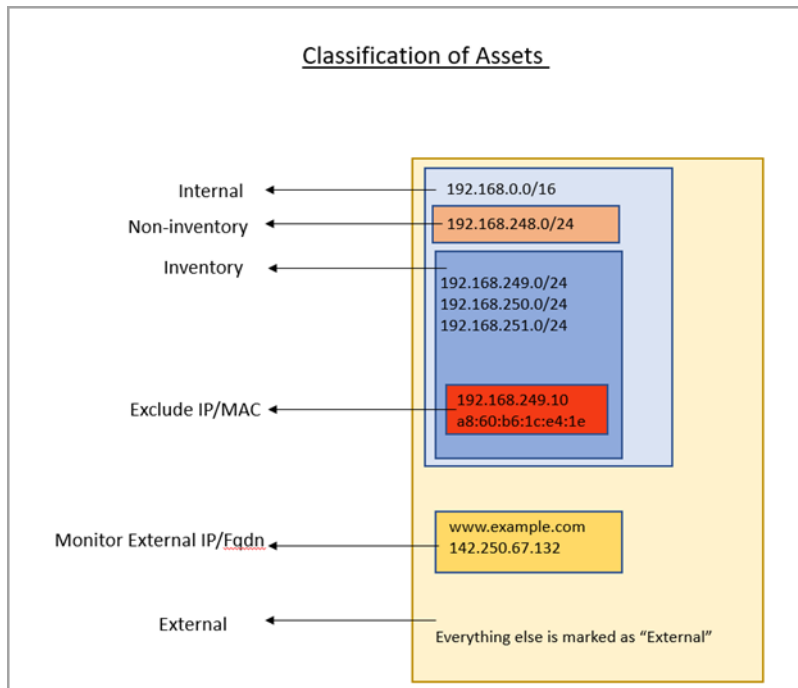
## Appendix E- Classification of Assets in Passive Sensor

Passive sensor classifies IPs as internal and external for the purpose of asset inventory and traffic monitoring.

The area labelled “Internal” in the diagram below is the universe of IP ranges that exists within an enterprise and therefore worth building an asset inventory. Everything outside this range is "External" and not worth inventorying.

From a traffic monitoring perspective, PS tracks flows between assets in the inventoried IP range by 4-tuple. PS does not track individual IPs in the "External" range and attributes all external IPs to a single asset named “External”.

Following is a detailed explanation of how PS treats each class of IPs.



**What is Inventory**

PS uses IP addresses in this range to

- a) Create assets and inventory various asset attributes such as hostname, MAC address, protocol specific attributes, etc.
- b) Track traffic flows to/from these IPs to other all other IPs outside this range.

Assets with IPs in this range are listed under the CSAM inventory.

PS aggregates the traffic flows from an IP in the internal range to another IP in the internal range by 4-tuple of Source IP, Destination IP, Destination port, and TCP or UCP protocol. Appliance reports traffic flows at an interval of 5 minutes for new assets and at 30 minutes for asset updates.

The appliance aggregates multiple flows of the same tuple into one flow when reporting it in the 5- or 20-minutes reporting interval.

For example, if Asset A1 initiated HTTP flow to a webserver A2 multiple times within the 30 minutes interval, PS aggregates these flows and reports a single HTTP flow from A1 to A2 at reporting time.

## How to Configure Inventoried IP Range

To configure an IP range/subnet as internal inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range and set the radio button under "Do you want to inventory these assets?" to Yes.

**Internal Assets**

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name \*

Subnet-A

Include the Following Sensors Select Sensors

1 SENSOR SELECTED Remove All

NPS-A ×

Do you want to inventory the assets? ?

☒ Yes ☐ No

Internal Asset IP Range

Custom IP Ranges ▼

IP Ranges \*

10.10.10.0/24 +

Type

DHCP ▼

Cancel Save

## What is Non-inventory

PS uses IP addresses in this range only for tracking traffic flows to other IPs in the inventory range and NOT for inventory purpose. Assets in this IP range do not show in the CSAM inventory. However, traffic flows to/from these assets are listed in the Network tab of CSAM and under the inventoried asset-centric traffic tab of CSAM.

## How to Configure Non-Inventoried IP Ranges

To configure an IP range/subnet as internal non-inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range and set the radio button under "Do you want to inventory these assets?" to No.

**Internal Assets**

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name \*

Subnet-B

Include the Following Sensors [Select Sensors](#)

1 SENSOR SELECTED [Remove All](#)

NPS-A

Do you want to inventory the assets? ?

☐ Yes ☒ No

Internal Asset IP Range

Custom IP Ranges

IP Ranges \*

10.20.20.0/24

Type

DHCP

[Cancel](#) [Save](#)

To review the configuration, check the last column "Inventoried"

Configuration				
Internal Assets Excluded Assets Monitor External Assets General Settings				
<input type="checkbox"/>	Actions (0) <a href="#">Add</a>	1 - 13 of 13 <a href="#">Previous</a> <a href="#">Next</a> <a href="#">Refresh</a> <a href="#">Settings</a>		
NAME	IP RANGE	SENSOR	TYPE	INVENTORIED
Subnet-A	10.10.10.0/24	NPS-B	DHCP	No
Subnet-A	10.10.10.0/24	NPS-A	DHCP	Yes
Subnet-B	10.20.20.0/24	NPS-A	DHCP	No
Subnet-B	10.20.20.0/24	NPS-B	DHCP	Yes

## What is Excluded

If there is a need to not see some sensitive or confidential assets listed in the inventory, then the passive sensor allows the user to specify configuring IPs and/or MACs in the Excluded range.

PS excludes gathering all inventory information of the IPs/MACs added in this category/group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in the traffic listing, the asset is seen as Excluded without any IP-address.

### How to Configure Excluded IPs/MACs

To configure an IP / MAC as excluded, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the Excluded Assets configuration.

Network Passive Sensor		
Configuration		
Internal Assets	Excluded Assets	Monitor External Assets
<input type="checkbox"/> Actions (0) <span>Add</span>		
NAME	TYPE	IP RANGE
exclude-test-dns	IP	10.1.1.1/24
test-exclude	IP	10.1.1.1/24

Traffic summary representation for Excluded Assets:

curl 7 29 0		curl 7 29 0		Client	43.75 KB	12.98 KB	56.73 KB
TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCOL	PORT	INGRESS	EGRESS	TOTAL
Mar 02 2022 13:42	10.1.1.1	Excluded	tcp	3128	6.06 KB	1.88 KB	7.94 KB
Mar 02 2022 13:42	10.1.1.1	Excluded	tcp	3128	37.69 KB	11.1 KB	48.79 KB

### What is Monitored External

PS does not track IPs outside the inventoried and non-inventoried range and attributes them to one asset named External as explained earlier. However, the user may want to monitor traffic flows from internal assets to certain external IPs/FQDNs. For example, monitor the volume of traffic from internal assets to social media sites such as Facebook, Twitter, etc. PS provides a "Monitored External" configuration and uses FQDNs or IPs specified therein, to track traffic flows destined to an asset created per group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in traffic listing, the asset is seen as External if FQDN was added or the actual IP, if IP was added".

### How to Configure Monitor External FQDNs or IPs

Select the appliance from the Passive Sensor Module listing and navigate to its details to edit the External Assets configuration to add FQDN / IP in a group. The following screenshots shows 2 groups, each one with a unique name. PS will track traffic flows going to one of the 2 assets that represents each group.

Configuration		
Internal Assets   Excluded Assets <b>Monitor External Assets</b>		
<input type="checkbox"/> Actions (0) <span>▼</span> <span>Add</span>		
NAME	DETAILS	
social-media	31	www.facebook.com
yahoo-website		www.yahoo.com

Traffic summary representation of Monitor External Assets & External Assets:

FAMILY	APP/SERVICE	CLIENT/SERVER	INGRESS	EGRESS	TOTAL
Web Services	HTTPs	Client	10.59 MB	996.19 KB	11.57 MB

TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCOL	PORT	INGRESS	EGRESS	TOTAL
Mar 02 2022 19:01	10.1	External	top	443	8.51 MB	109.11 KB	8.62 MB
Mar 02 2022 19:01	10.1	External	top	443	15.06 KB	2.14 KB	17.2 KB
Mar 02 2022 19:00	10.1	External	top	443	6.29 KB	1.04 KB	7.33 KB
Mar 02 2022 18:57	10.1	98.137.11.165	top	443	4 KB	3.22 KB	7.22 KB
Mar 02 2022 18:55	10.1	31.13.65.36	udp	443	40.9 KB	28.5 KB	69.4 KB

External Assets Traffic
Monitor External Assets Traffic



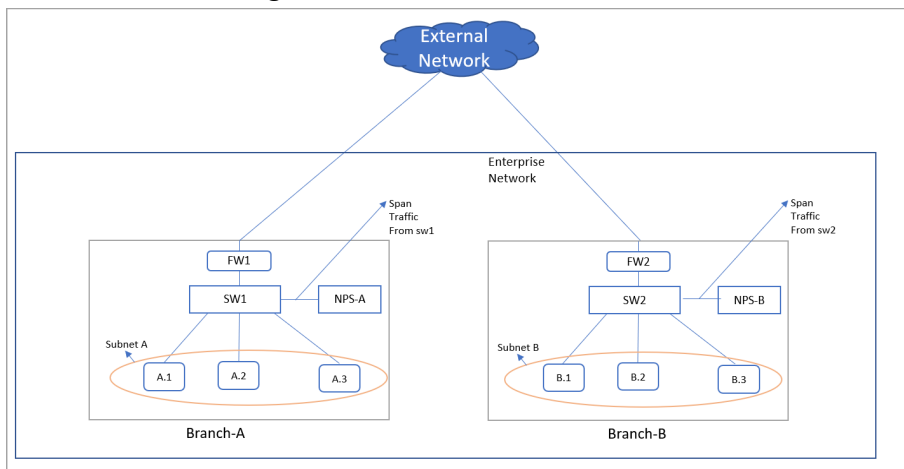
# Best Practices

This section contains certain best practices to follow when configuring the internal assets in PS appliances.

## 1. Avoid configuring overlapping subnets as internal (inventoried) assets on more than one sensor appliance

In deployments that have more than one passive network sensor appliances registered with the same Qualys cloud account, it is recommended that the configuration of internal inventory network ranges should not overlap between the sensors.

To explain this better, let us consider a sample deployment that has 2 sensors deployed in different locations registered to the same account.



The enterprise network in the above scenario has 2 branches A and B. There are 2 sensors deployed one each in branch A and B. For the enterprise network subnets A and B together make up the range on IPs for internal assets that have to be inventoried. Assets A.1, A.2, and A.3 belong to subnet A and B.1, B.2, and B.3 belong to subnet B.

Now consider a case where there is intra branch traffic. Each of the sensors in branch A and B will "see" traffic flows from/to assets in subnets A to B.

For example, if A.1 were to initiate a flow to B.1, both sensors would sense this flow. If both sensors are configured with subnet A and B as the internal (inventoried) range, then both sensors will report assets A.1 and B.1 causing the same assets to be reported twice to Qualys cloud. This causes additional workload on the cloud services and this may result in delayed or missed updates of the assets or traffic flows as seen in the asset or traffic listing.

This workload multiplies if there are flows from each one of the assets in subnet A to B.1, such as A.1 to B.1, A.2 to B.1, and A.3 to B.1.

So, adding the same subnet into multiple sensors is inefficient and not a recommended configuration.

### **Desired/Recommended configuration: Detect assets in location specific subnets and provision a "non-inventoried" asset category**

A recommended configuration to avoid duplicate processing on the cloud is to configure each sensor with a unique subnet as its inventoried range and add the other subnets internal to the organization as its internal non-inventoried range.

So in the above example, the sensor deployed in Branch A would only consider IPs of subnet A as the internal IPs and treat everything else as external. This means even subnet B which belongs to the universe on internal IPs of the organization would be considered external to the sensor in branch A. However, to track the inter-branch traffic flows so to know which asset in subnet A was talking to which asset in subnet B and vice-versa, it is recommended to add subnet B as internal (non-inventoried) range in sensor of location A. The passive sensor uses the non-inventoried range or IP to create assets whose attributes are not collected just as in the case of External assets but with a difference that its IP is recorded.

Similarly for the sensor in location B, configure subnet B as its internal inventoried range and subnet A as its internal non-inventoried range.

With the above configuration sensor in location A would report A.1, A.2, and A.3 as internal inventoried assets and B.1 as the non-inventoried assets. Similarly, the sensor in location B would report B.1 as its internal inventoried asset and A.1, A.2, and A.3 as its non-inventoried asset.

This configuration saves the PS services from the burden of additional processing. This also conserves the WAN bandwidth needed by sensors to report metadata to Qualys cloud as only one sensor reports the inventoried assets.

To summarize, the configuration of both passive sensors is as follows:

<b>Passive Sensor Appliance Location</b>	<b>Internal (inventoried)</b>	<b>Internal (non-inventoried)</b>
Branch A	Subnet A	Subnet B
Branch B	Subnet B	Subnet A

## **2. Avoid mirroring replicated IPs to a single appliance**

In topologies, more common in OT networks, multiple smaller networks can have the same IP subnet. Each such replicated IP subnets has to be mirrored to a separate PS appliance. Avoid mirroring multiple such subnets to one appliance.

For example, consider a site with a yard having many cranes and each crane is a small network having exactly the same type of devices with the same IPs configured.

The overlapping IP address space in each crane can be handled by the Network feature which the customer can subscribe to. This feature allows the same subscription to uniquely identify IP within a network.

The Network feature is already supported in VM and PC modules and is part of the PS 1.4.0.0 release. PS uses the network feature by de-duplicating passively sensed Unmanaged IPs/assets with managed assets belonging to the same Network. PS exercises the network-based merge to de-duplicate assets only when it has neither MAC nor hostname information to uniquely identify the assets for de-duplication.

So here is what the configuration of PS appliance in each crane would look like

#### Crane #1

- Add Crane#1 IP range R1 in Asset Group AG1 in Network N1 in VM module
- Run policy compliance scan for the asset group AG1 in N1 in VM module
- Add NPS1 to Network N1 and configure NPS 1 to sense IP range R1 in N1

#### Crane #2

- Add Crane#2 IP range R2 in Asset Group AG2 in Network N2 in VM modules
- Run policy compliance scan for the asset group AG2 in N2 in the VM module
- Add NPS2 to Network N2 and configure NPS 2 to sense IP range R2 in N2

### 3. Add NATed IPs in the excluded list

PS does not yet support the capability to detect NATed devices. All assets behind NAT devices get masqueraded by the NATed IP and if PS sees this NATed IP, it will associate meta-data/attributes of all such devices to a single asset which has the Nated IP, making the asset very large, and these slow down the processing pipeline on the cloud. So, it is recommended to add such IPs as internal assets to be excluded.

### 4. Do not feed multiple copies of the same packet to the sensor

It is important that the TAPs or SPAN ports that feed the traffic copy to PS do not contain duplicate copies of the same packet. This will result in PS reporting incorrect volumes of traffic flow.

### 5. Backup and restore of PS VM image

It is not recommended to backup PS VM images to be restored later. In case the VM fails to boot due to corruption, contact Qualys support instead of re-deploying the PS VM. The PS services on Qualys cloud account retains the sensor configuration and applies it to the appliance on reboot.