Network Passive Sensor

Getting Started Guide

July 21, 2021

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

Table of Contents

About this Guide

Welcome to Network Passive Sensor! We'll help you use the Network Passive Sensor to detect known and unknown devices on your network.

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 founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

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 online support information at 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.

Instant, complete detection

Qualys PS continuously monitors all network traffic and flags any asset activity. It identifies and profiles devices the moment they connect to the network, including those difficult to scan, corporate owned, brought by employees, and rogue devices. The asset metadata is sent immediately to the Qualys Cloud Platform for centralized analysis.

Continuous inventory enhancement

Qualys PS enriches existing asset inventory with additional details, such as recent open ports, traffic summary, network services and applications in use. This helps customers gain a deeper understanding of an asset and its activity on the network in near-real time.

Network Scanner and Cloud Agent complement

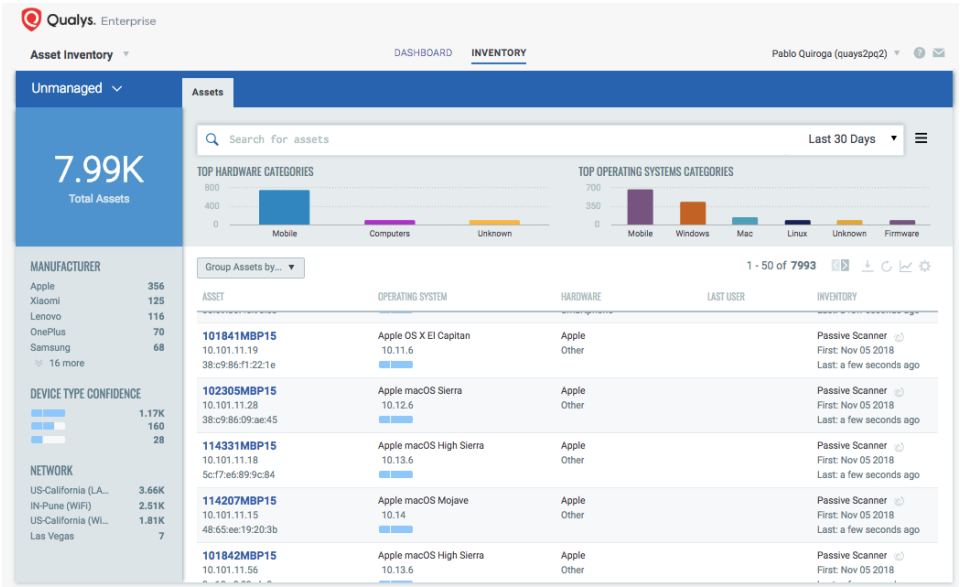
Qualys PS identifies assets that for different reasons can't be actively scanned or monitored with agents. That's often the case with assets like industrial equipment, IoT and medical devices.

Centralized control and visibility of assets

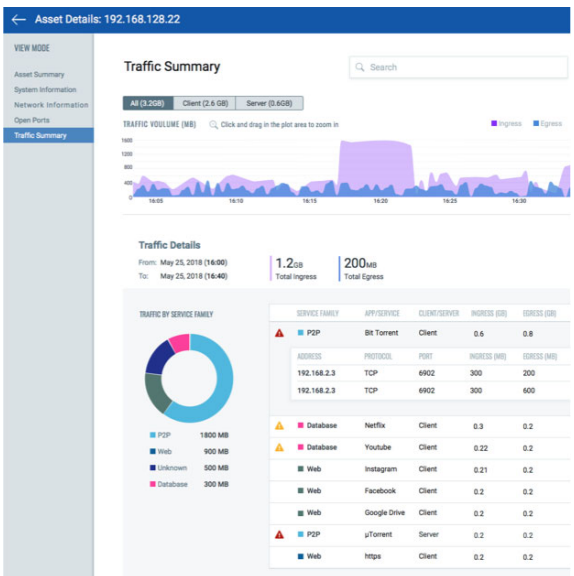
The Qualys Asset Inventory cloud app aggregates and correlates the data gathered by all Qualys sensors – Qualys Passive Sensors, the Qualys network scanners and the Qualys Cloud Agent – giving you a comprehensive, detailed inventory of all your hardware and software, as well as a multi-dimensional view of your global, hybrid IT environment.

What are the benefits?

You'll get complete visibility into managed and unmanaged assets, including asset details like hostname, operating system, device manufacturer and model, open ports, network services and much more.



Passive Sensor analyzes existing network traffic without sending a single packet to the devices being discovered.



Get insights to the asset's network activity, with traffic summary categorized by ingress/egress, service type, and port/protocol.

Drill down to traffic between a source and destination. You'll get enterprise application identification (e.g. database) based on traffic pattern.

How it works

The Network Passive Sensor is placed inside your network and takes snapshots of the data flowing over the network. It extracts metadata from these snapshots and sends them to the Qualys Cloud Platform for analysis. This allows us to then catalog assets by operating system and hardware.

All assets discovered by Network Passive Sensor are reported to Qualys Asset Inventory where you can see information about them.

If an asset discovered by the sensor is already known by active scans or by cloud agent then it is considered a managed asset and the asset data is correlated and merged using MAC or hostname as a criteria. So, if the MAC or hostname of passively sensed asset matches with that of the managed asset, then two assets are merged and shown in the **Managed** inventory.

The hostname based merge relies on exact match. Hence, in the case where passive sensor sensed "johndoe" as the hostname and the managed assets' hostname is reported as "johndoe.somedomain.org" and vice-versa, the assets will not merge. The asset reported by the passive sensor is placed in the **Unmanaged** inventory, if

- it is not detected by active scan

- it is detected by active scan but not merged

Sensor deployment options

Qualys Network Passive Sensor is available as both a physical and virtual appliance.

- Physical Appliance: 1Gbps, 4Gbps, and 10Gbps appliance

- Virtual Appliance: Support for VMware ESXi (6.0 and above) and Microsoft Hyper-V

Operational Mode: Out of band - fed by tap, span or packet broker

Centralized sensor management, including software updates, from the Qualys Cloud Platform for convenience.

Appliance connectivity and interfaces

The appliance has two types of interfaces: management interface and sniffing interface.

Management Interface

The management interface is used for connecting to the Qualys Cloud Platform and for streaming asset metadata to the Qualys Cloud Platform, as well as performing management and maintenance activities remotely from the Qualys UI.

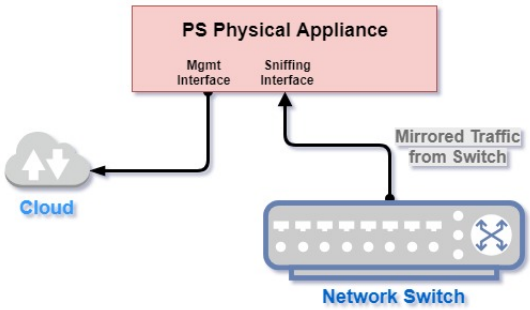
You'll assign an IP address to the management interface either statically or using DHCP. DHCP is enabled by default. Configuring the management interface is required for the Passive Sensor to have Internet connectivity and to connect to the Qualys Cloud Platform.

Sniffing Interface

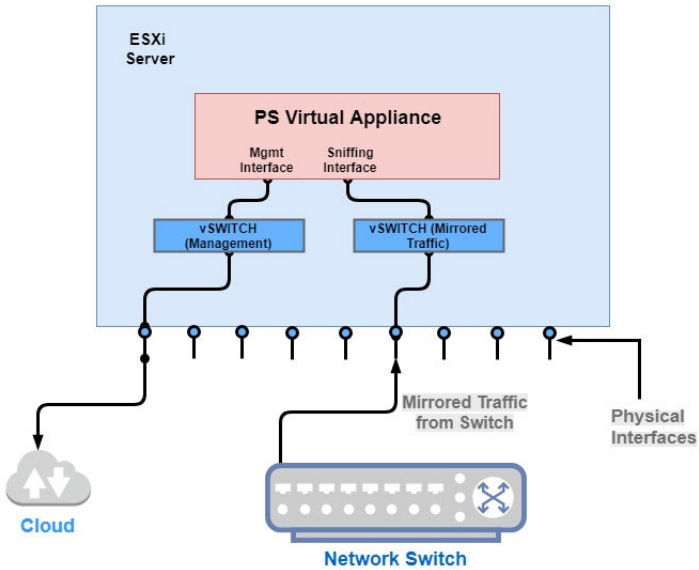
One or more traffic sniffing interfaces are used to receive mirrored traffic to the Network Passive Sensor. Once the traffic that needs to be monitored is identified: 1) Configure the switch that sees the traffic in question by mirroring the traffic to a port, 2) Connect that mirrored port to the passive sensor sniffing interface of the sensor, and 3) Enable "Promiscuous Mode" on respective vSwitch and port group.

You will not assign an IP address to the sniffing interface.

The following picture shows connectivity for a physical appliance. You'll see that the sniffing interface of the appliance is connected to the network switch and mirrored traffic is fed from the switch to the appliance. The management interface connects to the cloud.



The following picture shows connectivity for a virtual appliance. The virtual appliance is supported on the VMware ESXi Server virtualization platform and Microsoft Hyper-V. Again the sniffing interface is fed mirrored traffic from the network switch. The management interface is configured to connect to the cloud.



Network placement and sensor sizing

It's best to position passive sensors at points in the network that see maximum aggregate traffic. For effective traffic monitoring, passive sensors should be attached to tap/span ports of distribution switch/routers in the network.

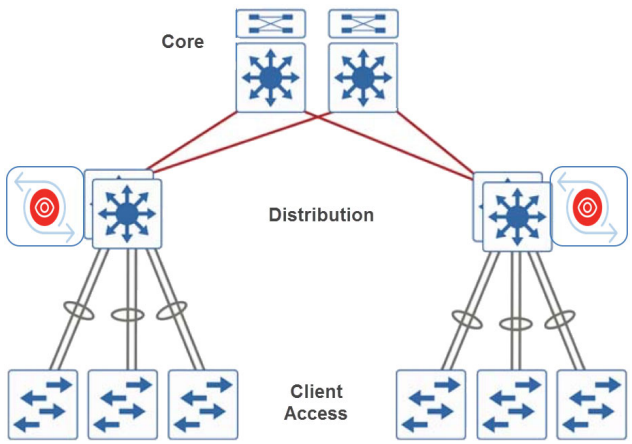
What size do you need?

You'll want to consider the traffic throughput at the deployment points, the need for accurate coverage of all assets and total count of all assets. Typically passive sensors with 1G interfaces would be sufficient for an aggregate traffic that does not exceed 900 Mbps from an average of up to 3,000 assets.

Where should you attach passive sensors?

Passive sensors attached to core switch/routers may not have visibility into the local traffic of the distribution switch, i.e. traffic between assets attached below the same distribution switch. Passive sensors attached to distribution switches will provide much better accuracy and visibility. Multiple passive sensors may have to be deployed depending on the network topology.

The following diagram shows passive sensors at the distribution layer. In this example, the traffic from all devices in the Client Access network gets aggregated at the distribution switches and traffic from the distribution switches gets aggregated at the core switch.



Quick Steps

You'll deploy the appliance on your network, generate a personalization code, and use the code to register the appliance with the Qualys Cloud Platform.

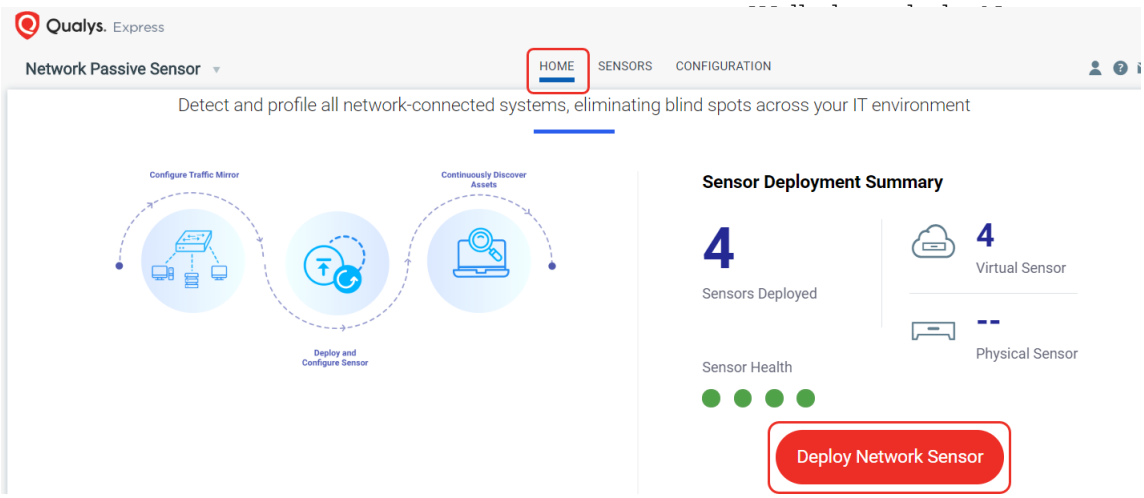
Before you begin - Mirror the traffic

You need to feed traffic to the sensor by mirroring the traffic (using physical tap or mirror port). Then 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.

Step 1 - Generate a personalization code

Each sensor needs a unique personalization code to register it with the Qualys Cloud Platform. Log into the Qualys UI and pick the **Network Passive Sensor** app. On the **Home** screen, choose **Deploy Network Sensor** OR on **Sensors** tab, choose **New Sensor** and pick **Physical Sensor** or **Virtual Sensor**.



Step 2 - Deploy and register the appliance

Add the appliance to your network and make network configuration settings.

Physical Appliance

Depending on your appliance variant (with LCD or without LCD), you can do your configurations using LCD interface for using remote console connected using serial port.

Configurations using LCD interface - Plug-in the physical appliance on your network. Then use the LCD display on the appliance to make network configuration settings (static IP, proxy). You'll also register the appliance using the personalization code copied from Step 1 by entering it using the LCD display on the appliance. Refer to the Physical Appliance User Guide for the detailed steps.

Configurations using serial port- Plug-in the physical appliance on your network. Then use PuTTY to connect using serial port and to display remote console for network configuration settings (static IP, proxy). You'll also register the appliance using the personalization code copied from Step 1 by entering it using the option in the remote console. Refer to the Physical Appliance User Guide for the detailed steps.

Virtual Appliance

Download the virtual appliance image from the New Sensor wizard or from Home > Deploy Network Sensor > Virtual Sensor in the Network Passive Sensor UI and deploy it in VMware ESXi or Microsoft Hyper-V. When you start up the new virtual machine a virtual console window appears where you'll make network configuration settings (static IP, proxy). You'll also register the appliance using the "Personalize this scanner" option in the console window. Refer to the Virtual Appliance User Guide for the detailed steps.

Step 3 - Configure assets

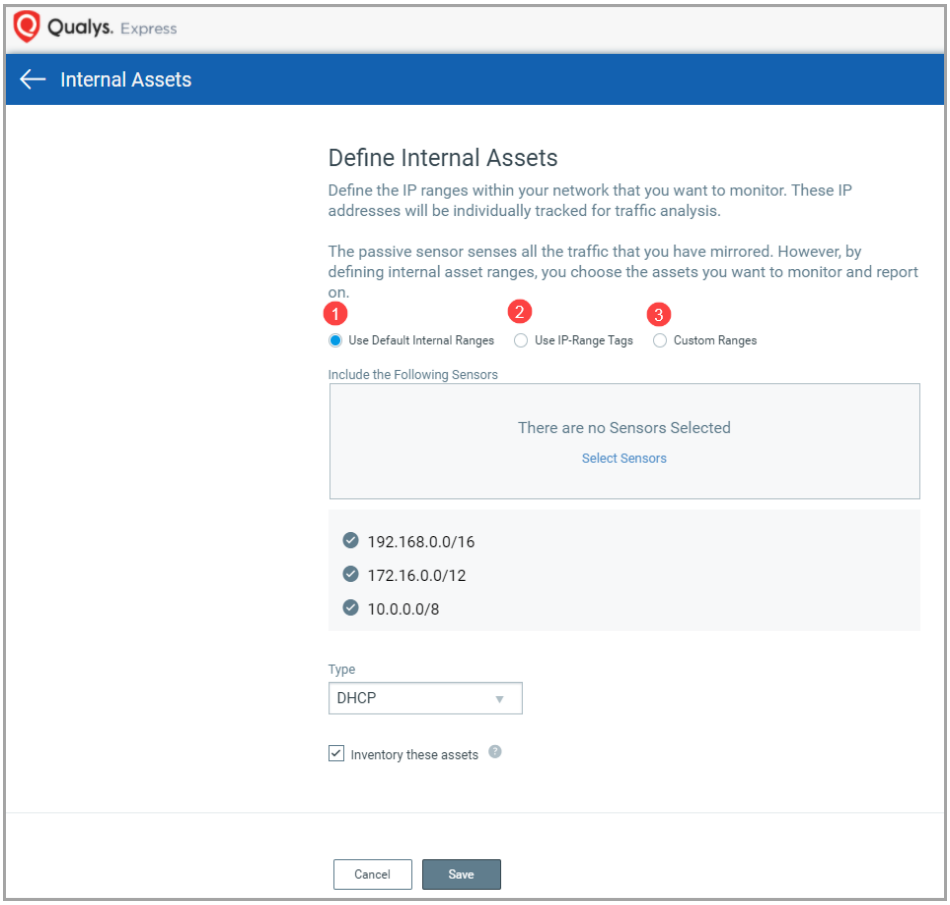
Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

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 IT Asset Inventory**.

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

Internal Assets

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

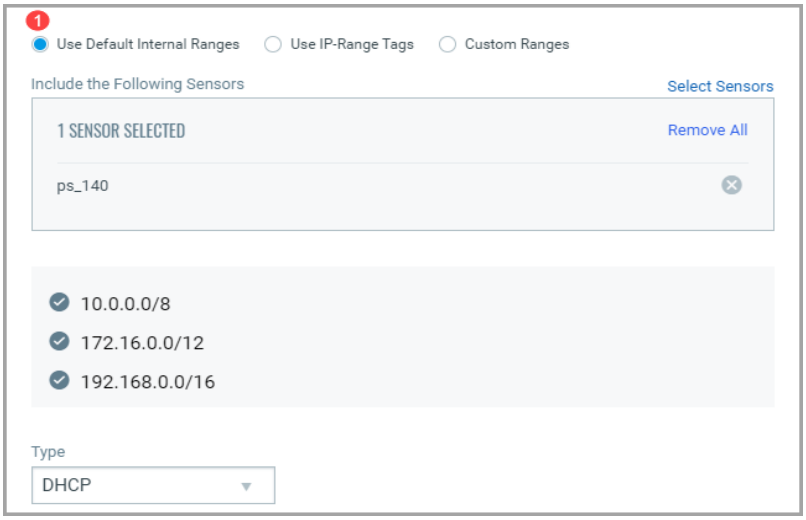


Here, you'll define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges, IP range tags, or customized IP ranges options to define range of internal assets. Select **Inventory these assets** check box for marking inventoried assets.

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.

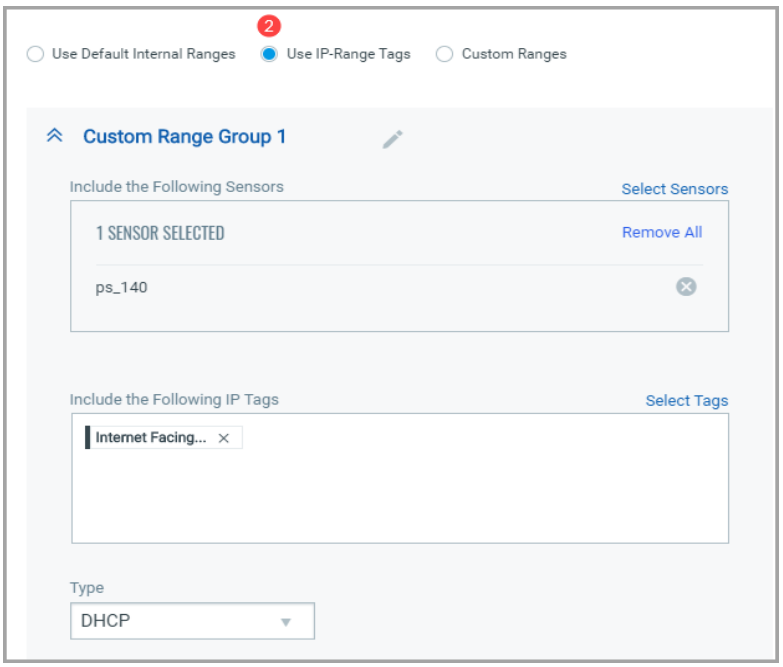
1 - Use Default Internal Ranges

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.



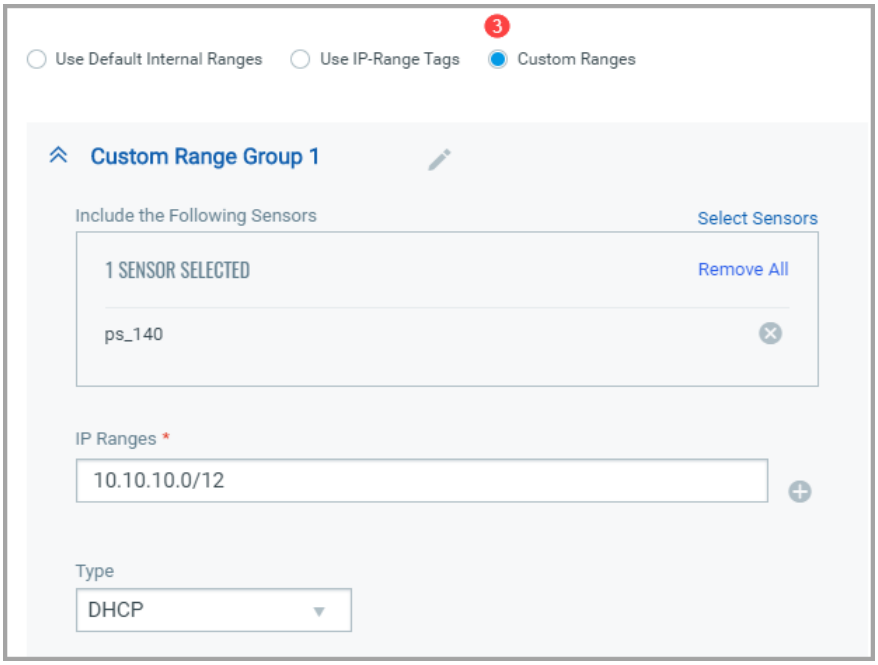
2 - Use IP-Range Tags

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 Tags** to select IP tags from the list of tags for which you want to define internal asset.



3- Custom Ranges

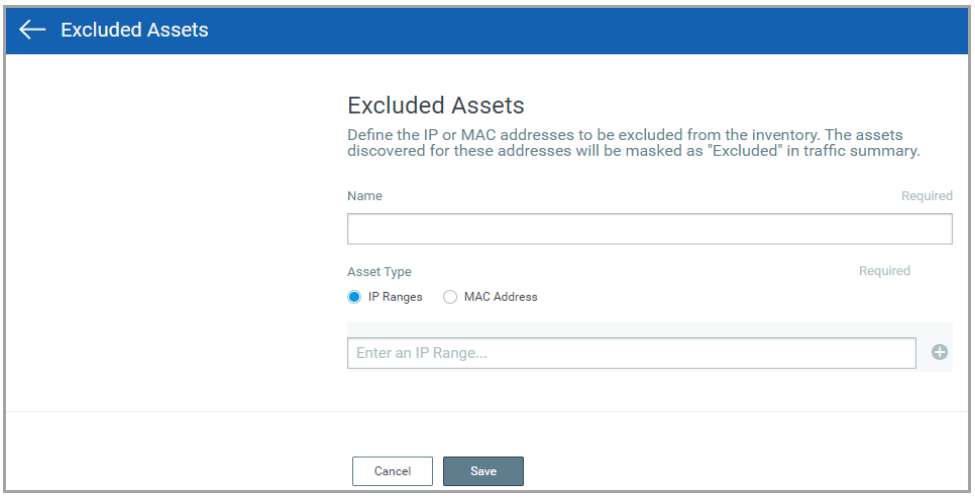
This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.



Excluded Assets

Here, you'll 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.

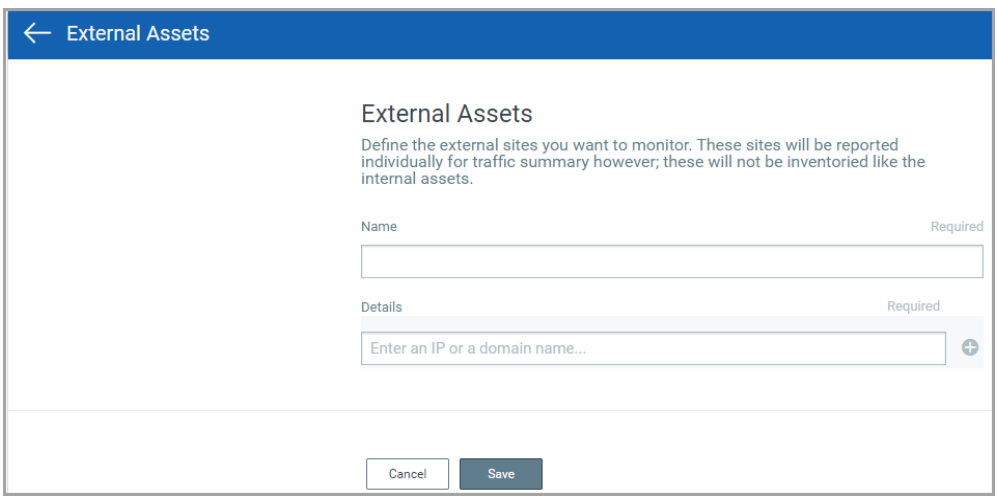
To add excluded assets, simply go to **Configuration** > **Excluded Assets** > **Add**.



External Assets

Here, you'll 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.

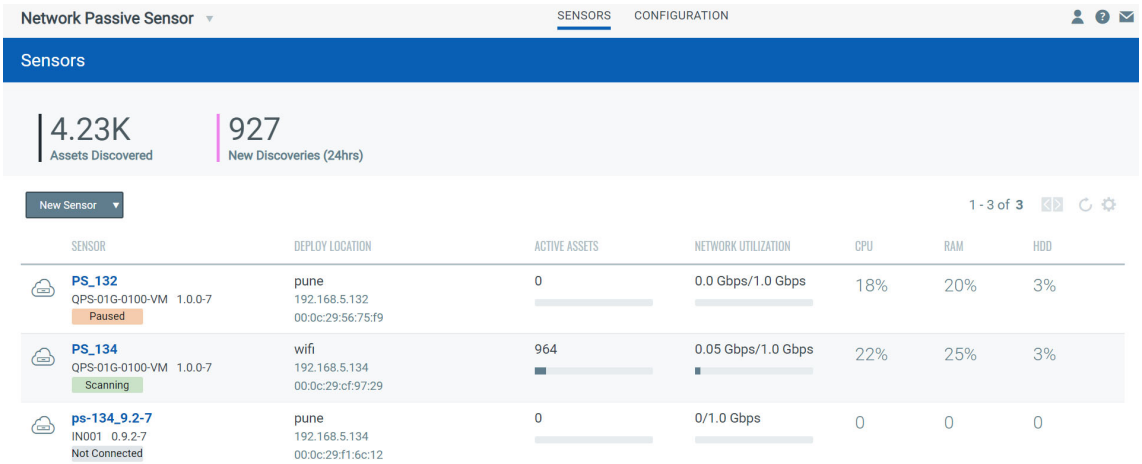
To add external assets, simply go to **Configuration** > **External Assets** > **Add**.



Step 4- Check the status

Your sensor needs to successfully connect to the Qualys Cloud Platform to start discovering assets. The **Sensors** tab in the **Network Passive Sensor** UI shows the status for each sensor that's been added.

Once connected, the sensor will start reporting new discoveries. On the Sensors tab you'll see the count for total assets discovered and assets discovered in the last 24 hours.



Step 5- View asset details in Asset Inventory

Network Passive Sensor reports all discoveries to Qualys Asset Inventory, where discoveries are first checked against the existing list of managed assets. Assets that are already known by active scans or from cloud agents are considered managed assets. When such assets are found by the sensor, the asset data is correlated and merged. Assets that are previously unknown are considered unmanaged assets.

You can toggle your view between managed and unmanaged assets at any time.