Network Passive Sensor

Virtual 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

About this Guide **4**

Welcome to Qualys Network Passive Sensor **5**

Network requirements / configuration 5
Get Started 5
- Mirror the traffic 6
- Step 1 - Download Virtualization Image 6
- Step 2 - Generate Personalization Code 6
- Step 3 - Deploy Virtualization Image 7
- Step 4 - Register the Virtual Appliance 15
- Step 5 - Check the Status 16
- Manage Sensors 17
- Configure Assets 19

Network Configurations **27**

Configure Static IP Address 27
Proxy Configuration 28

Appendix **29**

Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resources 29
Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware 29
Adding/Removing Sniffing Interfaces from Virtual Appliance 33
Classification of Assets in Passive Sensor 37

Best Practices **43**

About this Guide

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to set up your virtual appliance for Qualys Network Passive Sensor.

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.

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/.

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.

Virtual Appliance supports a maximum throughput of 2Gbps. It can be scaled up or down depending on the resources allocated to it. Refer to the Appendix section for more details.

It's easy to set up a virtual appliance. We'll help you with the steps.

Network requirements / configuration

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 (port 443) access to the Internet, so that the Network Passive Sensor can communicate with the Qualys Cloud Platform. Tip - Log into your account and go to Help > About to see the Qualys Cloud Platform URLs.
DHCP or Static IP	By default the Network Passive Sensor 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 Network Passive Sensor 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

Network Passive Sensor will start discovering assets on your network once you complete the setup. It takes just a couple of minutes. It's important that you complete the steps in the order shown.

Mirror the traffic

You need to feed traffic to the appliance by mirroring the traffic (using physical tap or mirror port). Connect the mirrored port to the sniffing interface of the appliance. 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 - Download Virtualization Image

1) Log in to the Qualys UI and select **Network Passive Sensor** from the app picker.

2) On the **Home** tab, scroll down and click **Deploy Network Sensor**.

3) From the **Sensors** tab, go to **New Sensor** > **Virtual Sensor** and then click **Download** link from Deploy Image step of the New Virtual Sensor wizard. For VMWare ESXi, you can download the image (OVA file) to your local system. For Hyper-V, you can download zip file of the Hyper-V image. Click **I Agree** from **Review and Agree to Virtual Scanner License** popup. The image download will start.

Step 2 - Generate Personalization Code

You'll need a unique personalization code to register your appliance with the Qualys Cloud Platform. Follow these steps to generate a personalization code:

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** > **Virtual Sensor** to register a new sensor.

3) In the **New Virtual Sensor** wizard, provide a name for your sensor and the location. Click the **Generate Code** button. **Copy the code and keep it handy. You'll need it later.**

4) Click **Next** to go to the Installation screen. If you have not downloaded image from Home screen, you'll be able to download it form there.

5) Click **Next** to go to the Define Internal Assets screen. 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 or use customized IP ranges. Select **Inventory these assets** check box for marking inventoried assets. You'll be able to apply existing tags to these assets. To configure internal, external and excluded type of assets, refer Configure Assets.

6) Click **Finish** to complete the registration steps. A pop up will be shown with Sensor not connected text. Now complete the next steps and the sensor status will change once registration is successful in Step 4 - Register the Virtual Appliance.

Step 3 - Deploy Virtualization Image

You can deploy the image on the VMware ESXi or Microsoft Hyper-V. VMware ESXi or Microsoft Hyper-V monitors the network activity without any active probing of the device in order to detect the active assets on the network. It identifies the key device attributes that help the web services on the cloud to catalog the devices into operating system/hardware.

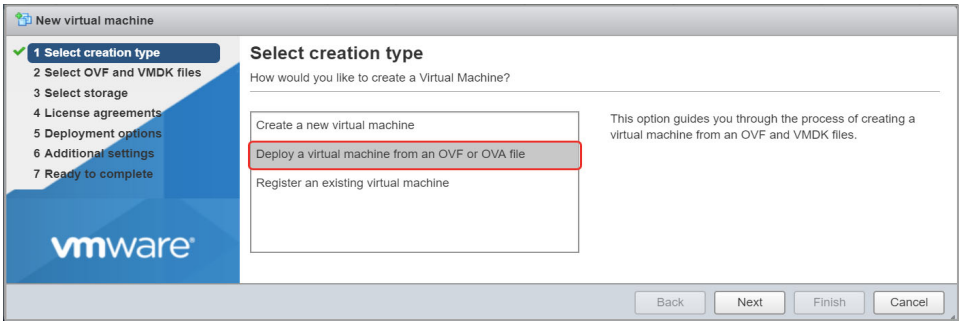
Deployment on VMware ESXi

ESXi server requirements: VMware ESXi 6.0 or later, 50 GB HDD, 16 GB Memory, Octa-Core Processor

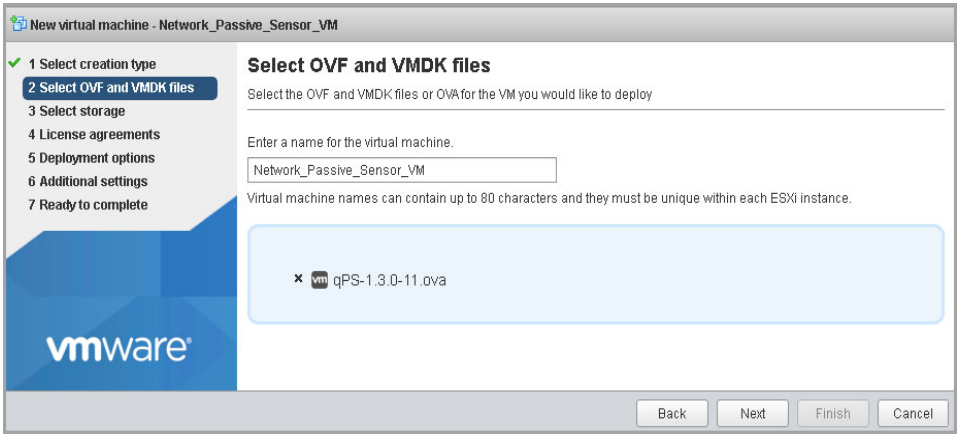
Follow these steps to deploy an image on ESXi server:

1) Login to your ESXi Server, and go to **Virtual Machines** > **Create/Register VM**. It will open New Virtual Machine wizard.

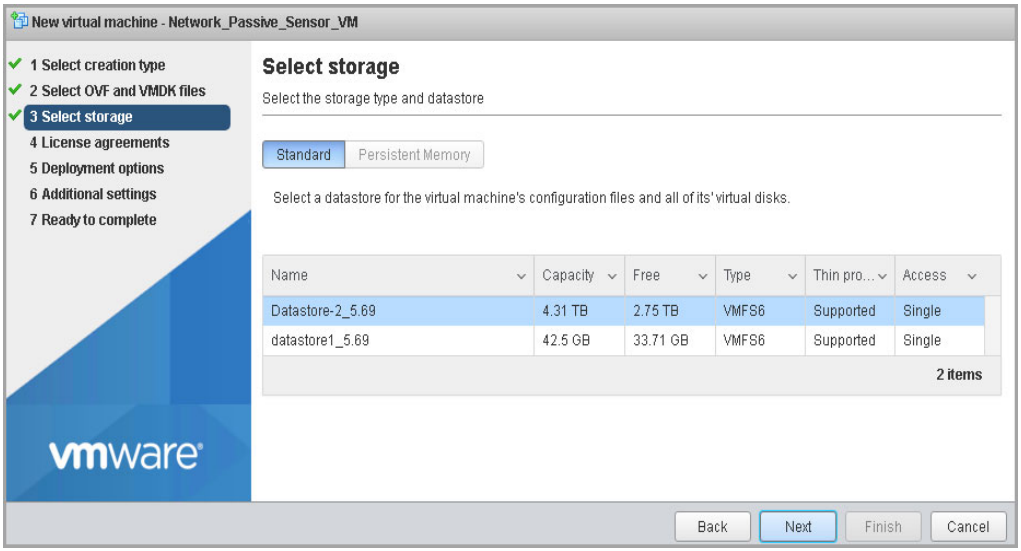
2) For creation type, choose **Deploy a virtual machine from an OVF or OVA file**.



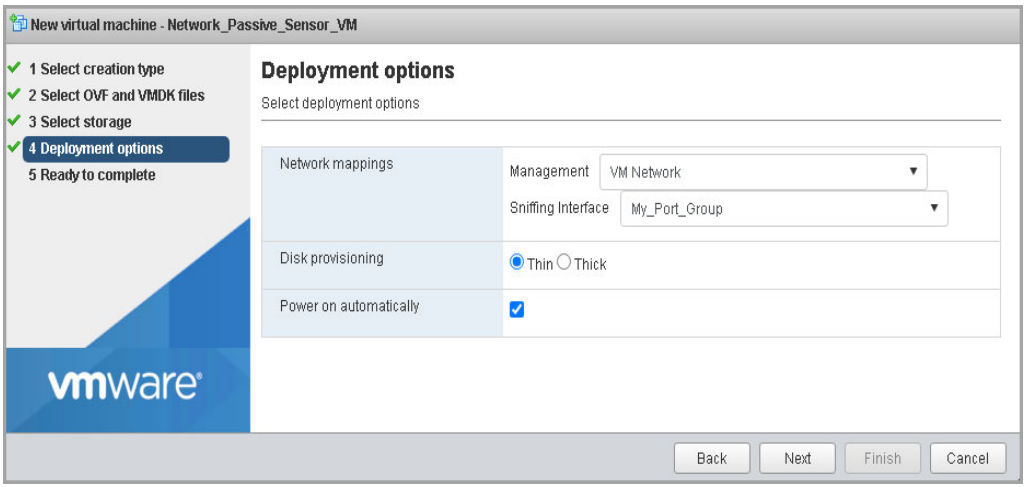
3) Click **Next** and enter a name for your virtual machine. Select or drag/drop the virtual sensor image you downloaded in Step 1 - Download Virtualization Image.



4. Click **Next** and select the destination datastore for the virtual machine configuration files and all of the virtual disks.



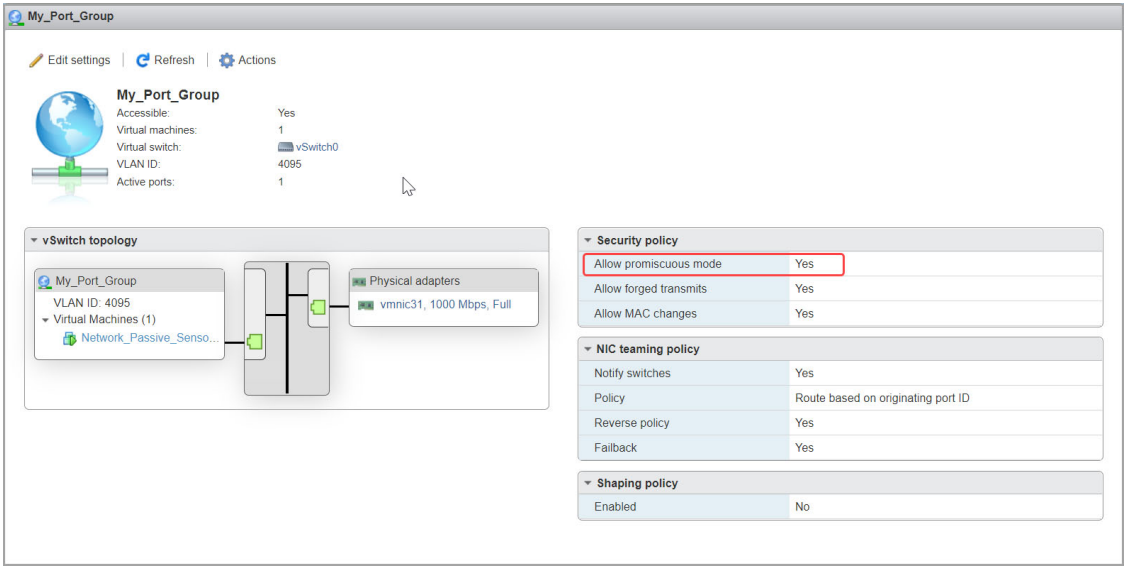
5. Click **Next** to go to the **Deployment Options** page. The OVA file creates a VM with two interfaces - Management and Sniffing.



The Management interface is required to connect the virtual appliance to the Qualys Cloud Platform. Make sure the Management interface is connected to the pre-configured port group having WAN or Internet connectivity.

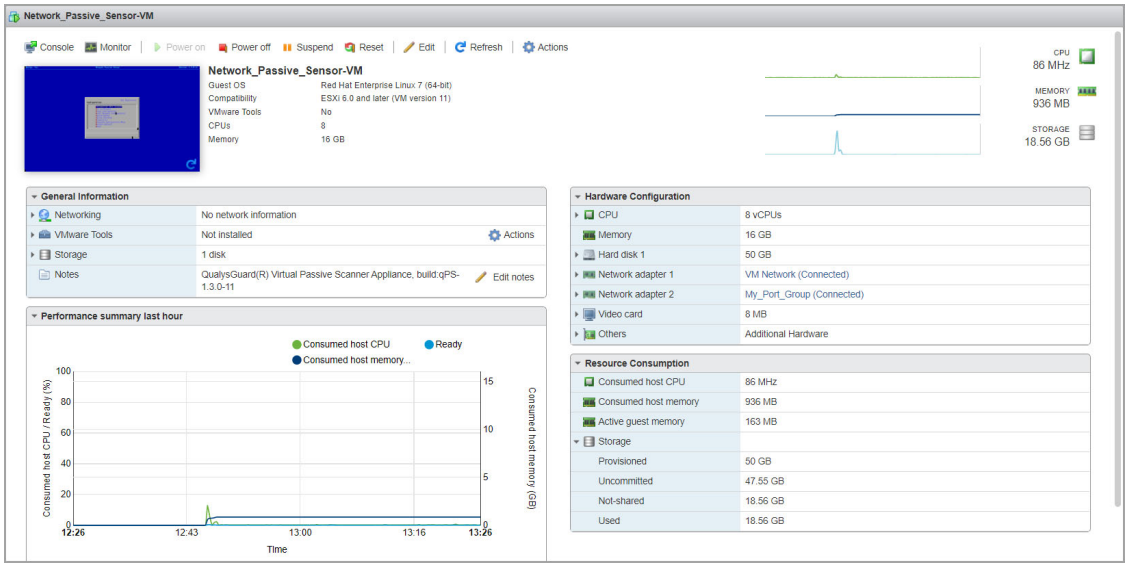
The Sniffing interface is used by the appliance to inspect the traffic. Make sure the Sniffing interface is connected to the pre-configured port group having TAP/TUN interface. Also make sure that “Promiscuous Mode” is enabled on respective vSwitch and port group.

Following screen shows typical vSwitch topology with port group settings.



6. Click **Next** and review the settings configured earlier. Click **Finish** and wait for some time to complete the virtual appliance deployment using OVA.

7. Once the deployment is complete, open the virtual appliance console by selecting the VM and navigating to **Console** > Open browser console. Wait while the VM boots up.



8) There are some network configuration settings (static IP, proxy) you'll need to set before proceeding to the next step. Complete Network Configurations.

Deployment on Microsoft Hyper-V

Hyper-V server requirements: Microsoft Hyper-V 2012 R2 or later, 50 GB HDD, 16 GB Memory, Octa-Core with total 14 GHz dedicated CPU Clock Processor

Follow these steps to deploy an image on Hyper-V server:

1) Login to your Hyper-V Server and go to **Start** > **Server Manager** > **Tools** > **Hyper-V Manager**. Right-click your Hyper-V host and select **New** > **Virtual Machine.**

2) For Specify Name and Location, provide the name that will be displayed on Hyper-V Manager and select the location where virtual machine will be stored.

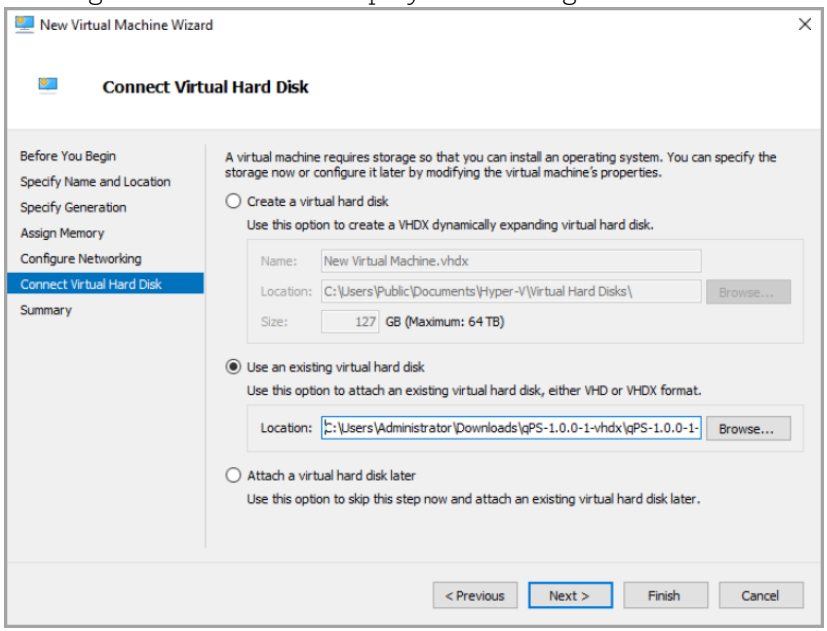
3) For Specify Generation, select the appropriate generation(recommended - Generation 1) for the virtual machine.

4) For Assign Memory, provide appropriate memory (RAM) for the virtual machine. Minimum recommended RAM is 16384 MB.

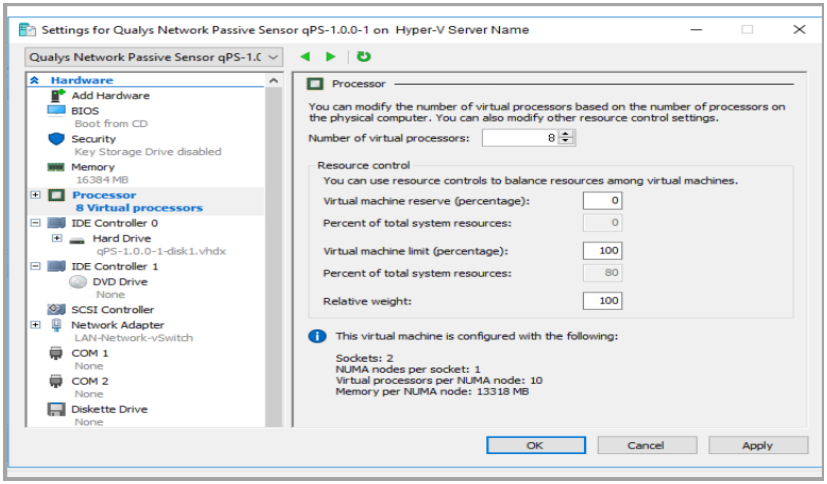
5) For Configure Networking, select appropriate virtual switch with Internet connectivity so that the network adapter on the sensor can use a virtual network for communication with Qualys cloud platform.

6) For Connect Virtual Hard Disk, select “Use an existing virtual hard disk” and provide the location of the .vhdx file (Unzip the zip file downloaded in Step 1 - Download Virtualization Image to obtain the virtual hard disk file. As an example, unzip qPS-1.0.0-1-vhdx.zip to obtain the virtual hard disk qPS-1.0.0-1-disk1.vhdx).

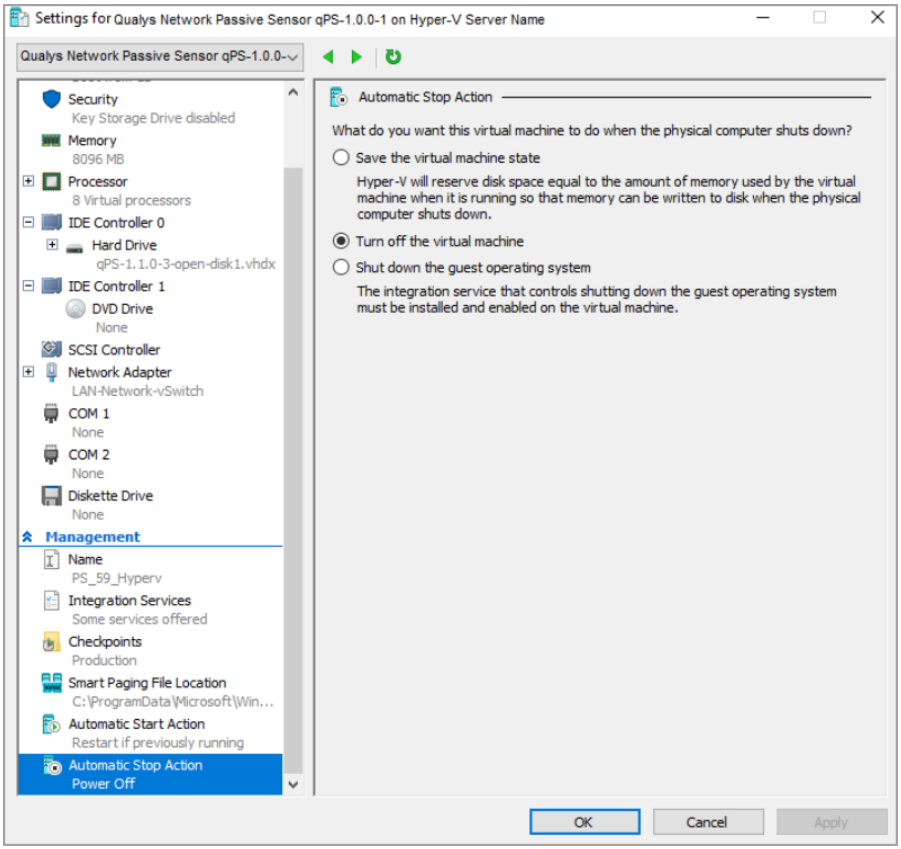
7) Click **Next** and review Summary. Click **Finish** and your virtual machine is ready. Following screen shows the deployment configurations.



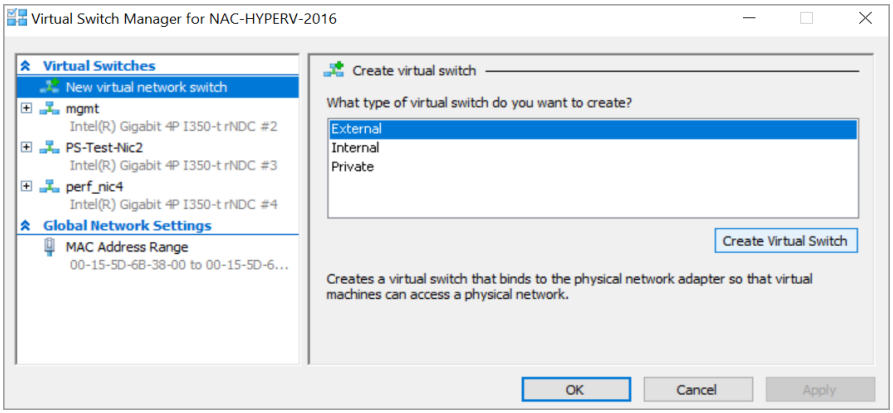
8) Select the virtual machine (just created) and navigate to Settings. Change default number of virtual processors to 8.



9) Make sure that “Automatic Stop Action” the VM is set to “Turn off the virtual machine” and apply changes.



10) Navigate to **Virtual Switch Manager** and create a new virtual network switch > Select type of switch as **External**.

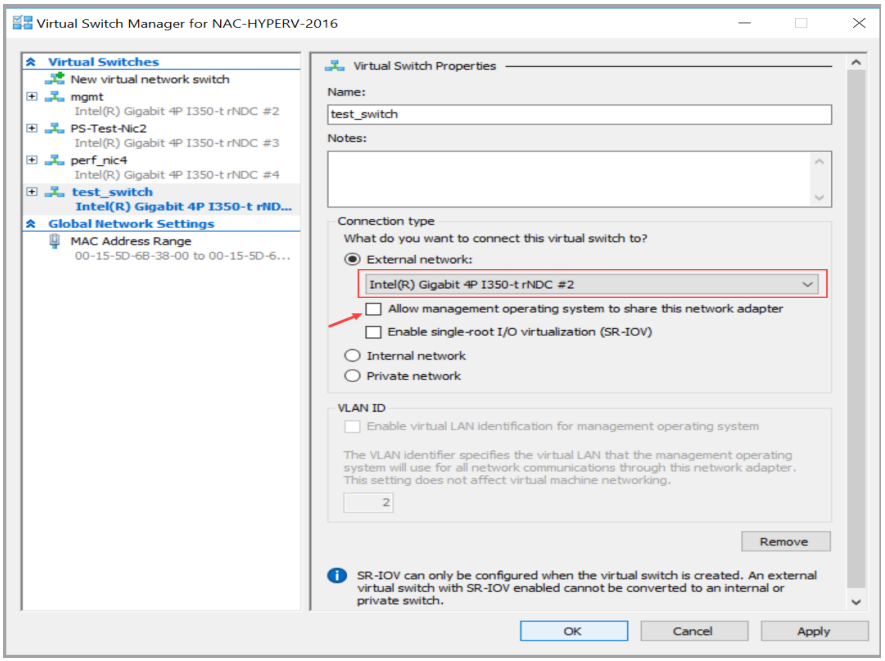


11) Give a name to the virtual switch, e.g., “test_switch”.

12) Select the appropriate external physical **NIC** interface to connect the virtual switch from the drop-down menu.

13) Uncheck the option **Allow management operating system to share the network adapter**.

14) Click OK.



15) In Powershell, execute the following commands:

- Set the port feature property to the virtual switch created.

```
$portFeature = Get-VMSystemSwitchExtensionPortFeature -
FeatureName "Ethernet Switch Port Security Settings"
```

- Configure the port monitor mode.

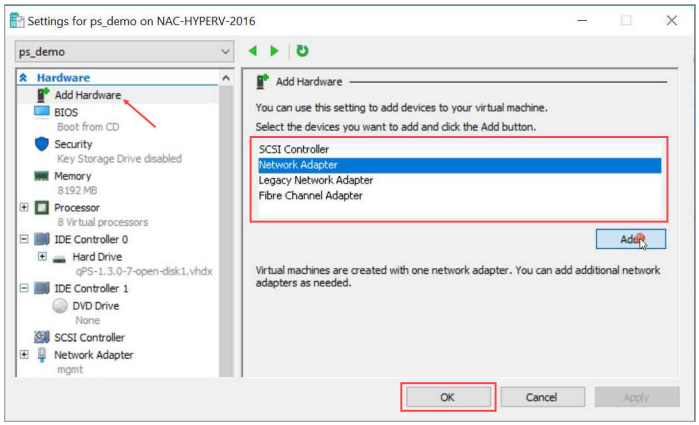
```
$portFeature.SettingData.MonitorMode = 2
```

- Use the same switch name as defined earlier

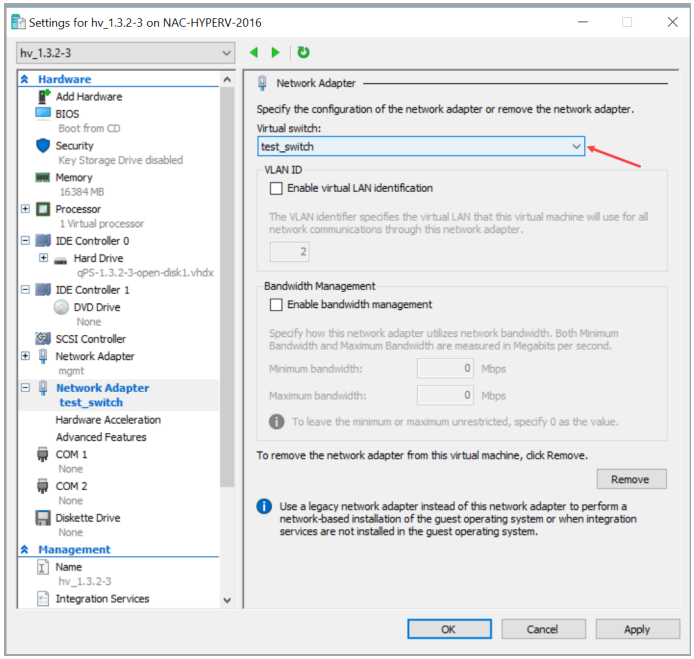
```
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
test_switch -VMSwitchExtensionFeature $portFeature
```

16) Select the virtual machine and go to **Settings**.

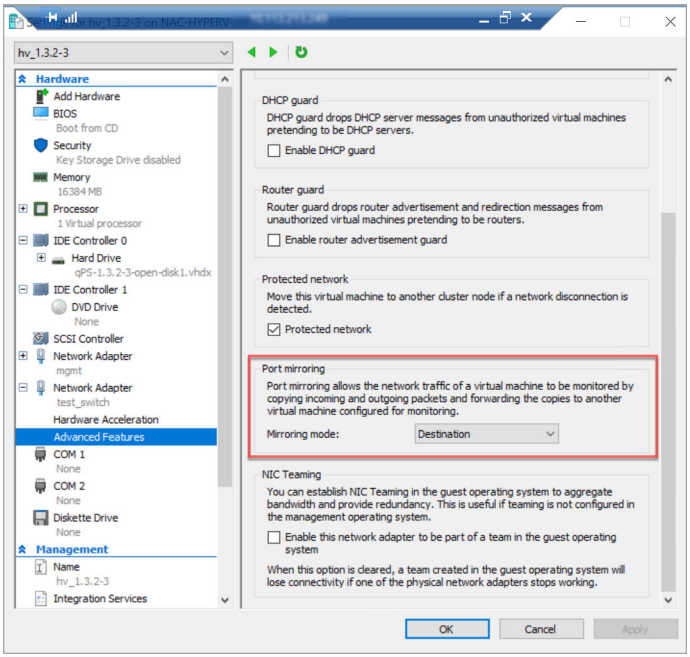
17) Go to **Add Hardware** > Select **Network Adapter** > Click **Add** > Click **OK** to add new network adapter in Hyper-V.



18) Select the second Network Adapter tab from the drop-down > Select the newly created virtual switch (**test_switch**).



19) Go to **Advanced Features** > Select **Destination** from Mirroring Mode drop-down in Port Mirroring Section.



20) Power on the VM.

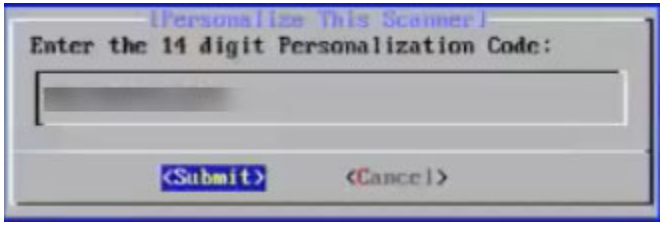
21) There are some network configuration settings (static IP, proxy) you'll need to set before proceeding to the next step. Complete Network Configurations.

Step 4 - Register the Virtual Appliance

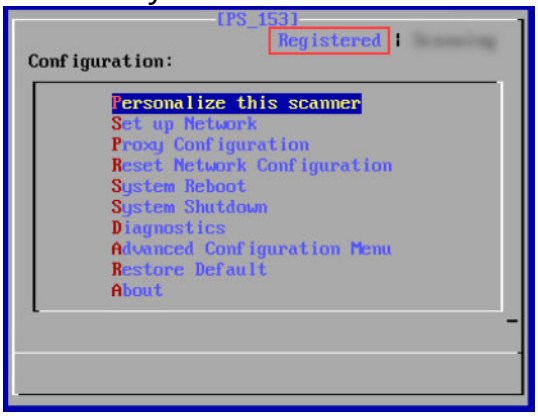
1) Open the Virtual Appliance console by selecting the VM and then navigating to **Console** > Open browser console.

2) Choose the **Personalize this scanner** option.

3) Enter your 14 digit personalization code which you generated in Step 2 - Generate Personalization Code.



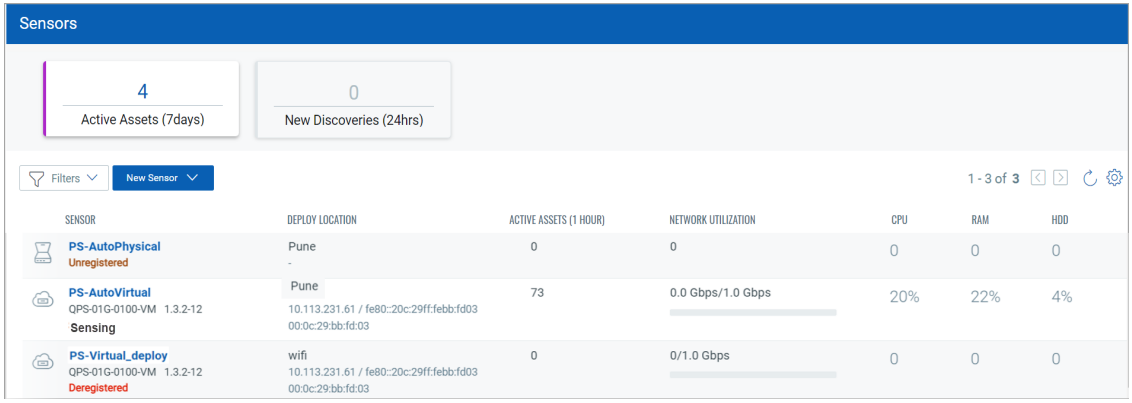
4) Click **Submit** and wait for the confirmation message **Appliance registration completed successfully**. Check that the status on the console is Registered.



5) Once your appliance successfully registers to the Qualys Cloud Platform, you'll start seeing appliance with status as paused.

Step 5 - Check the Status

Log in to the Qualys UI and select **Network Passive Sensor** from the application picker. Navigate to the **SENSORS** tab to view list of sensors in your account and their status.



You'll see the status for each appliance in the list: Paused, Sensing or Not Connected.

If the status is **Unregistered**, you can view details for the sensor and deregister.

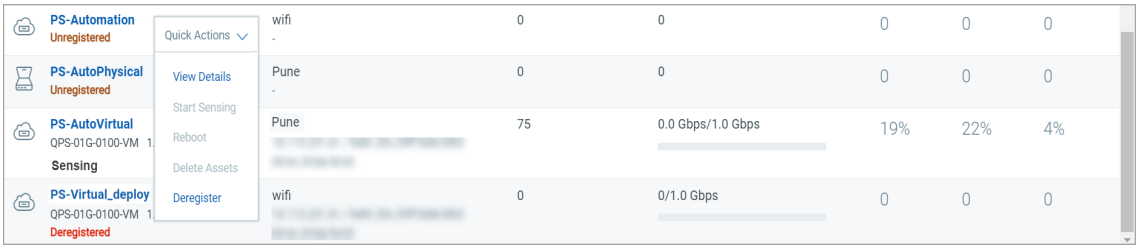
If the status is **Sensing**, you can view details and pause the sensing.

If the status is **Deregistered**, you can view details for the sensor and delete Sensor.

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.

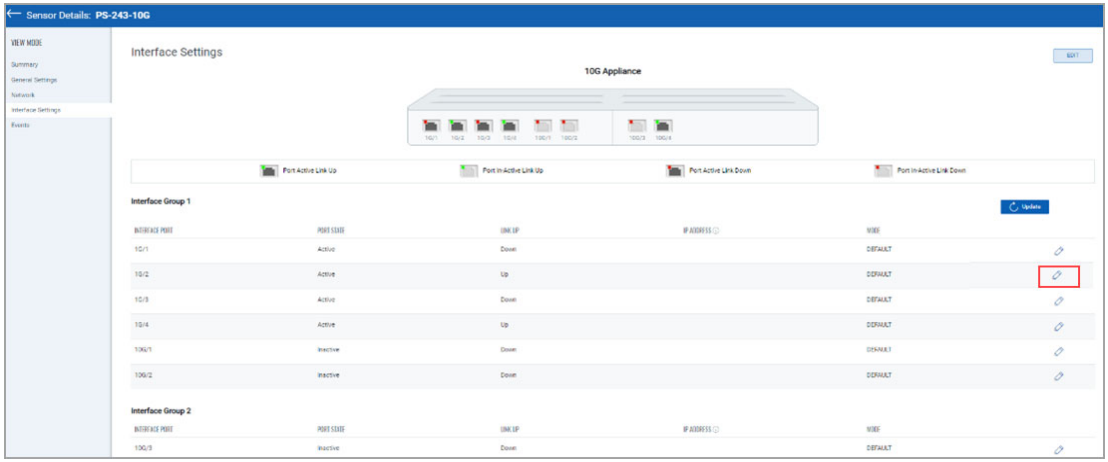


For more detailed information about the **Sensors** tab, refer to online help.

Assigning/Removing IP Addresses to the Appliance Sniffing Interfaces

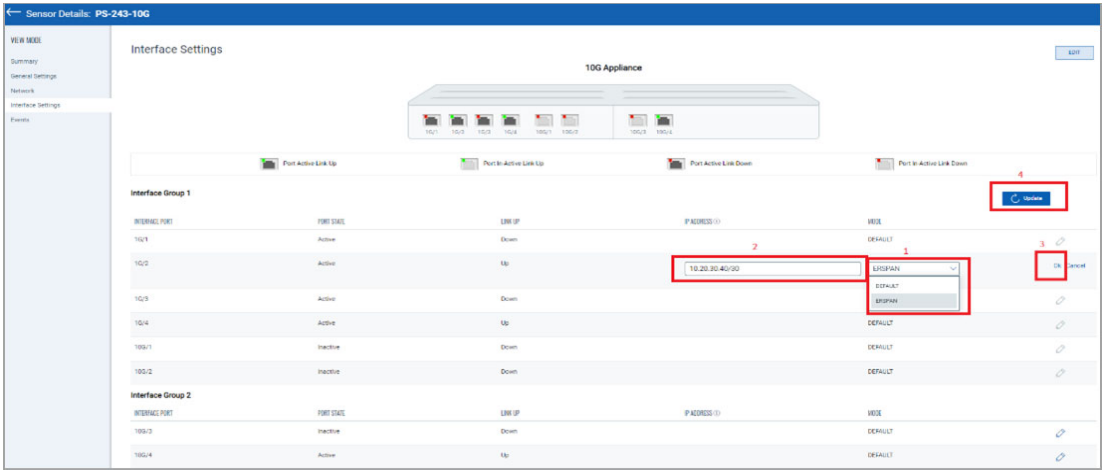
To assign or remove the IP address from the appliance sniffing interface, go to the **Sensors** tab and from the Quick Actions menu of a sensor, click **View Details** > **Interface Settings**. Alternatively, you can click on the sensor to go directly to the sensor view details page.

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



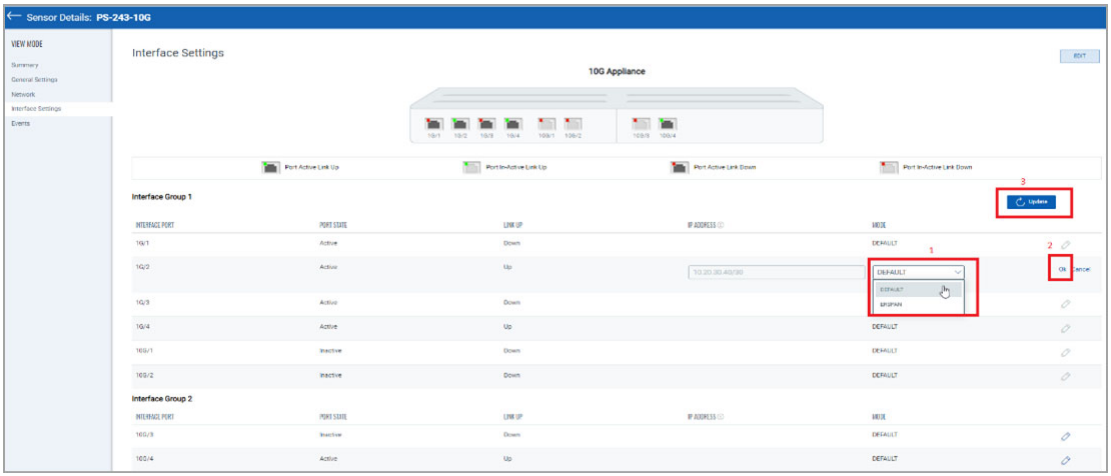
Select **ERSPAN** mode and assign IP to the interface along with subnet mask.

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. As shown in the above screenshot.

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



Important:

- 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

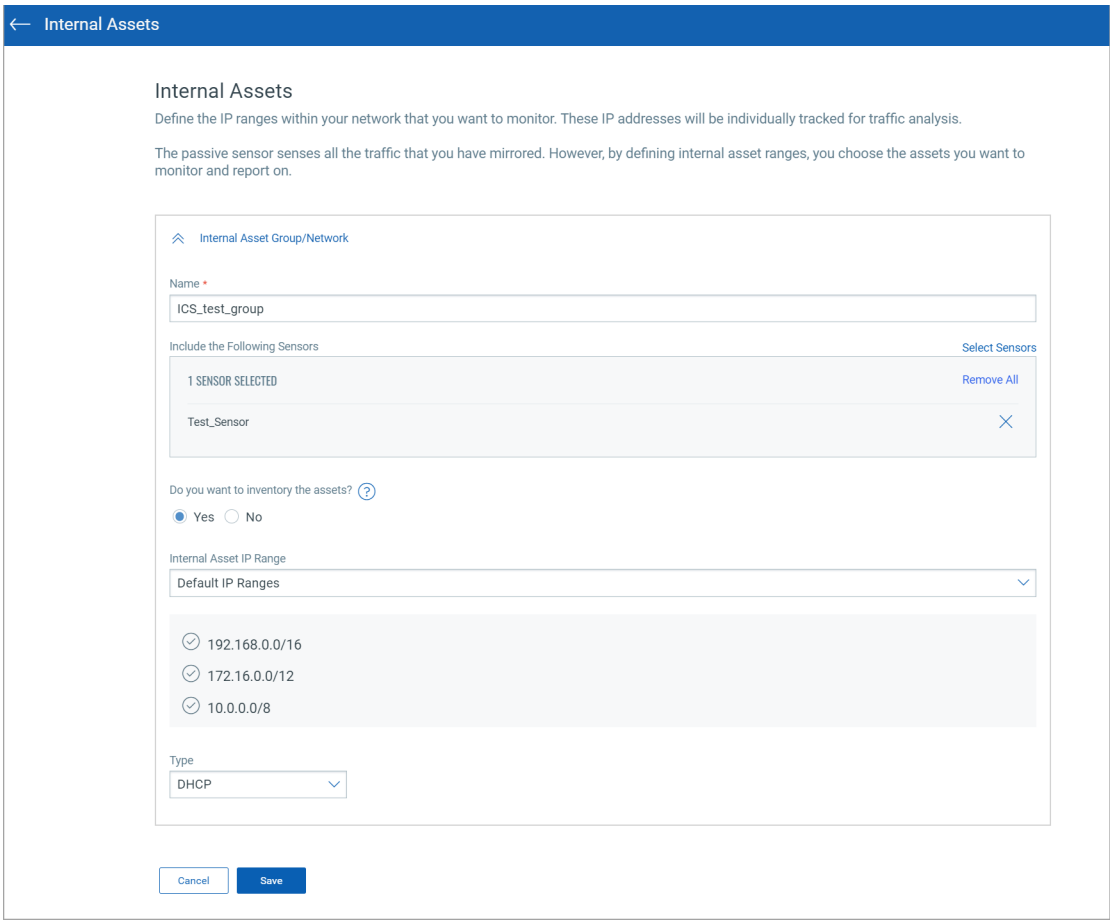
Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

You can configure how you want to categorize your assets discovered by the sensors while monitoring traffics 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**.



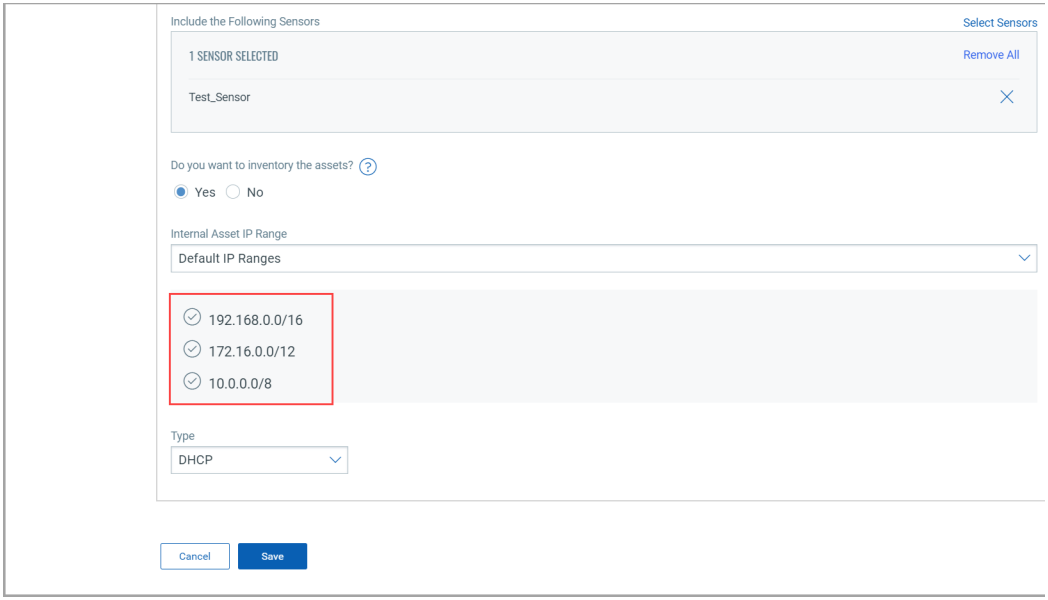
Here, you define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges, IP range tags, or customized IP ranges options to define range of internal assets. NPS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

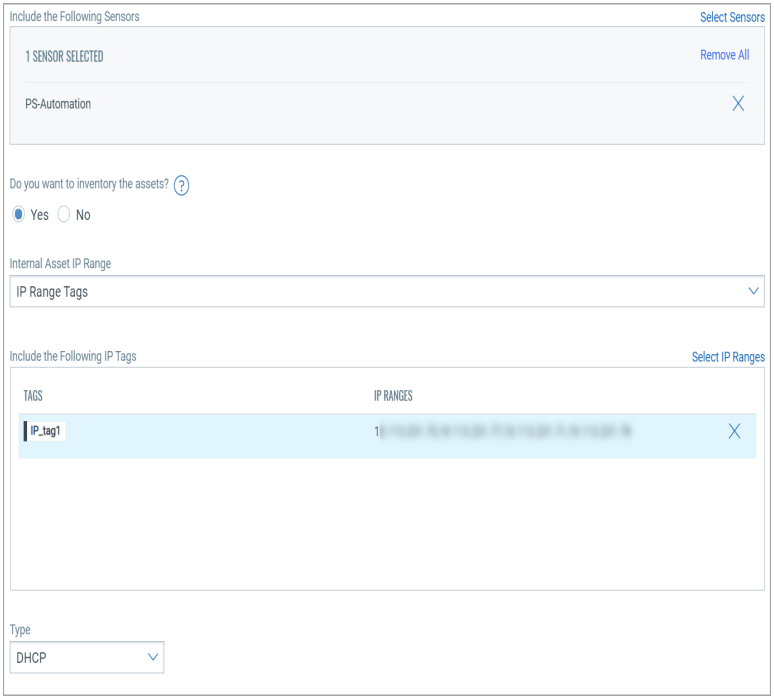
This option defines internal assets discovered within default internal ranges for your network. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.



2 - IP-Range Tags

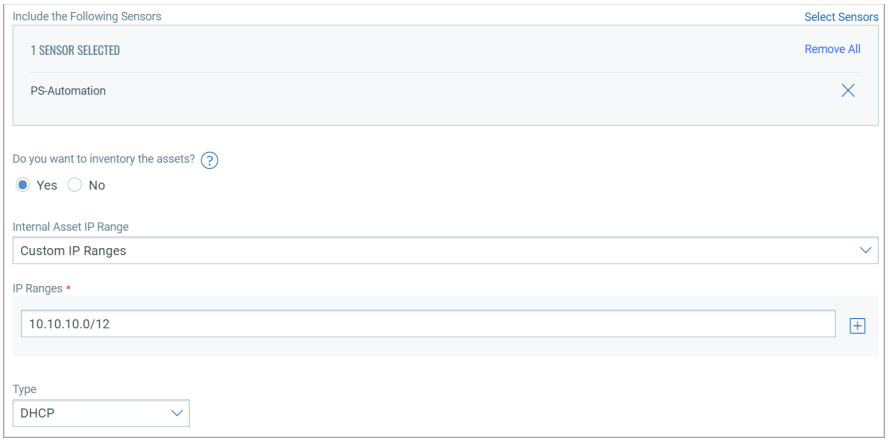
This option defines internal assets discovered with IP range tags. These are the dynamic tags created with 'IP Address In Range(s)' rule engine. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

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



3- Custom IP Ranges

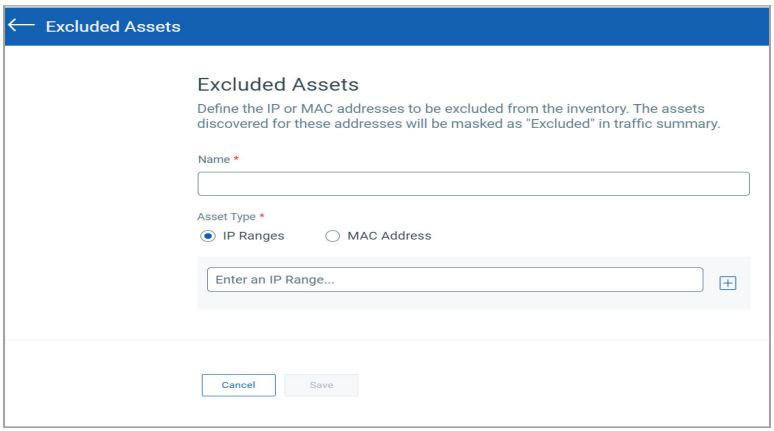
This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.



Excluded Assets

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

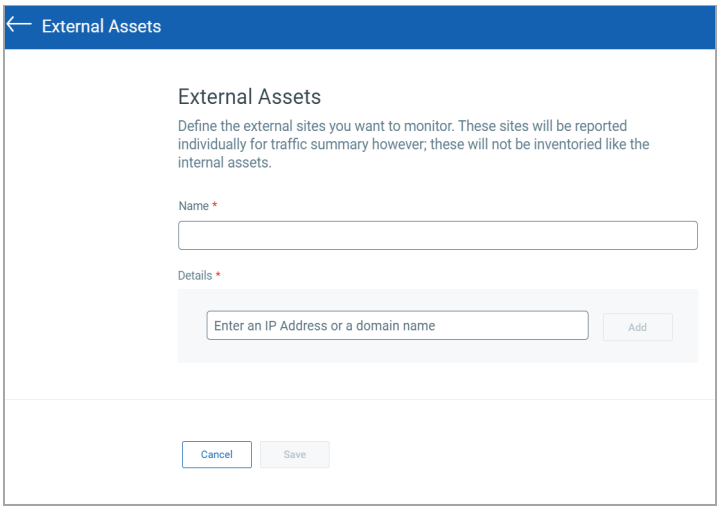
To add excluded assets, simply go to **Configuration** > **Excluded Assets** > **Add**.



Monitor External Assets

Here, you define the external sites you want to monitor. These sites are 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

- 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..

Exclusion

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

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).

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.

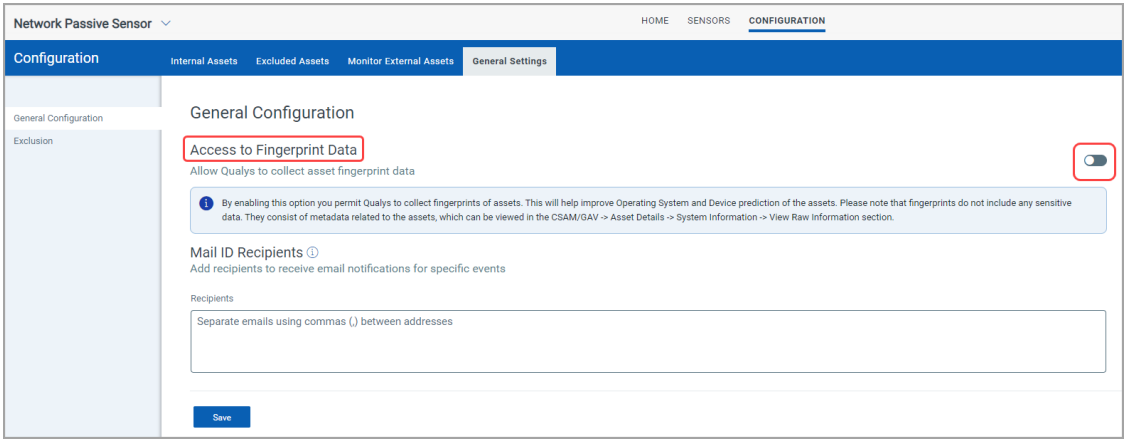
- Navigate to **Configuration** > **General Settings** > **General configuration**.

- To give consent to Qualys to access the metadata, toggle Access to Fingerprint Data to allow access.

Go to the Recipients text box and add the e-mail. You can add multiple e-mails using comma separated.

Click **Save.**

Once you add the recipients, they receive the events in their e-mail inbox.

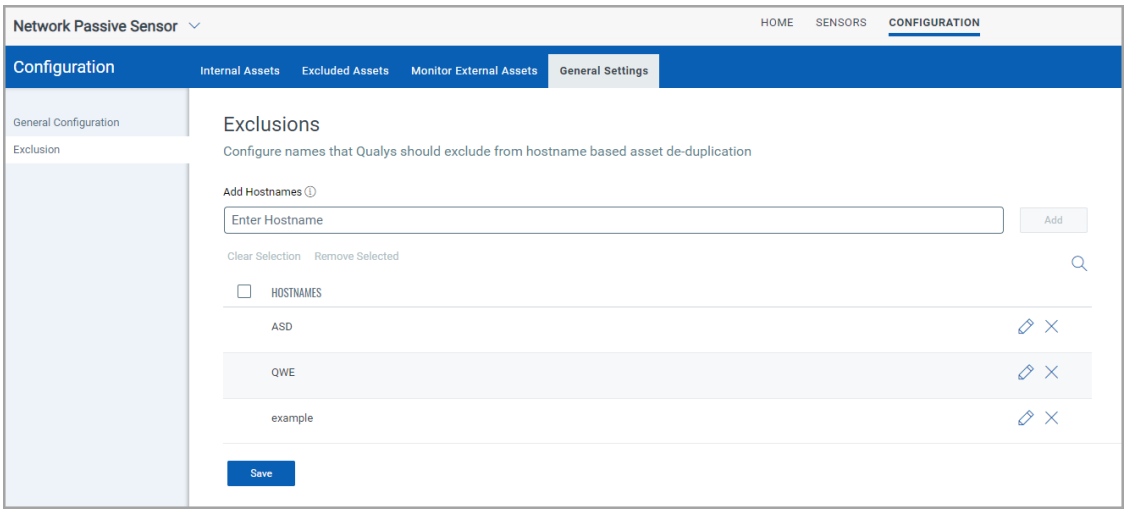


Exclusion

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.



Note: Contact Qualys Customer Support to get them deleted to avoid deduplication in the future.

Network Configurations

You'll need to complete certain network configuration settings under Set up Network. This is where you'll enable and configure the management interface of the appliance.

These configurations are described:

Configure Static IP Address

Proxy Configuration

Configure Static IP Address

If the core group to which Management interface is connected has DHCP server, then you can view the Management Network Configurations with **Show** option. If DHCP is not on your network, you must enable the Virtual Sensor with a static IP address using the **STATIC IP** option. One of these configurations is required.

To enable a static IP address, follow these steps:

1) Go to the **Set up Network** menu option and press **Enter** to continue.

2) Press Space Bar to 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.

Proxy Configuration

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

The Virtual Sensor uses Secure Sockets Layer (SSL) protocol (HTTPS) 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 Virtual Sensor. 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 Virtual Sensor.

To configure Proxy support, follow these steps:

1) Go to the **Set up Network** menu option.

2) Choose **Proxy Configuration** and press **Enter** to continue.

3) Select **Enable Proxy** and click **OK**.

4) 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.

5) 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.

Appendix

Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resources

The Virtual Network Passive Sensor (PS) appliances auto-scaling capability starts automatically at the boot time to calculate how much packet throughput it can handle.

The delta increase in the throughput depends on the additional dedicated resources made available to the appliance. The resources include the CPU clock, the type of CPU, and the type of RAM in the VM appliance system.

To handle continuous traffic, the CPU GHz must be allocated in a dedicated manner. The estimated maximum throughput is visible on the sensor details page. The throughput may vary depending on the dedicated nature of the resources and the type of traffic visible to the sensor.

Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware

The throughput of the VM appliance is directly dependent on the CPU resources allocated to the VM. In addition, it is strongly advised to increase memory as well. Use the following comparison chart as a guideline for resource allocation for the desired throughput.

Comparison Chart

The throughput is dependent on multiple factors, such as

a) The composition of the data fed to sniffing interface: Example number of flows in the traffic, few flows having heavy traffic volume as compared to the rest, the constitution of application data within a flow, etc.

b) Resources allocated to the VM: number of CPU cores, frequency of the CPU core, and the type of memory.

The following is the throughput as measured in the Qualys lab on hardware with the following specifications and with reasonable well-conditioned test data.

Hardware Specifications:

CPU core: Intel(R) Xeon(R) CPU @ 2.30GHz

RAM: RAM DDR4 2133

Virtualization Platform: VMware ESXi 6.7.0

Capacity (MBps)	RAM (GB)	CPU Core
500	8	4
750	12	6
1000	16	8
1250	18	10
1500	20	12
1750	22	14
2000	24	16

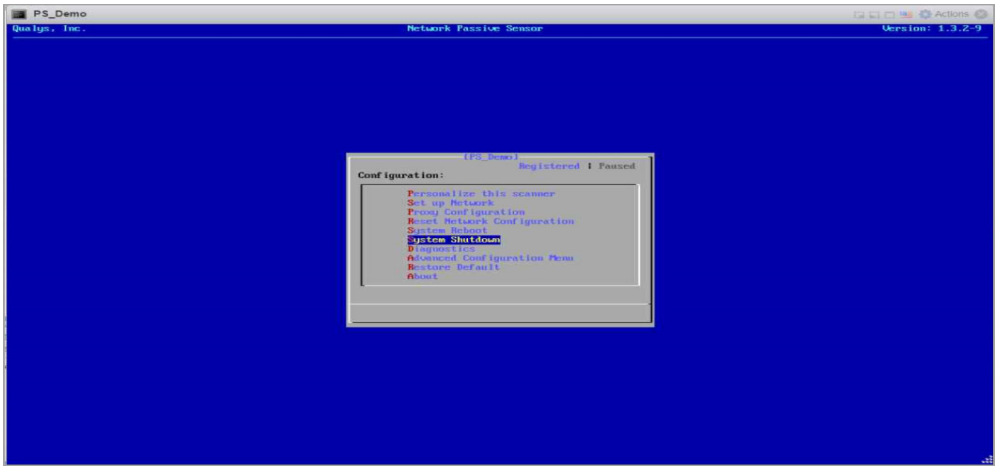
Notes :

- For the desired throughput above 1000Mbps, Qualys strongly advises to add 4 GB RAM (if not possible, a minimum of 2 GB RAM) with every addition of 2 CPU cores to ensure smooth functionality of PS appliances.

- The throughput achieved with a single core by varying the CPU core frequency were as: 150 MBps (CPU core frequency < 1.5 GHz), 200 MBps (1.5 GHz > CPU core frequency > 2 GHz), and 250 Mbps (CPU core frequency > 2 GHz).

How to Modify Hardware Resources for VM Deployed on the ESXi Server

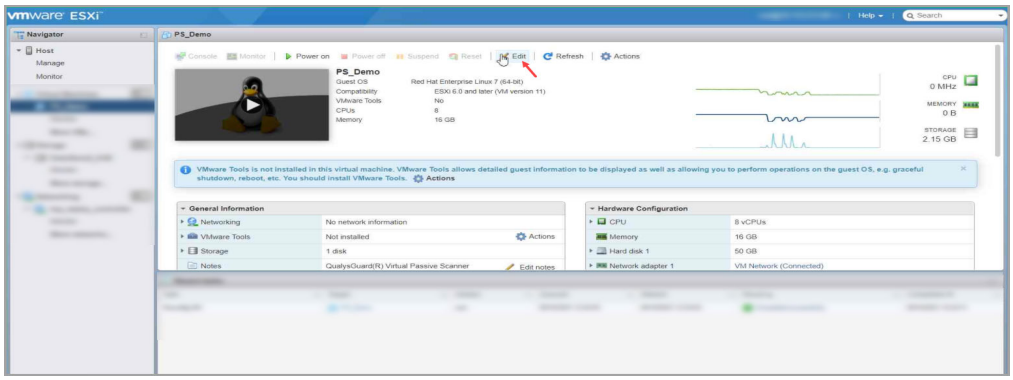
1. Go to **System Shutdown** option and press **Enter** to shutdown the appliance via console.

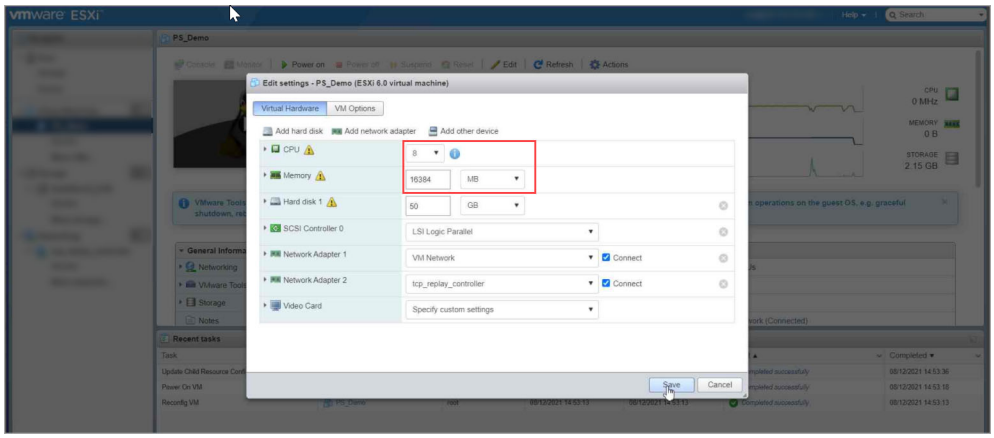


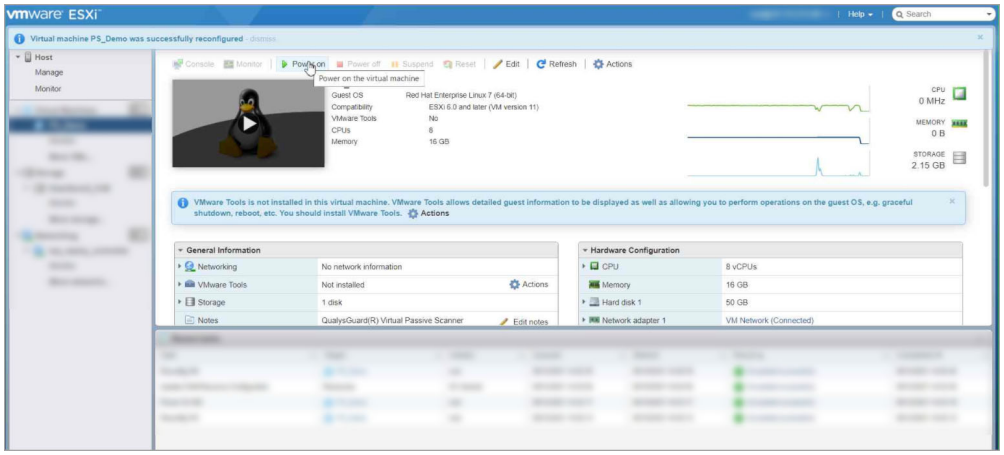
2. Click **Edit**.

3. Increase the **CPU** cores and **Memory** as per your throughput requirements and click **Save** to save your configuration.

4. Click **Power ON** to start your appliance.



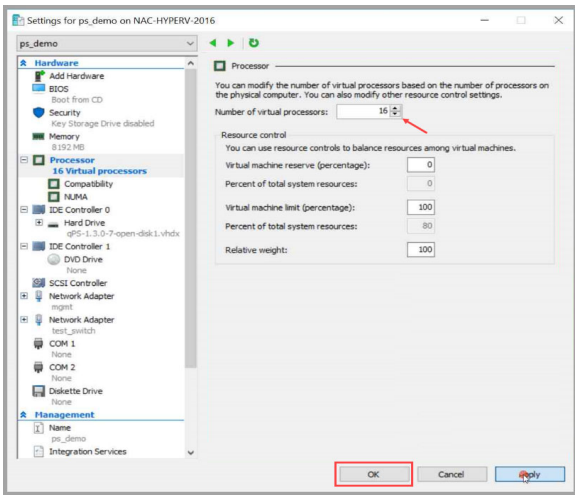


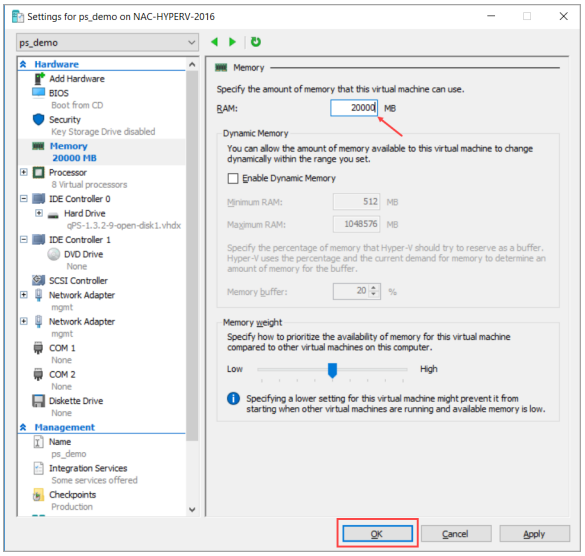


How to Modify Hardware Resources for VM Deployed on the HyperV Server

1. Follow Step 1 same as mentioned above.

2. Select the virtual machine and go to **Settings**. Modify the **CPU** cores and **Memory** as per your throughput requirements > Click **Apply** to apply the changes > Click **OK** to save your configuration.





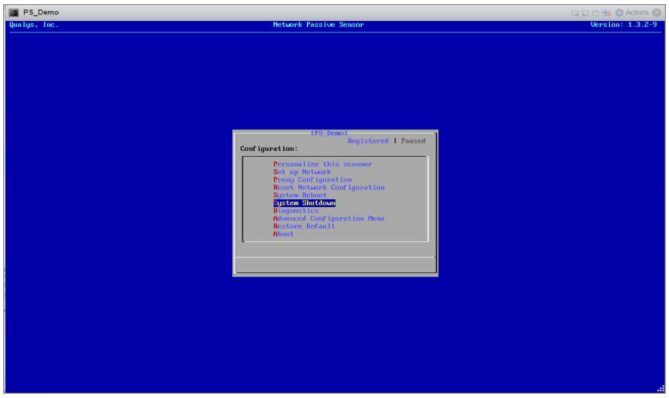
3. **Power ON** the VM.

Adding/Removing Sniffing Interfaces from Virtual Appliance

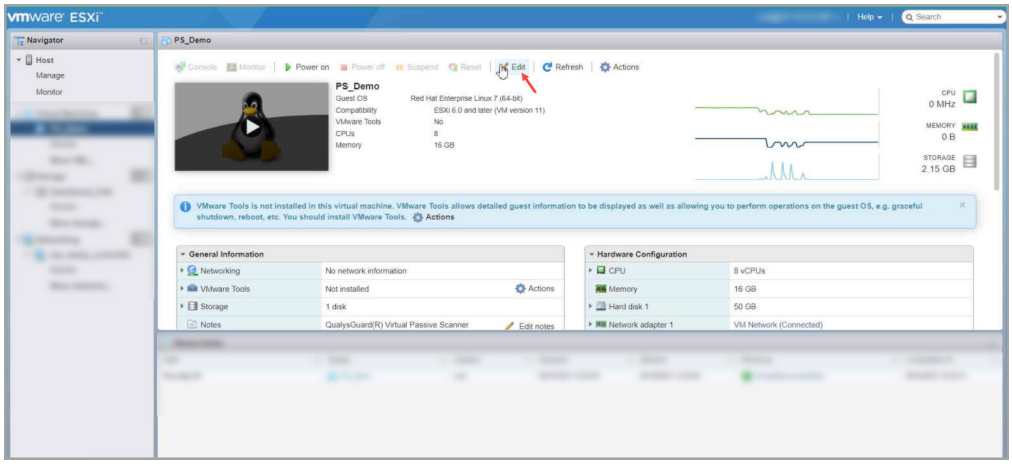
Network Passive Sensor (PS) now supports an aggregated/bonded sniffing interface. A virtual interface aggregates multiple physical interfaces allow the appliance to add one or more sniffing interfaces.

How to Add Sniffing Interface to the PS Appliance Deployed on the ESXi Server

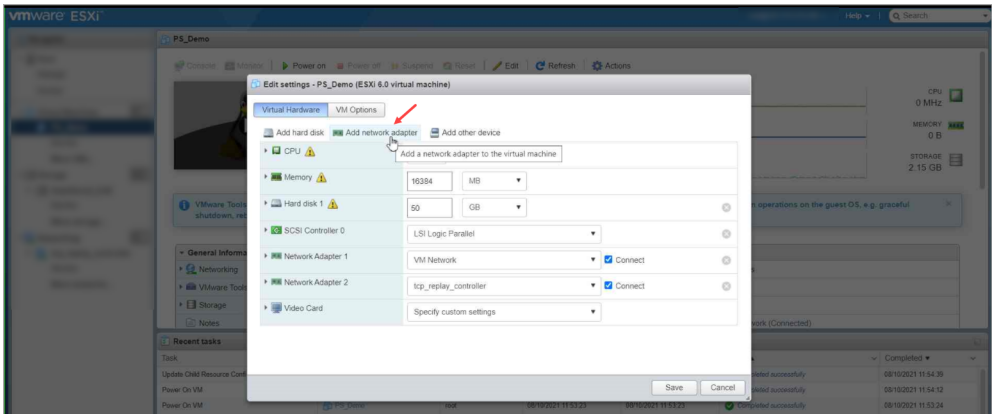
1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.



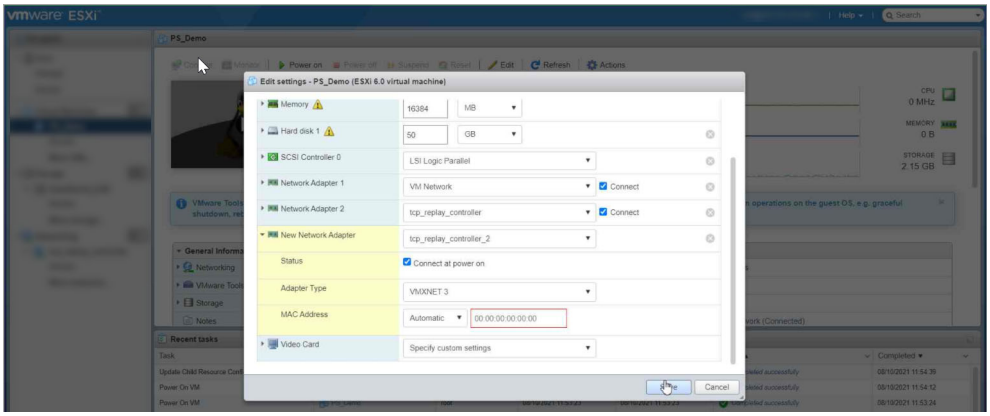
2. Click **Edit**



3. Click **Add Network Adapter** for adding new sniffing interface.



4. Select appropriate port group > Select the adapter type **VMXNET 3** > Click **Save** to save your configuration.

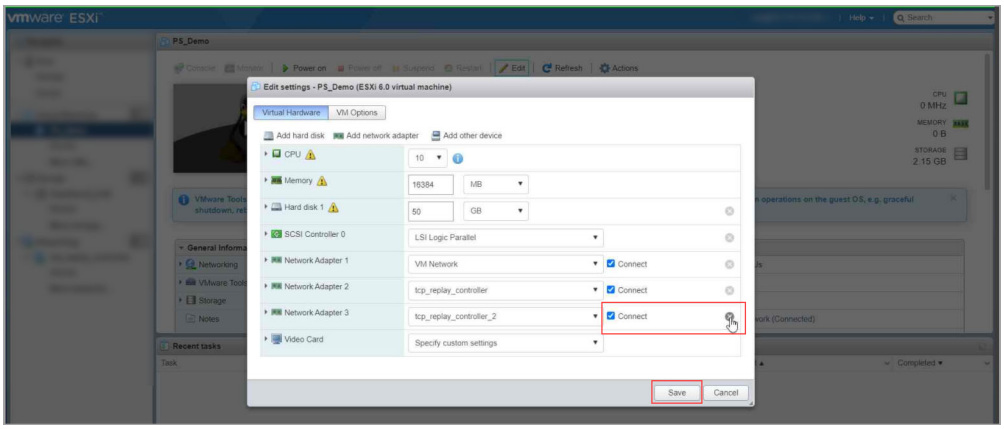


5. **Power on** the VM.

How to Remove Sniffing Interface to the PS Appliance Deployed on the ESXi Server

1. Follow the Step 1 and Step 2 same as mentioned above.

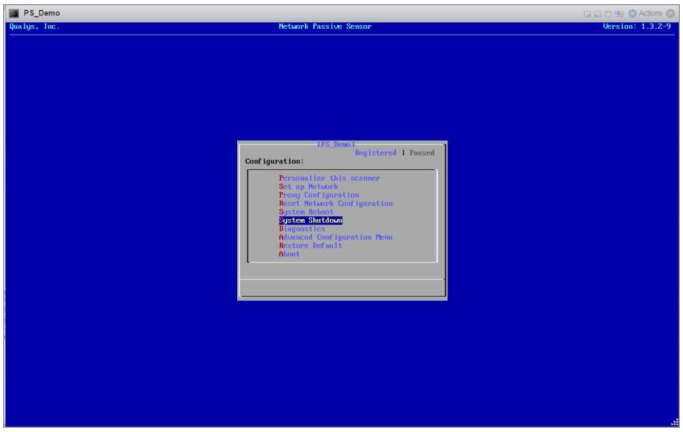
2. Remove the newly added interface and click **Save** to save the configuration.



3. **Power on** the VM.

How to add Sniffing Interface to the PS Appliance Deployed on the HyperV Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.

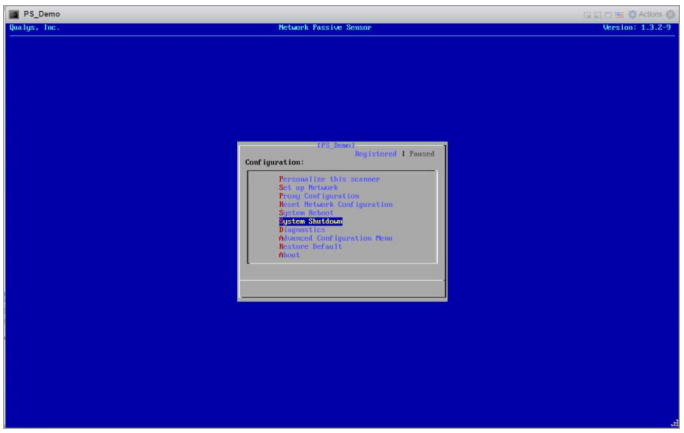


Note: A virtual switch that views the mirrored network traffic should be connected to the newly created interface.

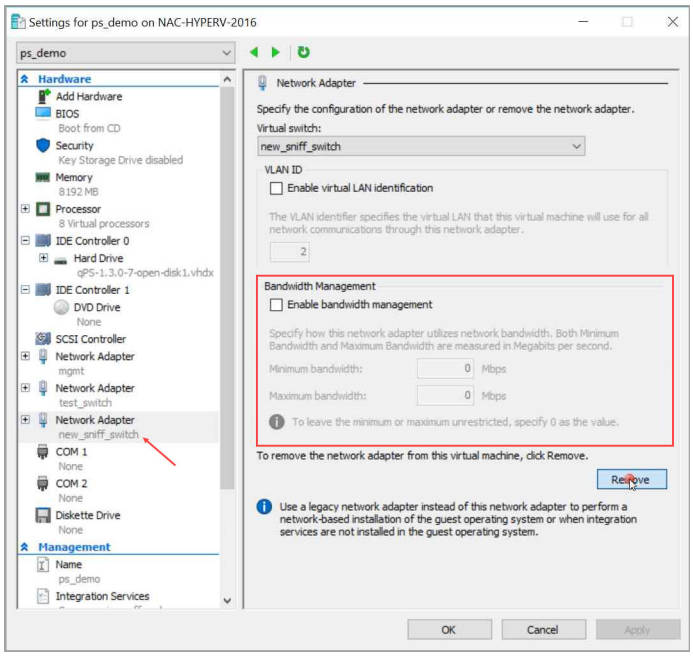
Click here to follow steps 10 to 20 in the Deployment on Microsoft Hyper-V section to create a virtual switch and add a new sniffing interface to it.

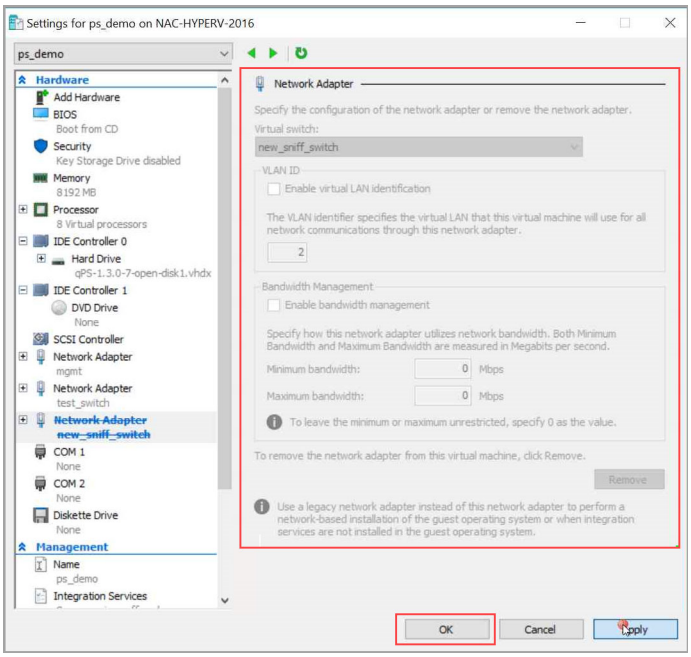
How to Remove Sniffing Interface to the PS Appliance Deployed on the HyperV Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.



2. Select the virtual machine and go to **Settings** > Select the Network Adapter tab that needs to be removed > Click **Remove** > Click **Apply** > Click **OK** to remove the network adapter.





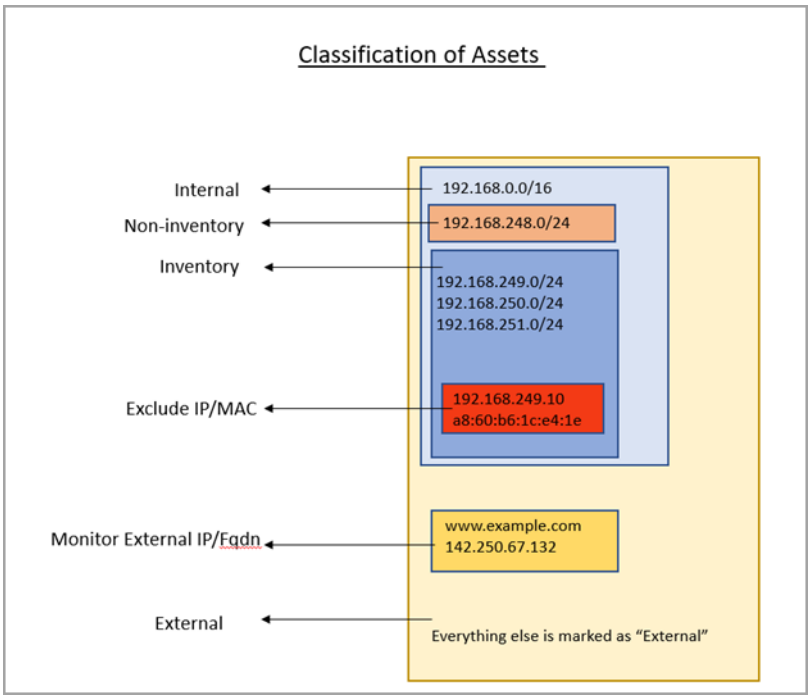
Classification of Assets in Passive Sensor

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.

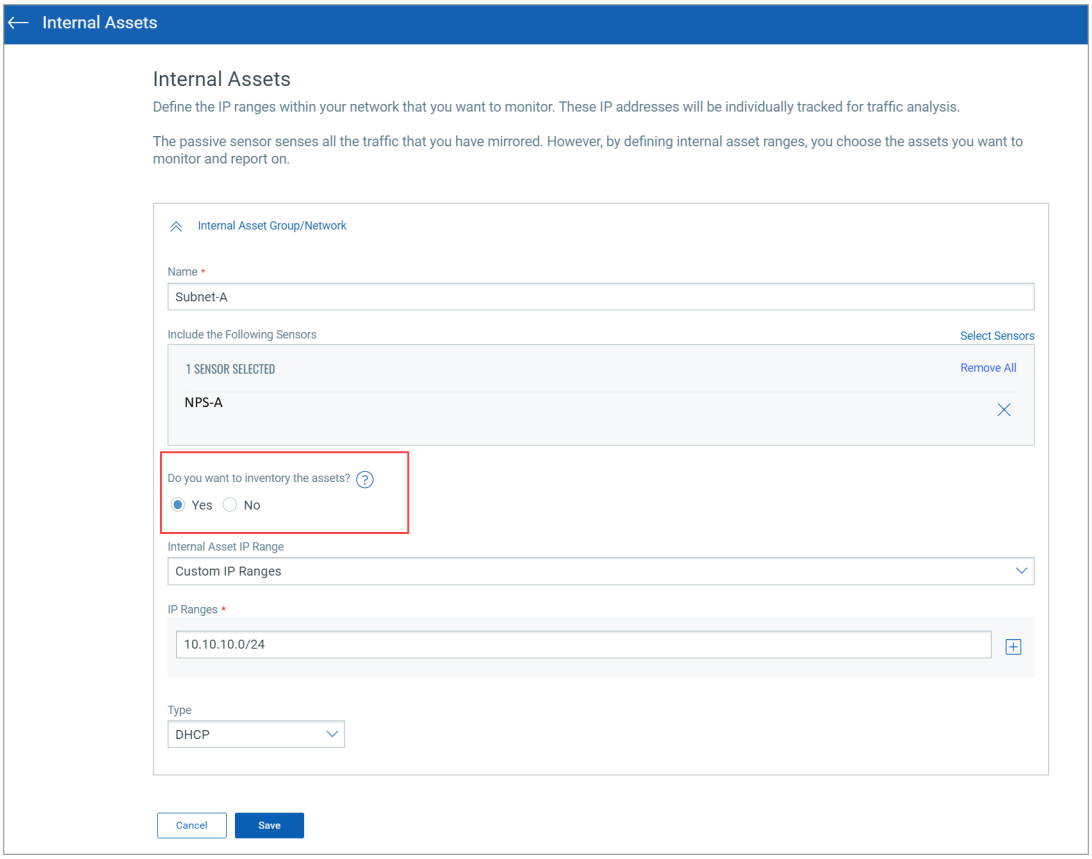
PS aggregates the traffic flows from an IP in the internal range to another IP in the internal range by 4-tuple of Source IP, Destination IP, Destination port, and TCP or UCP protocol. Appliance reports traffic flows at an interval of 5 minutes for new assets and at 30 minutes for asset updates.

The appliance aggregates multiple flows of the same tuple into one flow when reporting it in the 5 or 30-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.

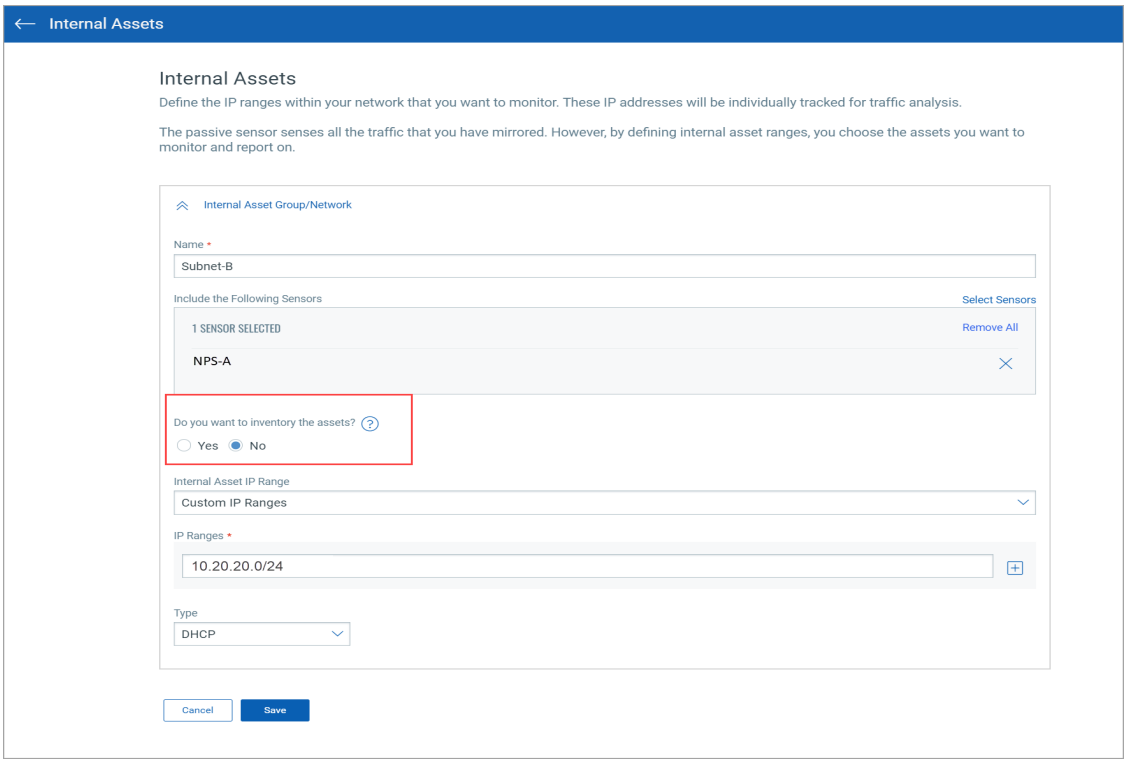


What is Non-Inventory

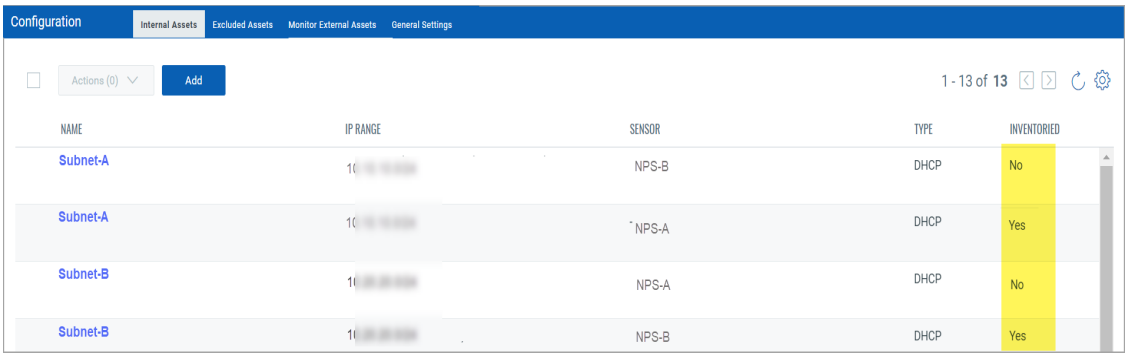
PS uses IP addresses in this range only for tracking traffic flows to other IPs in the inventory range and NOT for inventory purpose. Assets in this IP range do not show in the CSAM inventory. However, traffic flows to/from these assets are listed in the Network tab of CSAM and under the inventoried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



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



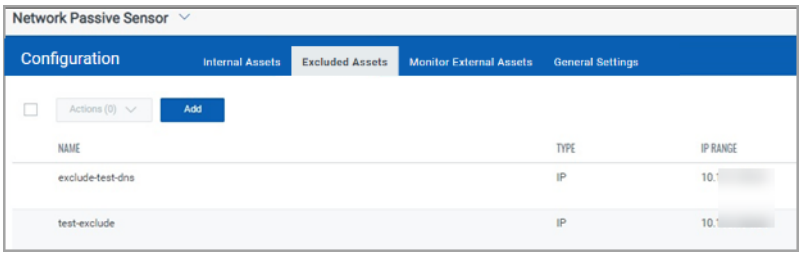
What is Excluded

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.

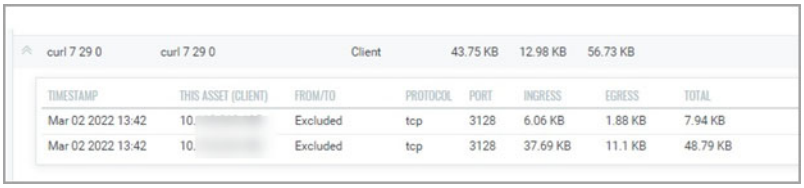
PS excludes gathering all inventory information of the IPs/MACs added in this category/group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in the traffic listing, the asset is seen as Excluded without any IP-address.

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.



Traffic summary representation for Excluded Assets:

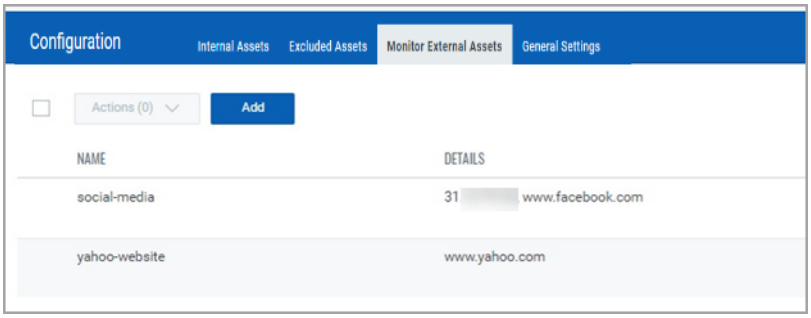


What is Monitored External

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. If Monitor External FQDNs or IPs are configured, then traffic flows of Monitor External assets will be tracked with the actual IP address. i.e., Traffic flows between inventoried assets & Monitor External assets will be shown with the actual IP address of Monitor External IP's/FQDNs assets in the traffic listing of inventoried assets.

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.



Traffic summary representation of Monitor External Assets & External Assets:

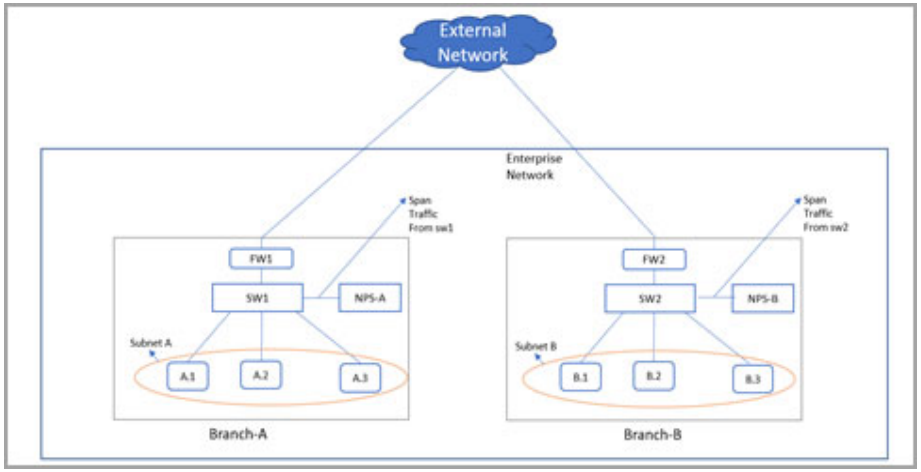
Best Practices

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:

Passive Sensor Appliance Location	Internal (inventoried)	Internal (non-inventoried)
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.