Network Passive Sensor

Virtual Appliance User Guide

January 16, 2020

Copyright 2020 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

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.

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.

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 Get Started with Sensors screen, click Download Image link under Virtual Sensor to download the image (OVA file) to your local system. 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. (Similarly, you can go to the registration step directly from Home > Deploy Network Sensor > Virtual Sensor > Deploy).
3. In 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 here.
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.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" on page 8.

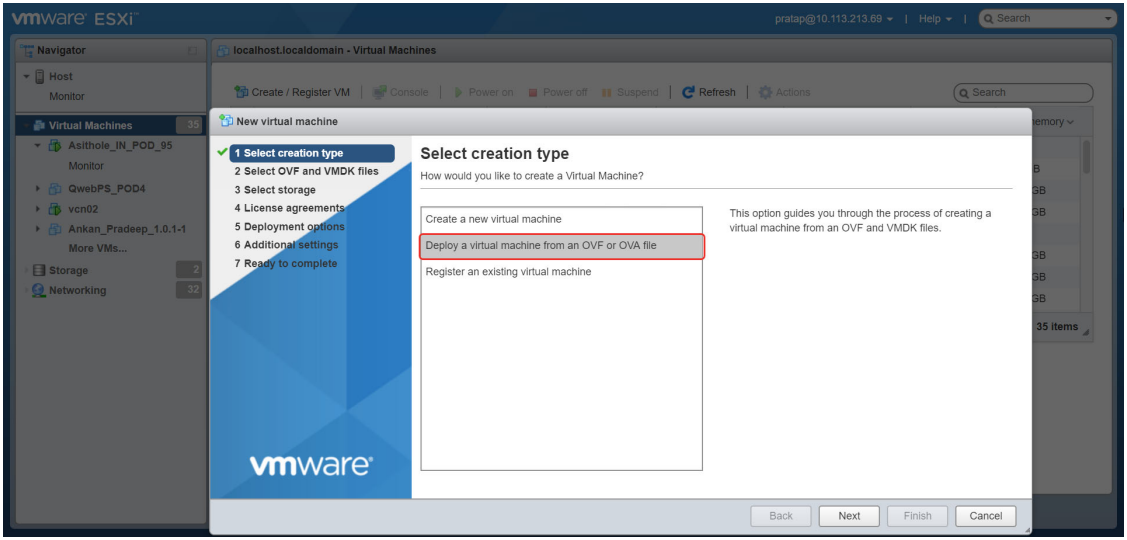
Step 3 - Deploy Virtualization Image

You'll deploy the image on VMware ESXi. VMware ESXi 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.

ESXi server requirements: 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.

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.

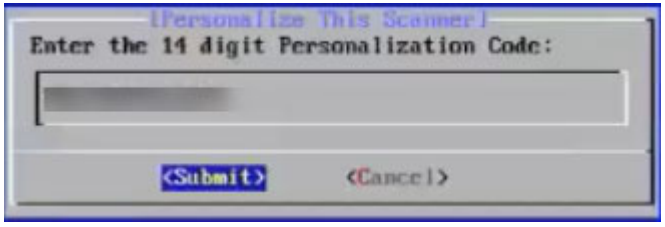
8 There are some network configuration settings (static IP, proxy) you'll need to set before proceeding to the next step. Complete Network Configurations.

Step 4 - Register the Virtual Appliance

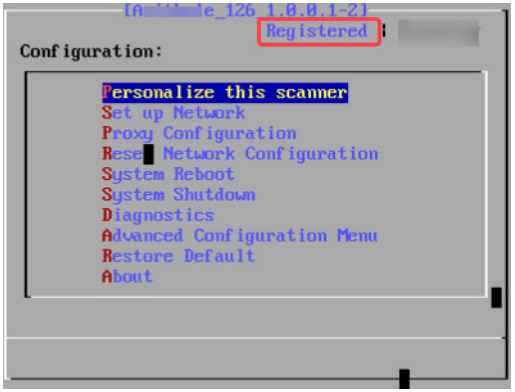
1 Open the Virtual Appliance console by selecting the VM and then navigating to Console > Open browser console.

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

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



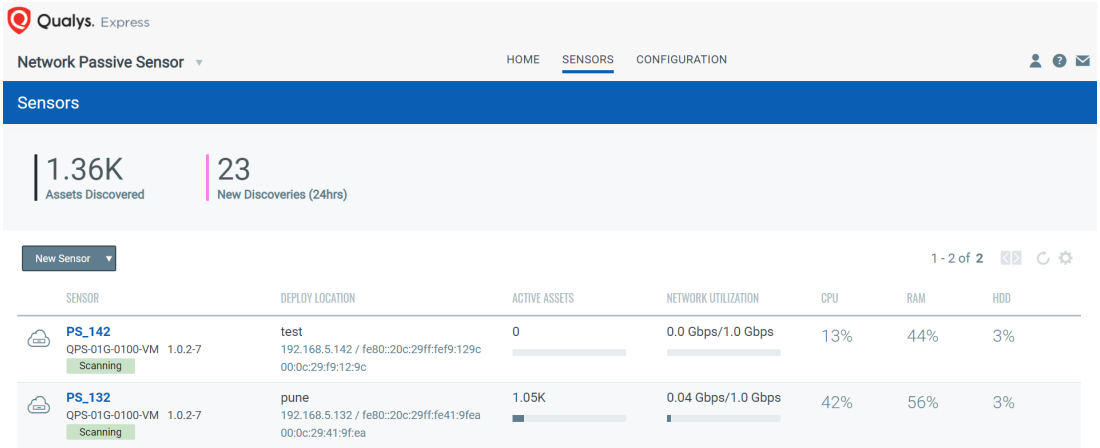
4 Click **Submit** and wait for the confirmation message **Appliance registration completed successfully**. Check that the status on the console is Registered.



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, Scanning or Not Connected.

If the status is Paused, you can view details for the appliance, reboot the appliance, start scanning, delete assets and deregister.

If the status is Scanning, you can view details and pause scanning.

If the status is Not Connected, you can view details for the appliance.

Configure Assets

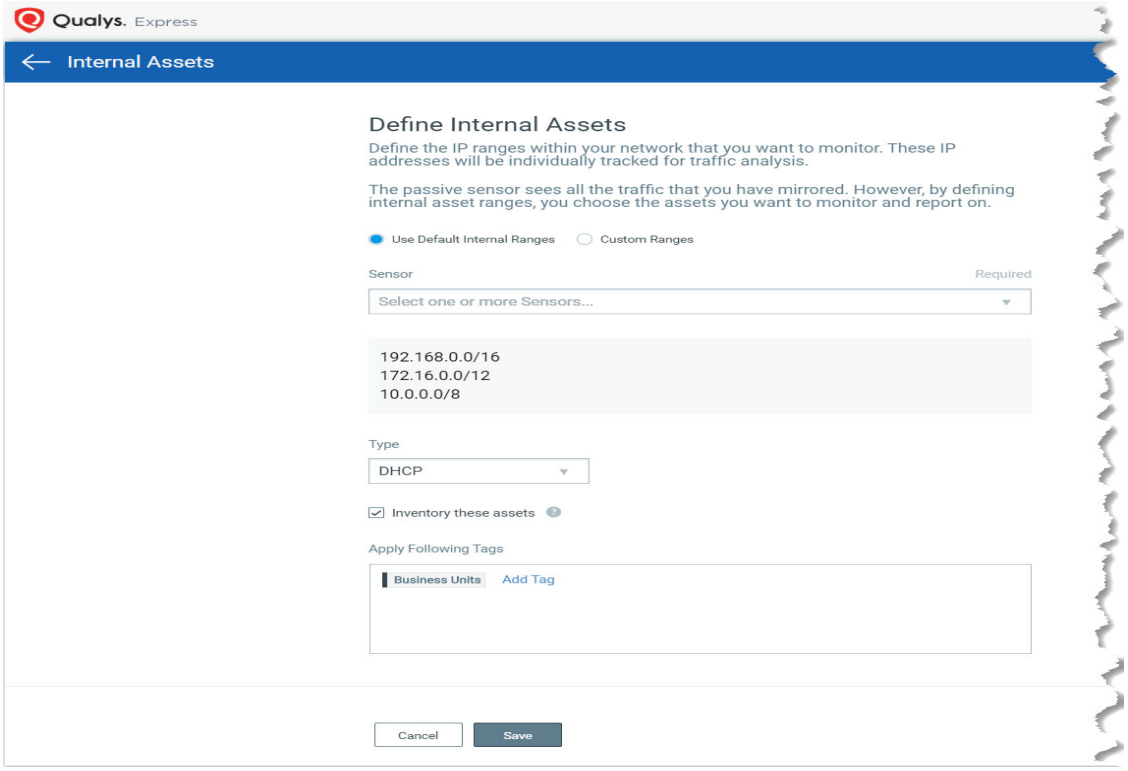
Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

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 > Add.

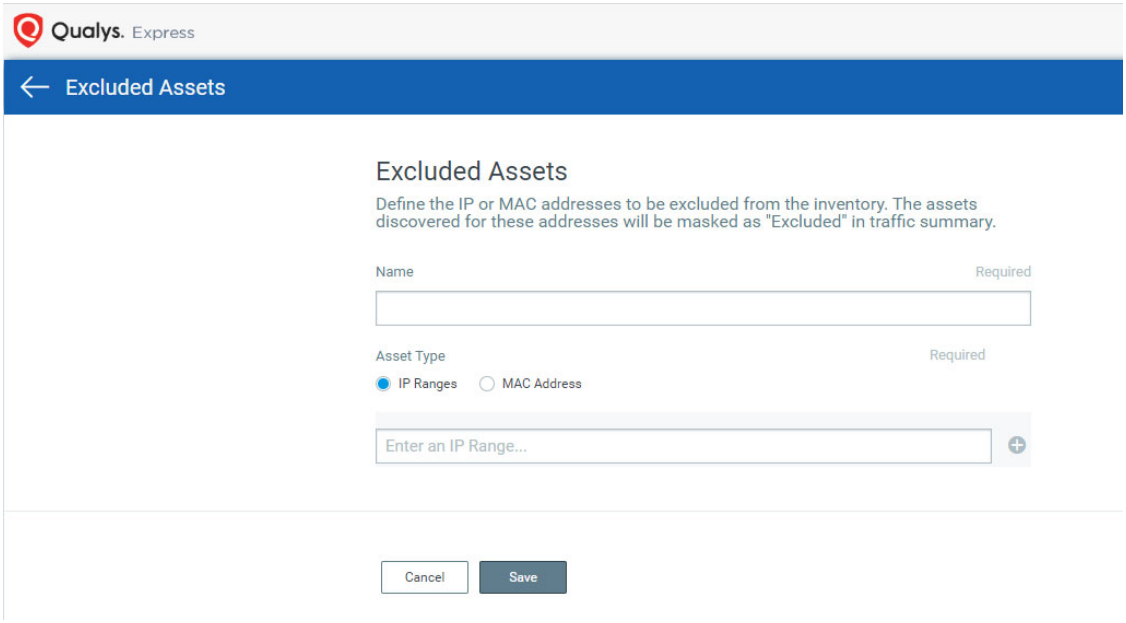


Here, you'll define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges or use customized IP ranges. Select Inventory these assets check box for marking inventoried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

To 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.

Excluded Assets

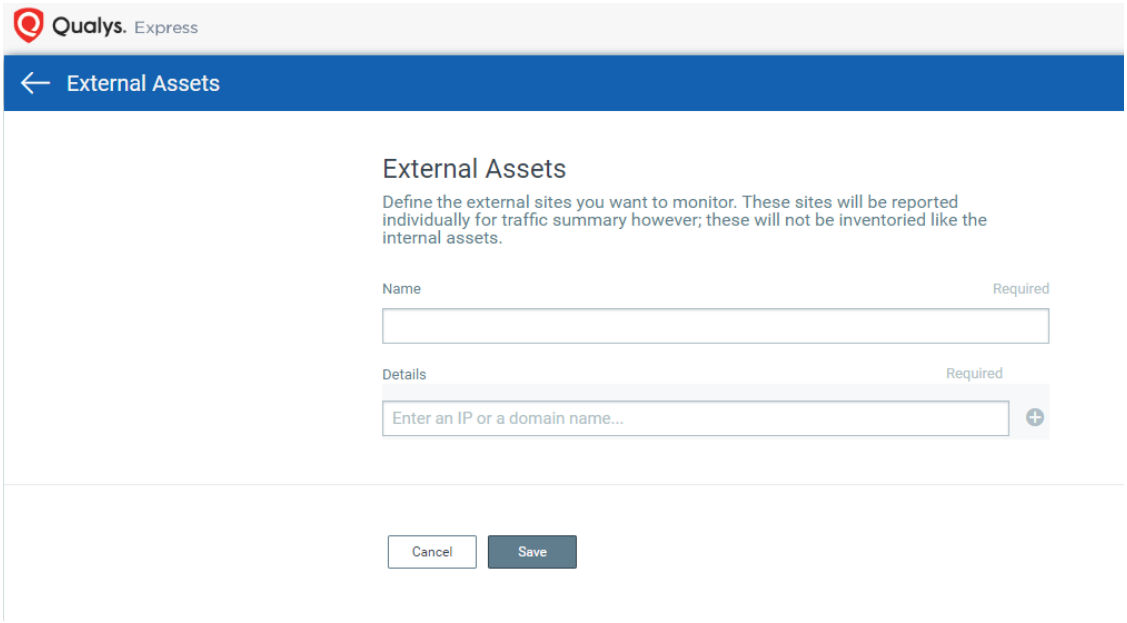
To add excluded assets, simply go to Configuration > Excluded Assets > Add.



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.

External Assets

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



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.

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

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. 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.