



Offline Scanner Appliance

User Guide

June 12, 2018

Copyright 2014-2018 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



Contents

| | |
|--|-----------|
| About this guide..... | 4 |
| About Qualys | 4 |
| Qualys Support | 4 |
| Get Started | 5 |
| Some things to consider... .. | 5 |
| Overview | 5 |
| About managing instances | 6 |
| It's easy to add an Offline Scanner | 6 |
| Start the Wizard | 6 |
| Configure your Offline Scanner | 8 |
| We recommend a few things | 9 |
| Log in to the Web User Interface | 10 |
| Start Offline Scanning..... | 11 |
| All about the modes | 12 |
| Ready for your first scan? | 14 |
| Download scan results..... | 20 |
| Upload scan results..... | 21 |
| Discover live devices on your network..... | 22 |
| VMware Configuration..... | 23 |

About this guide

Thank you for your interest in Qualys Offline Scanner Appliance. This lets you scan for vulnerabilities in secure air gap networks that do not have Internet access. We'll help you get started quickly.

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

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/

Get Started

Qualys Offline Scanner Appliance lets you scan for vulnerabilities in secure air gap networks that do not have Internet access. This is distributed as a virtual appliance for VMware Workstation.

Some things to consider...

- 1) You'll need VMware Workstation. We support v9.0 on Windows.
- 2) Check network access to scanners to ensure you can connect to the Qualys Cloud Platform (this is required for activation to be successful). [Learn more](#)
- 3) Your offline virtual scanner appliance has 2 modes: CLOUD SYNC and OFFLINE SCANNING. You'll be in CLOUD SYNC mode to start. You'll switch to OFFLINE SCANNING mode when you're ready to scan. Be sure to review your network settings in VMware **before** you switch modes. Bridged mode is required for scanning. [Learn more](#)

Overview

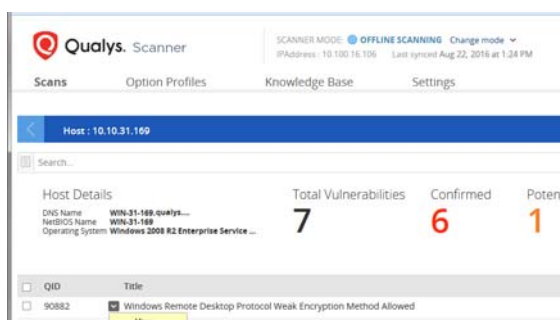
First use the Console Interface for the initial Personalization workflow.



This workflow will complete the registration of the appliance within your account. Later you'll use this interface for low-level administration (i.e. reboot, shutdown).

How does it work? This is equivalent to plugging a keyboard/mouse/monitor into a hardware appliance and can't be directly reached over a network. It is only viewable through console access provided by the virtualization software.

Then use the Web User Interface for scanning.



This is where you launch scans and manage your account data (option profiles, scan results). The web user interface can be accessed using any standard web browser (e.g. Internet Explorer, Chrome, Firefox) running on the host OS. The virtual NIC for the web interface should be deployed on a host-only network between the host (e.g. Windows) and the appliance virtual machine.

About managing instances

Instance Snapshots/Cloning Not Allowed

Using a snapshot or clone of a scanner instance to create a new instance is strictly prohibited. The new instance will not function as a scanner. All configuration settings and platform registration information will be lost. This could also lead to scans failing and errors for the original scanner.

Moving/Exporting Instance Not Allowed

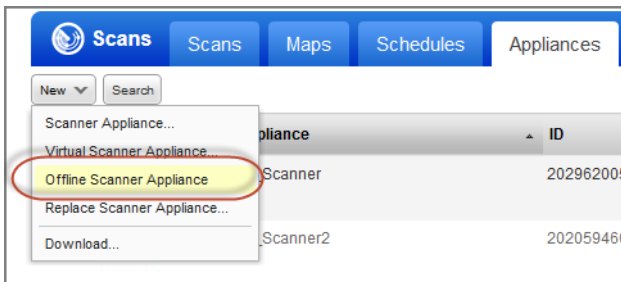
Moving or exporting a registered scanner instance from a virtualization platform (HyperV, VMware, XenServer) in any file format to a cloud platform (AWS, Azure, GCE, OpenStack) is strictly prohibited. This will break scanner functionality and the scanner will permanently lose all of its settings.

It's easy to add an Offline Scanner

You can add an offline scanner to your account in just a couple of minutes. Then you'll be ready to scan devices in your secure air gap network. Let's do it!

Start the Wizard

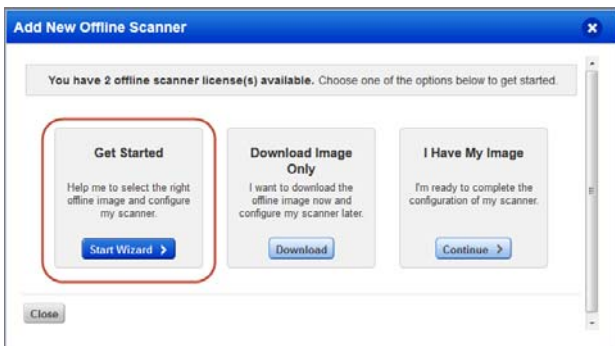
Go to Scans > Appliances and select New > Offline Scanner Appliance



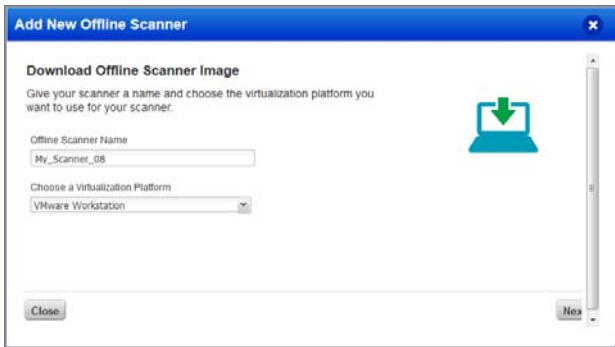
Don't see this option?

That means the Offline Scanner feature is not enabled. Please contact Qualys Support or your Technical Account Manager

Click **Start Wizard** and we'll walk you through the steps.

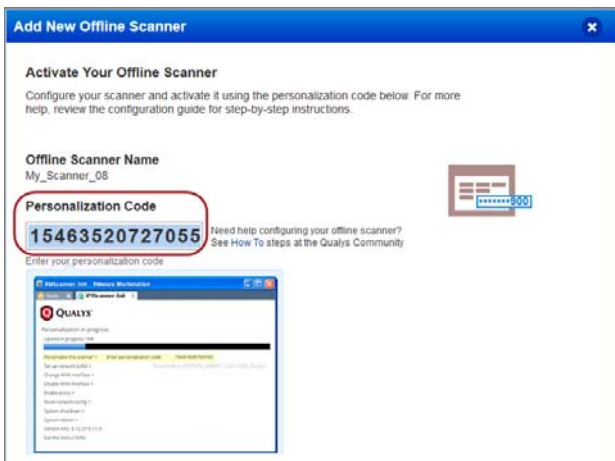


Download the image Give your scanner a name and choose VMware Workstation.



We support VMware Workstation v9.0 on Windows. The image should be expected to work on other virtualization platforms but we can only assist in troubleshooting on this supported platform.

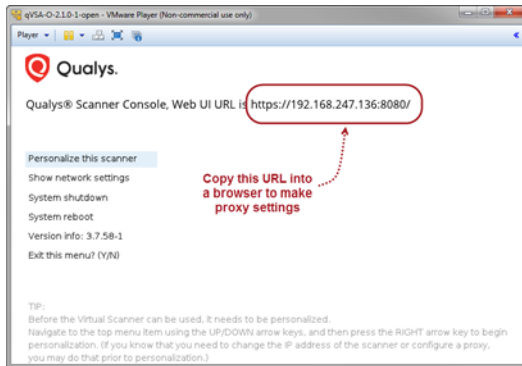
Get your personalization code You'll want to copy the code to a safe place (you'll need it later). Once you have your code you can close the wizard.



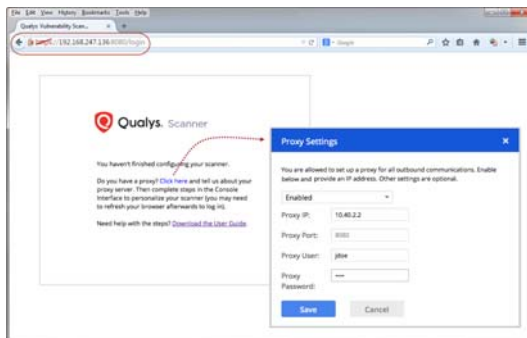
Configure your Offline Scanner

Start your virtualization platform Locate the offline scanner image file (starts with qVSA-O) on your local system, open the image and power on the virtual machine.

Do you have a proxy? You'll need to tell us about your proxy server.



Copy the Web UI URL and paste it into a new browser window.



Click the text link on the screen to configure proxy settings.

Enter the IP address (required) and port number (8080 is implied but can be changed). If the proxy server requires authentication enter the proxy user name and password.

After saving your settings, return to the Scanner Console to personalize your scanner.

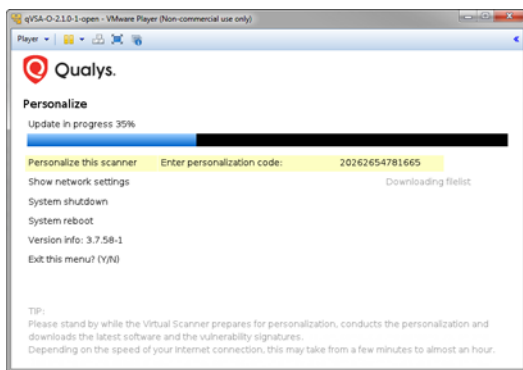
Personalize the scanner Follow these steps in the Scanner Console.



Press the Right arrow to select “Personalize this scanner” and then type in your personalization code.

Don't have your personalization code? Log in to Qualys and get it from the Scans > Appliances list.

Now your scanner will connect to the Qualys Cloud Platform to complete the activation and download the latest software.

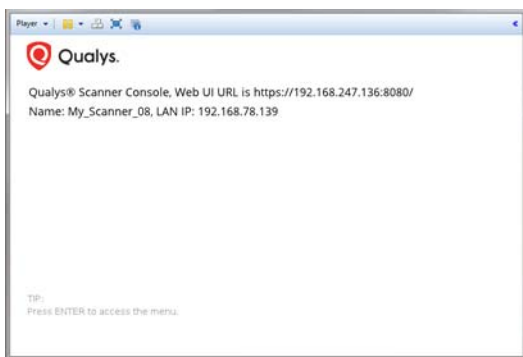


You'll see the activation progress.

Having trouble activating your scanner?

1 - Check settings in VMware. [Learn more](#)

2 - Check network access to scanners. Log in to Qualys and go to Help > About to see a list of URLs (at the SOC) that your scanner must be able to contact on port 443. [Learn more](#)

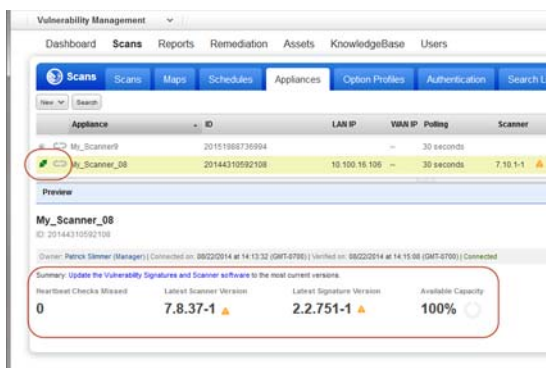



Upon success you'll see this scanner's name and IP address. That's it! You've added your offline scanner to your account.

Note the Web UI URL. You'll need this in a couple minutes to log in to the Scanner's Web UI.

We recommend a few things

Check the scanner appliance status Go to Scans > Appliances, and select your scanner to see details in the preview pane.



Is your scanner ready?  tells you the scanner is connected to our Cloud Platform and you're ready to start scanning.

It can take a few minutes for the Qualys user interface to get updated after you add a new appliance. Please refresh your browser periodically to see the latest details.

Tell us the option profiles you want to use Go to Scans > Option Profiles, edit the profile(s) you want to use for offline scanning and select the option “Make this option profile available to all offline scanners”.

New Option Profile

Option Profile Title > **Option Profile Title**

Scan > Title: * Offline Scanning

Map > Owner: Patrick Slinner (Manager: quays_ttt) >

Additional >

☐ Set this as the default option profile when launching maps and sca

☐ Make this a globally available option profile

☒ Make this option profile available to all offline scanners

Doing this now will save you time later. These profiles will be ready to use for your first scans.

Log in to the Web User Interface

Open a new browser window and enter the Web UI URL. Then use your personalization code for the initial password – you’ll be prompted to change it right away.

File Edit View History Bookmarks Tools Help

Qualys Vulnerability Scan...

Enter the Web UI URL from the Scanner Console

https://192.168.247.136:8080/login

Qualys. Scanner

Scanner name My_Scanner_08

Password

Enter your personalization code

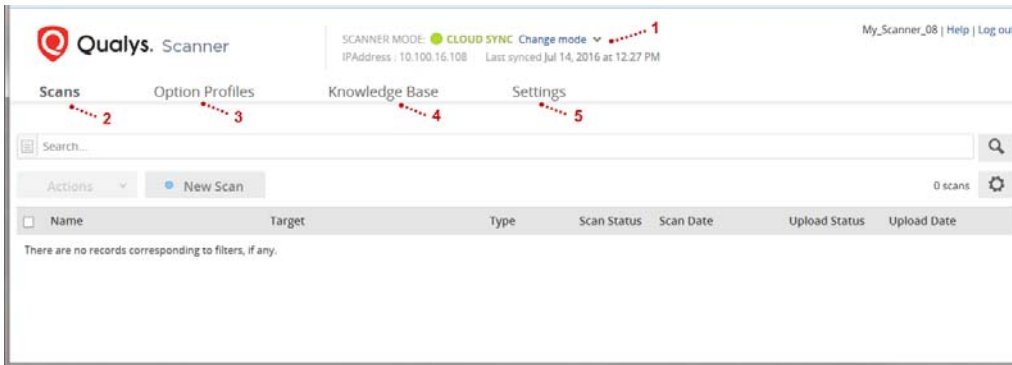
Sign in

Congrats, you’re now logged in and ready for offline scanning!

Start Offline Scanning

We'll help you launch a vulnerability scan on your secure air gap network using the offline virtual scanner that you set up on your laptop.

A quick look at the Web UI



- 1 At the top of the screen you'll see important details about your virtual scanner like its assigned IP address on the current network, the mode it's in – CLOUD SYNC or OFFLINE SCANNING – and when it last connected (synced) to the Qualys Cloud Platform.
- 2 Start new scans, view and download scan results, mark scans to be uploaded.
- 3 Check out the option profiles available for offline scanning.
- 4 Search and view the vulnerability checks (QIDs) that your offline scanner can perform.
- 5 Set up a static IP configuration for offline scanning and a proxy for cloud syncing.

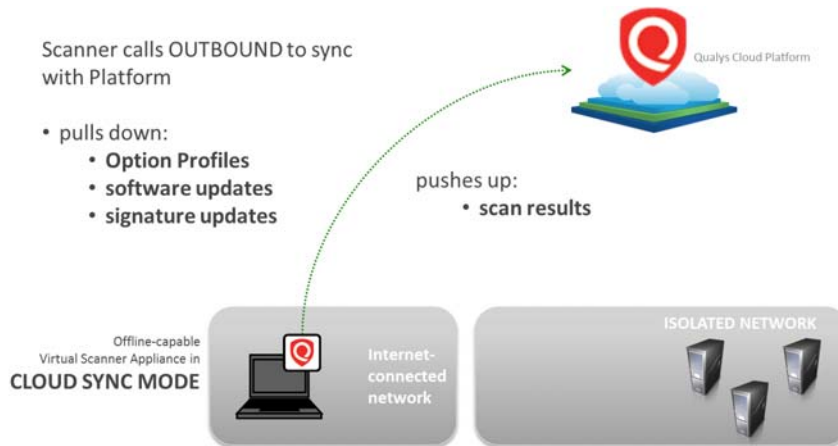
CLOUD SYNC vs. OFFLINE SCANNING

The first time you log in your virtual scanner (and every time your appliance comes online from a hard boot) it will be in CLOUD SYNC mode, and your virtual scanner can connect to our Cloud Platform. This is used to download option profiles, get the latest vulnerability checks and upload scan results to your Qualys account. You'll switch to OFFLINE SCANNING mode when you're ready to start a scan. In this mode your virtual scanner is connected to the secure network you want to scan, and it will not attempt to call home to the Qualys Cloud Platform via the Internet.

All about the modes

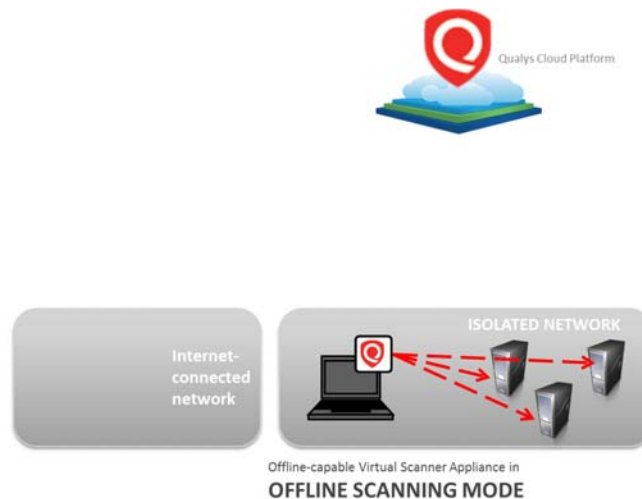
CLOUD SYNC Mode

Your offline scanner connects to the Qualys Cloud Platform to pull down option profiles, software updates and signature updates, and push up scan results.



OFFLINE SCANNING Mode

Your offline scanner connects to the secure network you want to scan, and it will not attempt to call home to the Qualys Cloud Platform via the Internet.



Switching between modes

Each time you switch modes (from CLOUD SYNC to OFFLINE SCANNING and vice versa) we will suspend your virtual scanner and then you'll manually resume it using VMware. Before making a switch, you must edit the network settings in VMware to prepare it for the new mode. That way your scanner has the correct settings when it is resumed. [Learn more](#)

Static IP configuration

When you're in OFFLINE SCANNING mode, we'll use DHCP by default to get an IP address for your scanner. You can, however, set up a static IP configuration if you prefer. It's easy to do. Choose "Manual" under Network Settings. Enter the IP address, netmask, default gateway and DNS servers. Each time you're in OFFLINE SCANNING mode, we'll use the static IP configuration. (Note - We always use DHCP in CLOUD SYNC mode.)

The screenshot shows the Qualys Scanner web interface. At the top, the 'Settings' tab is selected. The 'Settings - Offline Scanning' section is active, showing 'Network Settings' with a dropdown menu set to 'Manual'. Below this, there are input fields for IP Address (10.100.11.128), Netmask (255.255.255.0), Gateway (10.100.11.1), DNS1 (10.0.0.1), and DNS2 (10.0.0.2). A red box highlights the 'Manual' dropdown and the input fields. The 'Settings - Cloud Sync' section is also visible, showing 'Proxy Settings' with a dropdown menu set to 'Enabled'.

When should I make these settings? You can do this any time, in either mode. If you're in OFFLINE SCANNING mode, we'll make the change from DHCP to Static immediately and perform a network refresh. If you're in CLOUD SYNC mode, we'll save your settings and apply them the next time you switch to OFFLINE SCANNING mode.

Network Proxy configuration

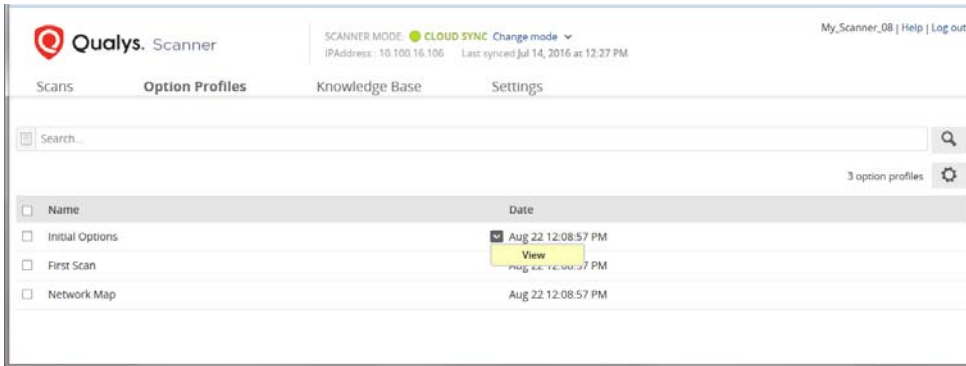
You have the option to set up a proxy for outbound communications when in CLOUD SYNC mode. Choose "Enable" under Proxy Settings and tell us about your proxy server. Enter the IP address (required) and port number (8080 is implied but you can change this). If the proxy server requires authentication then you'll also need to enter the proxy user name and password.

The screenshot shows the Qualys Scanner web interface. At the top, the 'Settings' tab is selected. The 'Settings - Cloud Sync' section is active, showing 'Proxy Settings' with a dropdown menu set to 'Enabled'. Below this, there are input fields for Proxy IP (10.200.42.212), Proxy Port (8080), Proxy User (jake), and Proxy Password. A red box highlights the 'Enabled' dropdown and the input fields. The 'Settings - Offline Scanning' section is also visible, showing 'Network Settings' with a dropdown menu set to 'Manual'.

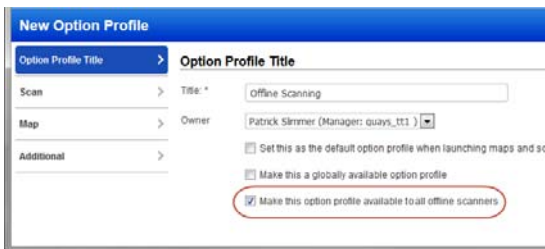
Ready for your first scan?

Review option profiles

The first thing you want to do is make sure you have option profiles in place. Click Option Profiles to see the option profiles that have been synced down to your account. Then select View from the Quick Actions menu to see specific scan settings.



Not seeing the profile you want? Log in to Qualys, go to Scans > Option Profiles, edit the profile(s) you want and select “Make this option profile available to all offline scanners”.

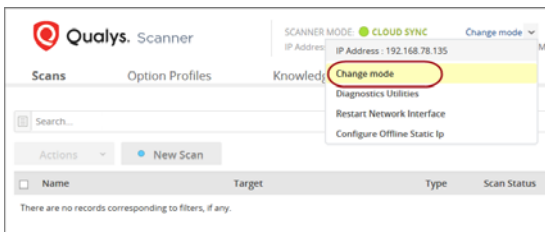


Your option profiles will be saved to the Scanner UI during the next sync. This could take more than 10 minutes.

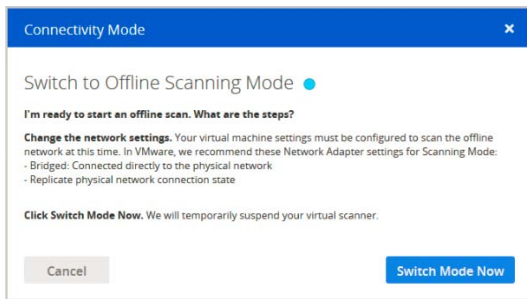
Want to check the status of the sync? Go to Scans > Appliances and choose Edit for your offline scanner. Then go to the Option Profile Sync section. You may hurry the process by clicking the Sync Now button.

Switch modes and make network settings

You'll need to switch to OFFLINE SCANNING mode.

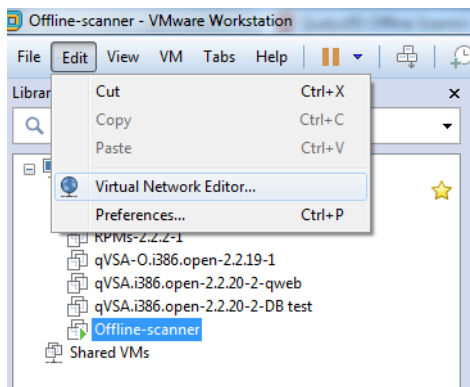


Choose Change mode to get started.

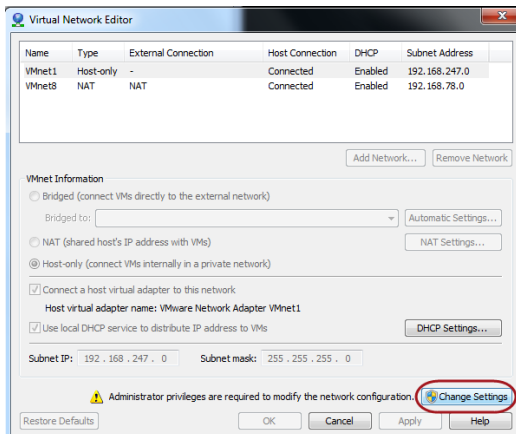


Go to VMware to make network settings.

Do **not** click the Switch Mode Now button. You'll do this later, after making settings in VMware.

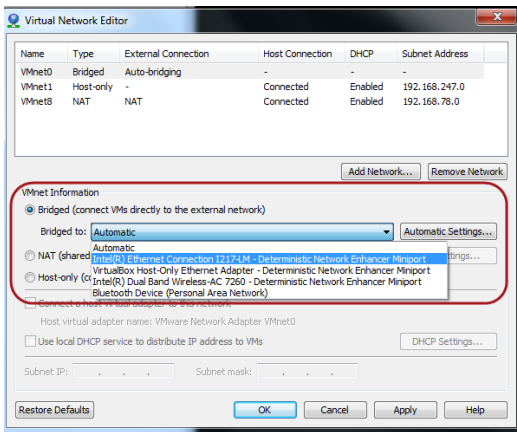


Bridged mode is required for offline scanning. To configure bridging in VMware, go to Edit > Virtual Network Editor.

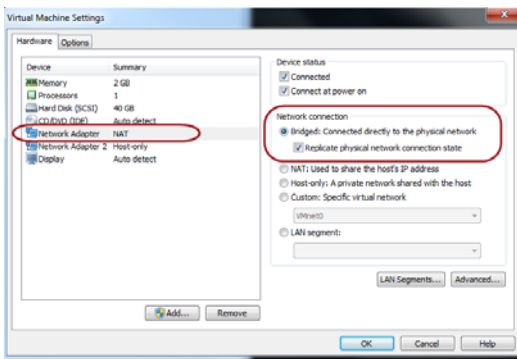


Click the Change Settings button. Administrator privileges are needed to modify network configuration.

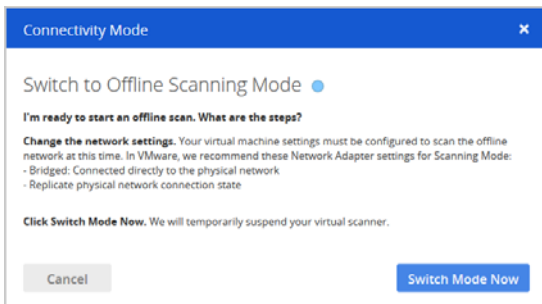
Click on Bridged and choose the correct interface from the menu for Bridged type.



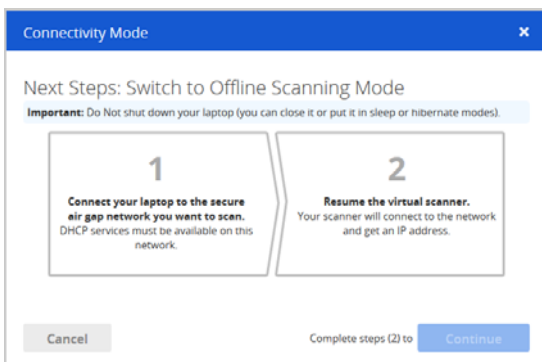
Configure virtual machine settings. For Network Adapter, select the Bridged network connection and “Replicate physical network connection state”. Save your settings.



Now that your network is configured for offline scanning, go back to the Web User Interface and click the Switch Mode Now button. We'll temporarily suspend your virtual scanner.

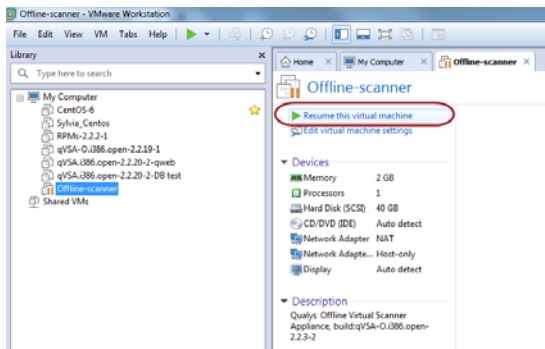


You'll see instructions on the screen to connect your laptop to the secure air gap network you want to scan and resume your scanner.

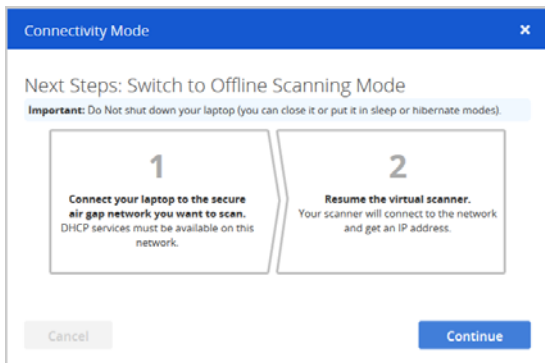


Start Offline Scanning

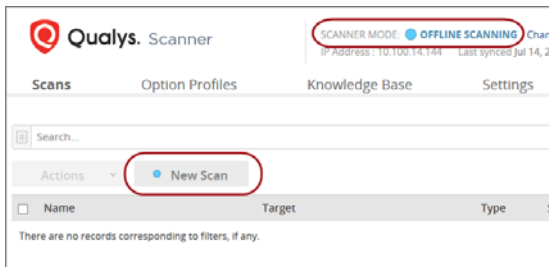
Ready for your first scan?



Start up the virtual scanner by choosing Resume this virtual machine.



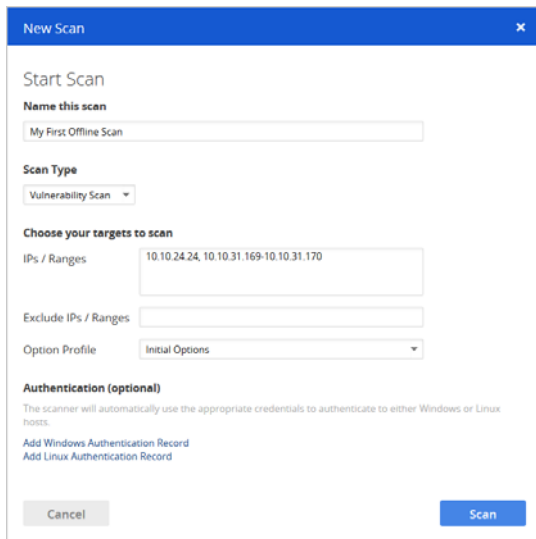
Once your virtual scanner is resumed, click the Continue button.



The scanner is now in OFFLINE SCANNING mode. Click the New Scan button to start your new scan.

Start your scan

You'll see the New Scan window. Give your scan a name, enter a scan target (the IPs you want to scan), select an option profile, and optionally provide authentication credentials. Then click Scan.



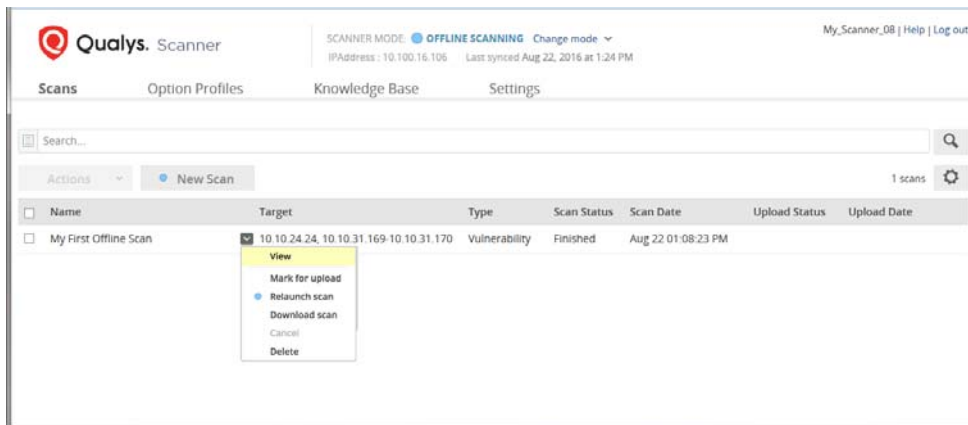
The 'New Scan' dialog box is shown. It has a blue header with the title 'New Scan' and a close button. The main content area is white and contains the following sections:

- Start Scan**
 - Name this scan**: A text input field containing 'My First Offline Scan'.
- Scan Type**: A dropdown menu with 'Vulnerability Scan' selected.
- Choose your targets to scan**
 - IPs / Ranges**: A text input field containing '10.10.24.24, 10.10.31.169-10.10.31.170'.
 - Exclude IPs / Ranges**: An empty text input field.
 - Option Profile**: A dropdown menu with 'Initial Options' selected.
- Authentication (optional)**
 - A note: 'The scanner will automatically use the appropriate credentials to authenticate to either Windows or Linux hosts.'
 - Two links: 'Add Windows Authentication Record' and 'Add Linux Authentication Record'.

At the bottom, there are two buttons: 'Cancel' (grey) and 'Scan' (blue).

Tip - You can provide both Windows and Linux authentication credentials. We'll automatically use the Windows credentials on your Windows hosts (in the scan target) and the Linux credentials on your Linux hosts.

Your scan will appear on the scans list where you can track the progress and view the results when the scan is finished - select View for any finished scan to see scan results.



The Qualys Scanner interface is shown. At the top, there's a header with the Qualys logo, 'Scanner', and 'SCANNER MODE: OFFLINE SCANNING'. Below this is a navigation bar with 'Scans', 'Option Profiles', 'Knowledge Base', and 'Settings'. A search bar is present. Below the search bar, there's a table of scans. The table has columns: Name, Target, Type, Scan Status, Scan Date, Upload Status, and Upload Date. One scan is listed: 'My First Offline Scan' with target '10.10.24.24, 10.10.31.169-10.10.31.170', type 'Vulnerability', status 'Finished', and scan date 'Aug 22 01:08:23 PM'. A context menu is open over the first scan, showing options: View, Mark for upload, Relaunch scan, Download scan, Cancel, and Delete.

| Name | Target | Type | Scan Status | Scan Date | Upload Status | Upload Date |
|-----------------------|--|---------------|-------------|--------------------|---------------|-------------|
| My First Offline Scan | 10.10.24.24, 10.10.31.169-10.10.31.170 | Vulnerability | Finished | Aug 22 01:08:23 PM | | |

You'll see scan details – total hosts scanned, total vulnerabilities found, etc. This is followed by a list of scanned hosts. Select View for any host to see host results.

The screenshot shows the Qualys Scanner interface. At the top, it indicates 'SCANNER MODE: OFFLINE SCANNING' and 'IP Address: 10.100.16.106'. Below this, there are tabs for 'Scans', 'Option Profiles', 'Knowledge Base', and 'Settings'. The main section is titled 'Scan : My First Offline Scan' and shows a 'scanning Finished' status. A search bar is present. The 'Scan Details' section lists the target IP range '10.10.24.24, 10.10.31.169-10.10.31.170', scan duration of '5 minutes', and upload status. The 'Total Hosts' section shows 3 total hosts, with 2 active, 1 excluded, and 1 dead. The 'Vulnerabilities' section shows 19 total vulnerabilities, with 13 confirmed, 6 potential, and 54 info gathered. Below this is a table of scanned hosts:

| IP | DNS | Operating System | Status | Total Vulns | Lev... | 5 | 4 | 3 |
|--------------|-----------------------|---|----------|-------------|--------|---|---|---|
| 10.10.31.170 | WIN-31-170.qualys.com | Windows 2008 R2 Enterprise Service Pack 1 | Finished | 12 | 2 | 1 | 5 | |
| 10.10.31.169 | WIN-31-169.qualys.com | Windows 2008 R2 Enterprise Service Pack 1 | Finished | 7 | 0 | 0 | 6 | |

A 'View' button is highlighted for the host 10.10.31.169.

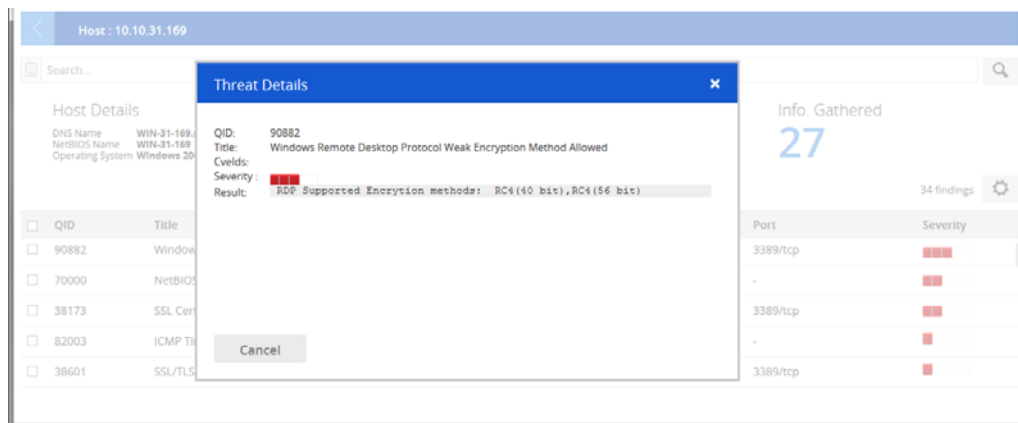
The host details are followed by a list of vulnerabilities and information gathered QIDs detected on the host. You can drill down further by selecting View for any QID to see threat details and scan results.

The screenshot shows the Qualys Scanner interface with the host details for 'Host: 10.10.31.169'. The 'Host Details' section lists the DNS Name 'WIN-31-169.qualys.com', NetBIOS Name 'WIN-31-169', and Operating System 'Windows 2008 R2 Enterprise Service ...'. The 'Total Vulnerabilities' section shows 7 total vulnerabilities, with 6 confirmed, 1 potential, and 27 info gathered. Below this is a table of vulnerabilities:

| QID | Title | Port | Severity |
|-------|--|----------|----------|
| 90882 | Windows Remote Desktop Protocol Weak Encryption Method Allowed | 3389/tcp | Critical |
| 70000 | Microsoft Remote Desktop Accessible | - | Critical |
| 38173 | SSL Certificate - Signature Verification Failed Vulnerability | 3389/tcp | Critical |
| 82003 | ICMP Timestamp Request | - | Critical |
| 38601 | SSL/TLS use of weak RC4 cipher | 3389/tcp | Critical |
| 90043 | SMB Signing Disabled or SMB Signing Not Required | - | High |
| 70004 | NetBIOS Bindings Information | - | Medium |
| 70022 | Open DCE-RPC / MS-RPC Services List | - | Medium |
| 45017 | Operating System Detected | - | Medium |
| 34011 | Firewall Detected | - | Medium |

A 'View' button is highlighted for the QID 90882.

The Threat Details include specific scan results returned for the QID on the host.

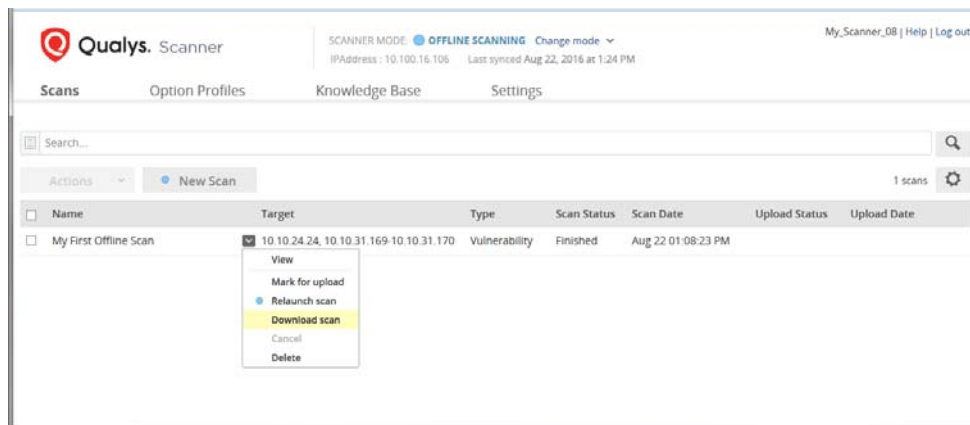


When you're done viewing results, close the Threat Details window and click the Back arrow in the blue bar to go back screen by screen.

Download scan results

Just choose the Download scan option for any finished vulnerability scan (not supported for map scans). You'll get a CSV report listing the QIDs detected on each scanned host along with info like the type, severity and specific scan results for each QID.

Good to Know- The Download scan option is disabled once the scan has been uploaded to your account, so you'll want to download results before uploading them.



Upload scan results

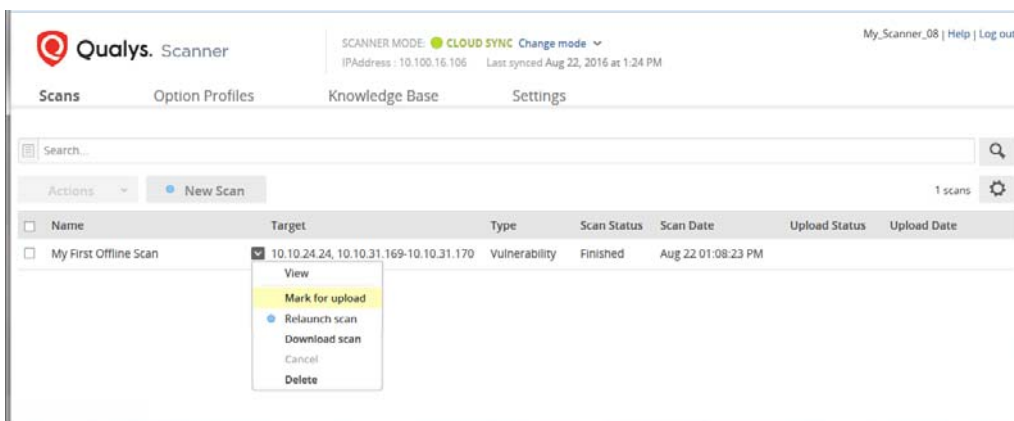
This will allow you to view your vulnerability scan results in your Qualys account and create reports based on the findings. Be sure you have Internet access to connect to the Qualys Cloud Platform.

A few things to consider...

- 1) Be sure to review and edit your network settings in VMware **before** switching to CLOUD SYNC mode. That way, when your scanner is resumed it will get the correct IP address assigned to it and you'll be able to connect to the Qualys Cloud Platform. [Learn more](#)
- 2) Any scanned IP that is not already in your account will be added to your account (and will count against your total IPs allowed).
- 3) The full scan results will no longer be available in the Scanner's Web UI. You will, however, still see scan summary information.
- 4) Only vulnerability scans can be uploaded, not map scans.

What are the steps?

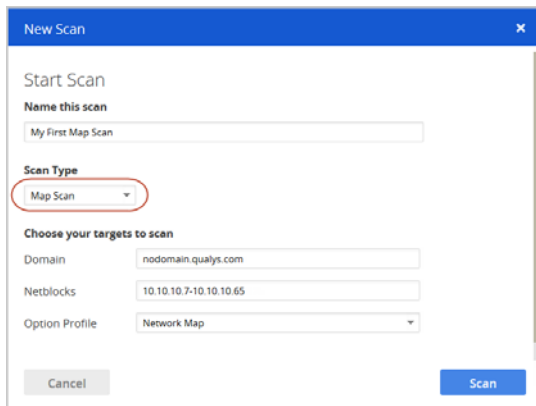
Click "Change mode" at the top of the page and switch to CLOUD SYNC mode. We'll connect to the Qualys Cloud Platform - this may take a few minutes. Once successfully connected, you're ready to continue. Select the scan you want to upload from the Scans list, and choose "Mark for upload" from the quick actions menu. That's it! The scan will be uploaded the next time you sync. (Tip – If you change your mind, go back to the quick actions menu and choose "Unmark for upload" before the sync happens.)



Discover live devices on your network

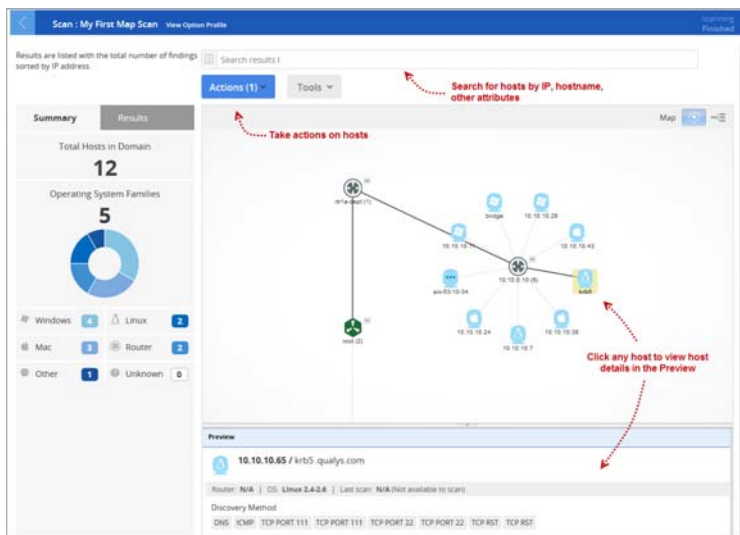
Run a map scan to get a visual map of your network devices. Once you know the devices on your network, you can scan them for vulnerabilities.

Go to Scans and click New Scan (you'll need to switch to OFFLINE SCANNING mode if you're not already there). In the New Scan window, select the type Map Scan, enter the domain and netblocks you want to map and choose an option profile. Then click Scan.



Tip - Want to map IPs and IP ranges without a domain name? Enter nodomain.qualys.com in the Domain field and your IPs in the Netblocks field, as shown in this example.

When your map scan is finished, select View to see the results. Check it out.



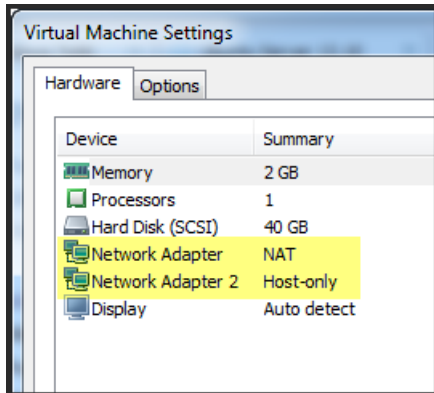
Want to learn more? Our Community has an article that explains the map images, how to change your map layout, and more.

From our Community

[New Maps](#)

VMware Configuration

The Qualys Offline Scanner Appliance should be configured with two virtual network adapters using your virtualization platform (i.e. VMware Workstation).



Your virtualization software should automatically create an instance of the appliance with the correct network adapters in place.

On VMware Workstation, these interfaces will be Network Adapter and Network Adapter 2. Initially, Network Adapter should default as type NAT; and Network Adapter 2 should default as type Host-only.

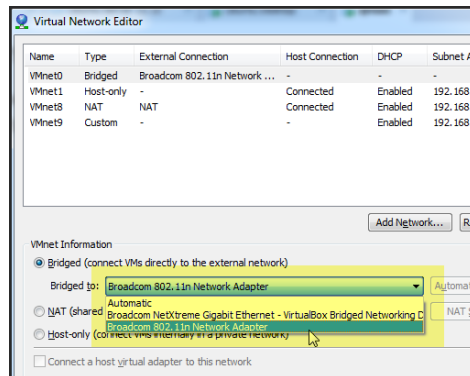
Network Adapter 1 must be configured for Bridged networking when in OFFLINE SCANNING MODE. It can be NAT or Bridged when in CLOUD SYNC MODE. Network Adapter 2 should always be configured for Host-only networking.

Here are the required network settings, depending on the mode you're in.

| | VMware Workstation default label | Appliance OS | Appliance Mode | Purpose | Required VMware network type | Connect a host virtual adapter | Local DHCP service |
|----------------|----------------------------------|--------------|------------------|--|------------------------------|--------------------------------|--------------------|
| Virtual NIC #1 | Network Adapter | eth0 | CLOUD SYNC | Communicate with the Qualys Cloud Platform | NAT* - or - Bridged** | enabled n/a | enabled n/a |
| | | | OFFLINE SCANNING | Scan hosts | Bridged** | n/a | n/a |
| Virtual NIC #2 | Network Adapter 2 | eth1 | any | Local scanner web UI | Host-only | enabled | enabled |

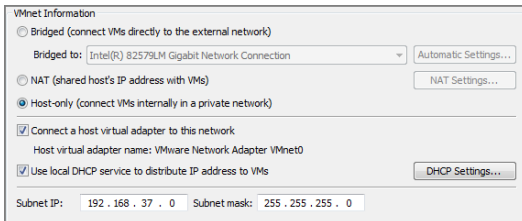
*** NAT configuration.** NAT is practically the only choice if your external connection goes over a VPN. Bridging from a virtual machine will not work over host VPN adapters.

**** Bridging to external networks.** VMware Workstation may be installed on a host system with multiple network adapters (wired, wireless, VPN). In the Virtual Network Editor, you'll need to determine which network adapter is appropriate for the external connection and select it. We do not recommend leaving the Bridged virtual network in "Automatic" mode because it almost never works and it is often problematic over wireless adapters.

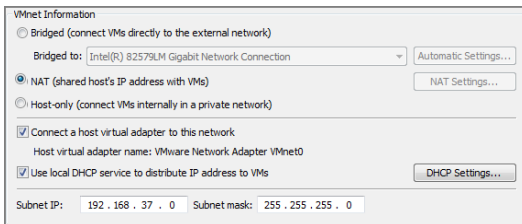


Sample network configurations

Host-only type

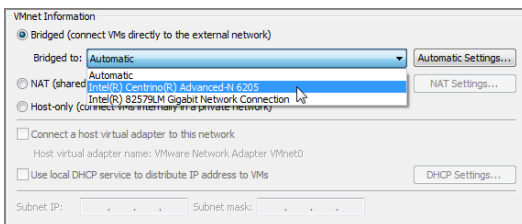


NAT type



Bridged type

If you've plugged into the physical network with an Ethernet cable, it is strongly recommended that you manually bridge your virtual network to the physical NIC of your host machine.



Leaving the "Bridged to:" setting in Automatic mode allows for the possibility that your virtual network will instead bind to a VPN port or other network adapter.