

# QUALYSGUARD® ENTERPRISE VIRTUAL SCANNER

## USER GUIDE

April 27, 2012



Copyright 2012 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.  
1600 Bridge Parkway  
Redwood Shores, CA 94065  
1 (650) 801 6100



# Table of Contents

<b>Welcome to Enterprise Virtual Scanner.....</b>	<b>4</b>
<b>Step 1: Provision a New Virtual Scanner.....</b>	<b>5</b>
How to provision a new virtual scanner .....	5
Next steps .....	6
<b>Step 2: Download and Save a Virtual Scanner Image.....</b>	<b>7</b>
How to download and save a virtual scanner image .....	7
Next step.....	8
<b>Step 3: Configure Your Virtual Scanner.....</b>	<b>9</b>
Review network requirements .....	9
Scanning and firewalls .....	9
Deploy the virtual scanner.....	10
View the Console for the virtual scanner .....	14
Check the Scanner Appliance status in QualysGuard.....	16
Optional configuration for VLANs and static routes .....	17
<b>FAQs .....</b>	<b>18</b>
How do I delete a virtual scanner?.....	18
What does the Network Error message mean? .....	18
What does the Communication Failure message mean?.....	19
Please tell me more about proxy support using the virtual scanner.....	19



## Welcome to Enterprise Virtual Scanner

QualysGuard® Enterprise Virtual Scanner is now available. QualysGuard Enterprise Virtual Scanner supports the same global scanning capabilities as the QualysGuard Scanner Appliance. VMware vCenter 5.0 and vSphere Client are required.

This user guide provides setup instructions using the new QualysGuard user interface.

### Requirements

VMware vCenter 5.0 and vSphere Client

The Pooled IPs feature must be defined and enabled for the destination network where the Enterprise Virtual Scanner will be installed. If your proxy requires authentication, you must include the credentials within the vCenter IP Pools Properties window in the “HTTP Proxy” field using this format: user:password@ip:port

### Availability

You must have a QualysGuard account with an active status, and the Enterprise Virtual Scanner option must be enabled for your subscription. Please contact your account representative if you would like the Enterprise Virtual Scanner option to be enabled for your subscription.



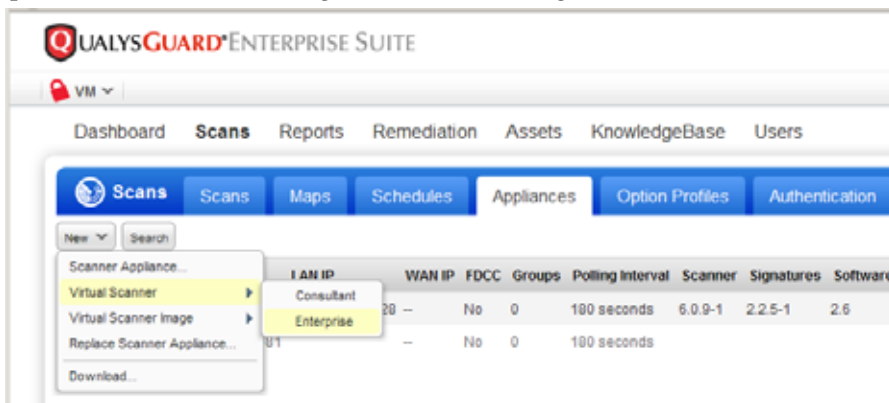
## Step 1: Provision a New Virtual Scanner

Provision a new Enterprise Virtual Scanner after you have registered for the Enterprise Virtual Scanner. Once provisioned, you must download a virtual scanner image and configure the virtual scanner using vSphere Client.

### How to provision a new virtual scanner

Login to your QualysGuard account to complete these steps.

**1) Go to Scans > Appliances, and then select New > Virtual Scanner > Enterprise.** (This option is available to Managers and Unit Managers).



**2) Enter a friendly name for the virtual scanner and then click the Provision button.**

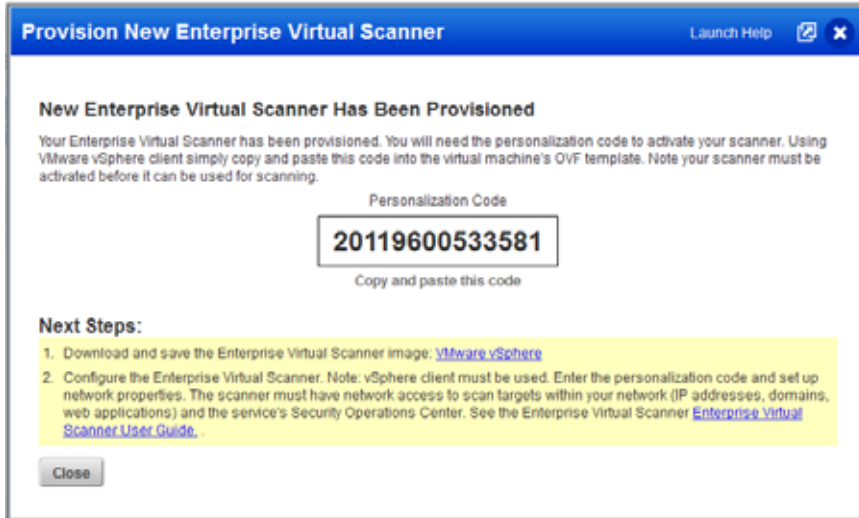
The friendly name can contain a maximum of 15 characters. These characters are allowed: ASCII characters, numbers and these special characters: - (dash), \_ (underscore), \ (backslash), and period (.).



(Unit Manager only) From the Assigned Groups menu (not shown above), select an asset group assigned to your business unit. Once provisioned and properly configured, the new scanner will be available to users in your business unit. The scanner will be available to all Unit Managers; it will be available to Scanners and Readers who have been assigned the asset group.

**3) Review the confirmation and copy the personalization code to a safe place.** You will need the personalization code to activate the scanner using vSphere Client.

Note: One personalization code can be used to activate one virtual scanner instance.



**4) Review Next Steps.** Click the “Enterprise Virtual Scanner User Guide” link in step 2 if you want to download the latest version of this user guide.

## Next steps

[Step 2: Download and Save a Virtual Scanner Image](#)

[Step 3: Configure Your Virtual Scanner](#)



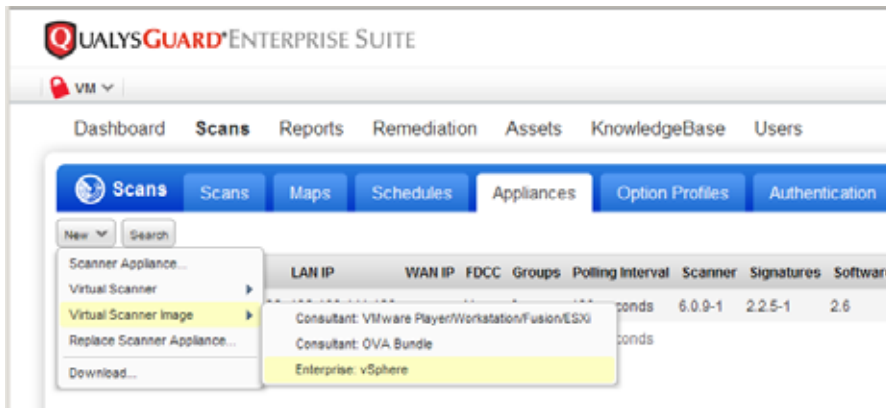
## Step 2: Download and Save a Virtual Scanner Image

Download and save an Enterprise Virtual Scanner Image after you have registered your account for the Enterprise Virtual Scanner. The master virtual scanner image may be used to activate multiple virtual scanner instances. Up to five instances may be activated within each subscription.

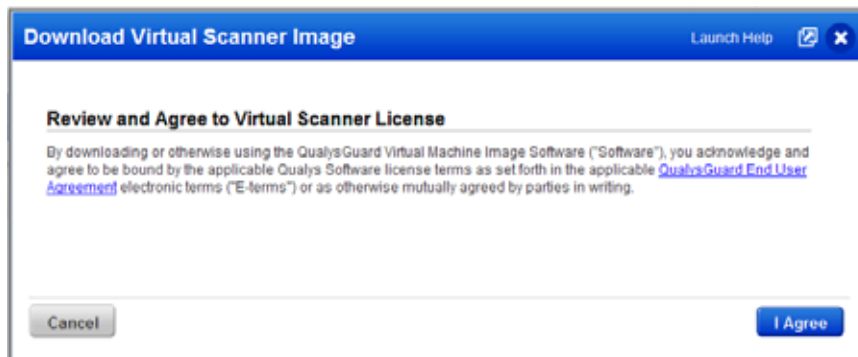
### How to download and save a virtual scanner image

Login to your QualysGuard account to complete these steps.

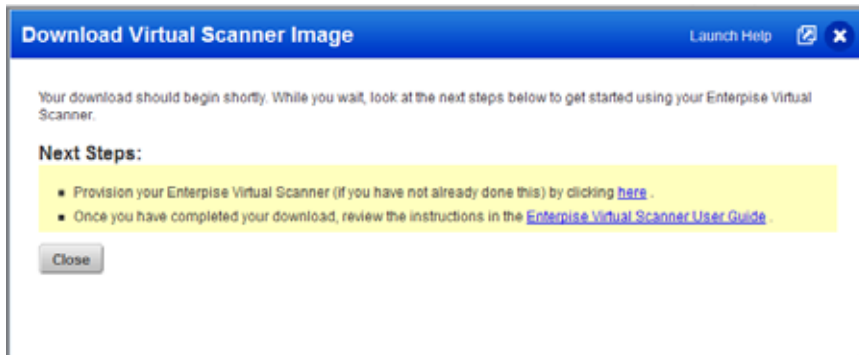
**1) Go to Scans > Appliances, and then select New > Virtual Scanner Image > Enterprise: vSphere.** (This option is available to Managers and Unit Managers).



**2) Review the end user license agreement and click "I Agree".** One virtual scanner image may be used to activate up to five virtual scanner instances.



**3) Save the virtual scanner image to your system.** The image will be saved to your downloads area, as defined by your browser settings. Then click Close to close the download window.



**4) Review the downloaded file.** Unzip the archive. One file is downloaded with this name: QVESA-<version>.ova (for example QVESA-1.0.0.ova).

## Next step

[Step 3: Configure Your Virtual Scanner](#)



## Step 3: Configure Your Virtual Scanner

After completing the previous steps, you are ready to configure your Enterprise Virtual Scanner using VMware vSphere Client and the Enterprise Virtual Scanner Image.

### Review network requirements

<b>Outbound HTTPS Access</b>	The local network must be configured to allow outbound HTTPS (port 443) access to the Internet, so that the virtual scanner can communicate with the QualysGuard platform.
<b>Accessibility of Target IP Addresses</b>	The IP addresses for the hosts to be scanned must be accessible to the virtual scanner.
<b>VMware vCenter 5.0</b>	Enterprise Virtual Scanner is supported using VMware vCenter 5.0. vSphere Client is required to complete the virtual scanner configuration and manage the virtual scanner using the console. Please consult your VMware documentation for proper installation and configuration of VMware vCenter 5.0.
<b>Bandwidth</b>	Minimum recommended bandwidth connection of 1.5 megabits per second (Mbps) to the QualysGuard platform.
<b>DHCP or Static IP</b>	By default the virtual scanner is pre-configured with DHCP. If configured with a static IP address, be sure you have the IP address, netmask, default gateway, and primary DNS.
<b>Proxy Support</b>	The virtual scanner includes Proxy support with or without authentication — Basic or NTLM. The Proxy server must be assigned a static IP address and must allow transparent SSL tunneling. Proxy-level termination (as implemented in SSL bridging, for example) is not supported.

### Scanning and firewalls

Executing a scan or map against a device shielded by a firewall is a common operation. Every day the Qualys scanning engine executes thousands of scans in network topologies that protect their servers with firewalls without any issues. Problems can arise when the scan traffic is routed through the firewall from the inside out, i.e. when the scanner is sitting in the protected network area and scans a target which is located on the other side of the firewall. Many modern firewalls are configured to track connections, maintain NAT and ARP tables and a scan operation against a large set of targets can overload these tables. The consequences of such overflows are varied and range from slowdown of the firewall functions to a complete crash.

We recommend placing scanner appliances and virtual scanners in your network topology in a way that scanning and mapping through a firewall from the inside out is avoided if possible. Otherwise, we recommend you perform your own assessment testing on your network to

validate the impact to your firewall. The accuracy of your scan may also be impacted so you should compare expected results against the detailed results provided in your QualysGuard reports. It's possible this can be service impacting as the scan results might differ.

## Deploy the virtual scanner

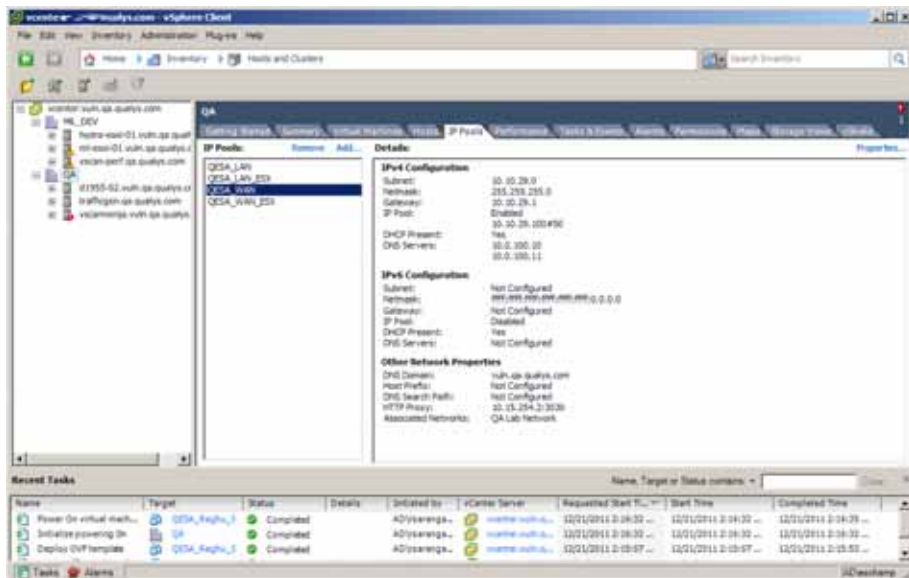
Use vSphere Client to deploy your Enterprise Virtual Scanner and add it to your vCenter server.

### 1) Install vSphere Client and log in.

**2) Check IP Pools.** Please check that IP pools for the virtual scanner's network interfaces are defined and enabled at this time. As described below in step 9 you will need to map the virtual scanner network LAN and WAN interfaces to destination networks (subnets).

**Requirement:** The destination networks must have IP pools defined and enabled in order to power up the virtual scanner.

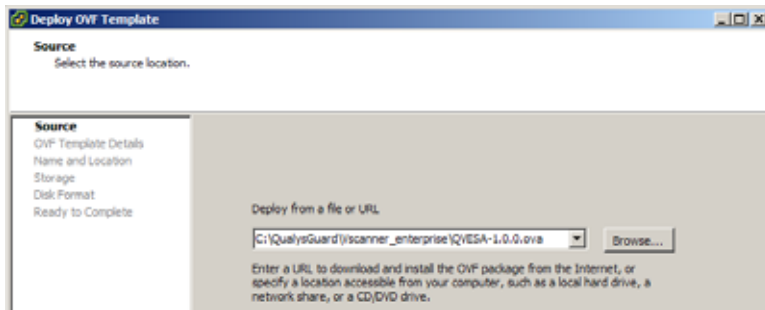
**Support for Authenticated Proxy:** If your proxy requires authentication, you must include the credentials within the vCenter IP Pools Properties window in the "HTTP Proxy" field using this format: user:password@ip:port



### 3) Select an ESXi host in the left panel.

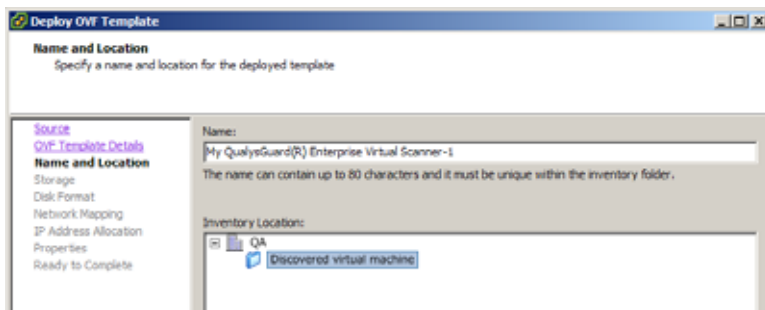
### 4) Go to File > Deploy OVF Template. Use the wizard to complete the sections below.

**5) Source.** Select the Enterprise Virtual Scanner Image OVA file you downloaded earlier. The filename will be QVESA-<version>.ova (for example QVESA-1.0.0.ova).



**6) OVF Template Details.** View the appliance details, including the Enterprise Virtual Scanner version number.

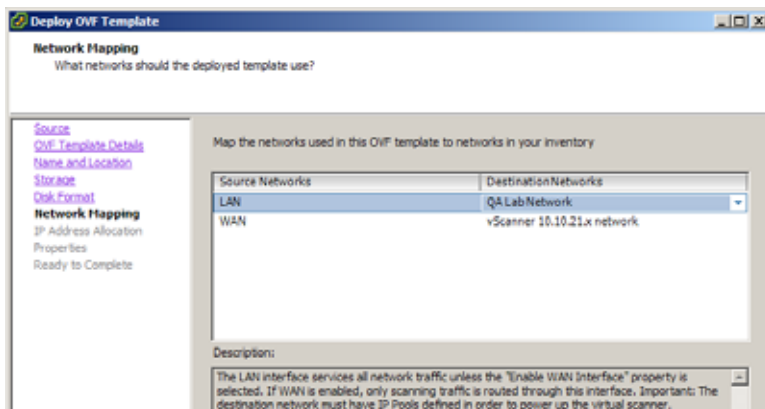
**7) Name and Location.** Provide a custom name and select a location.



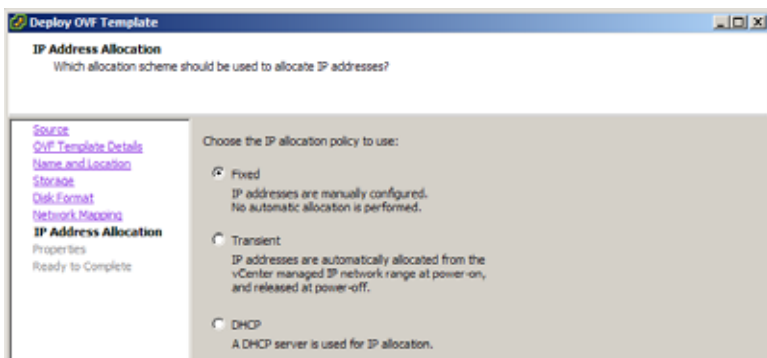
**8) Disk Format.** Select settings appropriate for your environment.

**9) Network Mapping.** Select destination networks for the LAN and WAN network interface that the deployed virtual scanner will use. Important: The destination networks must have IP pools defined and enabled in order to power up the virtual scanner.

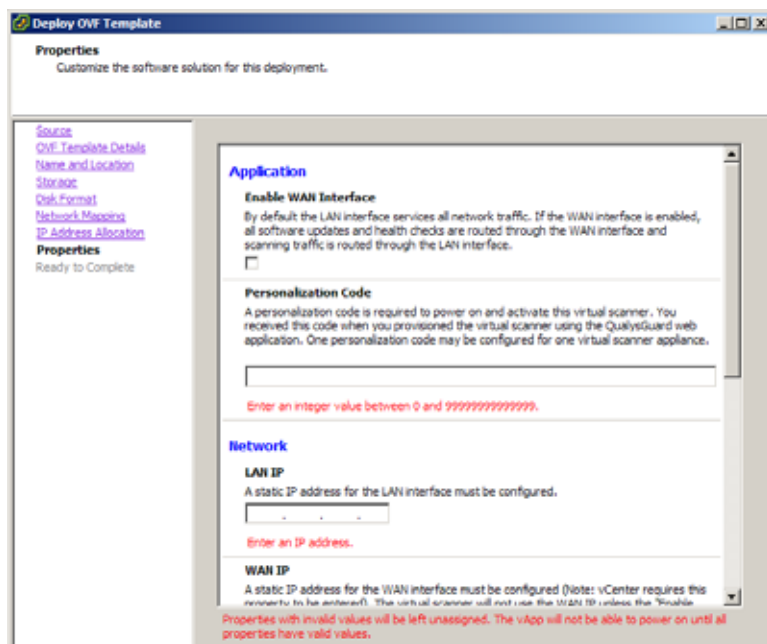
The LAN interface services all network traffic unless the “Enable WAN Interface” property is selected. If selected, only scanning traffic is routed through this interface. The WAN interface is used to service management traffic (software updates and health checks) if the “Enable WAN Interface” property is selected.



**10) IP Address Allocation.** Choose the IP allocation method to be used: Fixed, Transient or DHCP. Using Fixed or Transient, the IP address and network properties are inherited from pools. Using DHCP, the local DHCP server is used for IP allocation.



**11) Properties.** Additional properties for the virtual scanner appear in this section.



Important: A personalization code obtained from your QualysGuard account is required.

**Application**

Enable WAN Interface	By default the LAN interface services all network traffic. If the WAN interface is enabled, all software updates and health checks are routed through the WAN interface and scanning traffic is routed through the LAN interface.
----------------------	---

Personalization Code	A personalization code (14 digits) is required to power on and activate this virtual scanner. You received this code when you provisioned the virtual scanner using the QualysGuard web application. One personalization code may be configured for one virtual scanner appliance.
----------------------	--

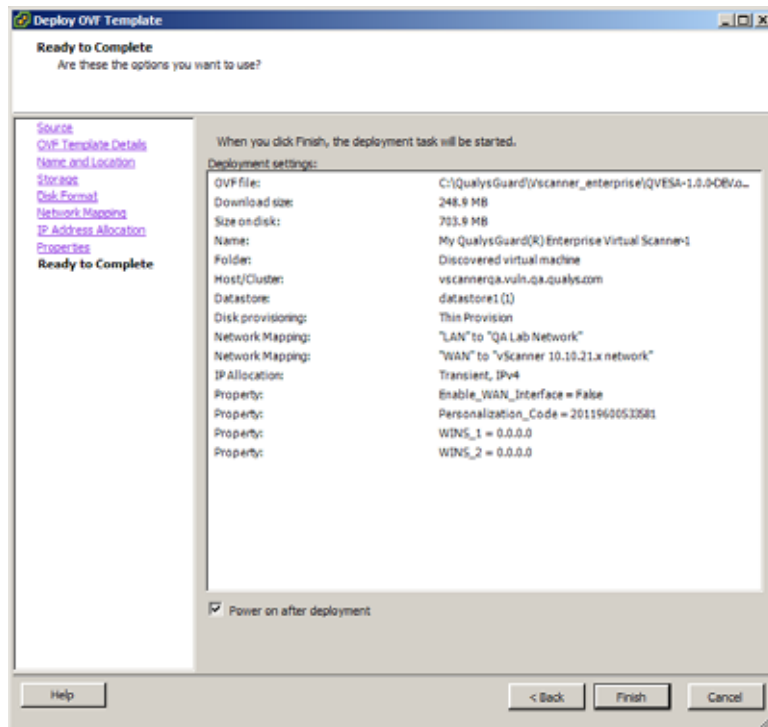
## Network

LAN IP	(Appears when "IP Address Allocation" is Fixed.) A static IP address for the LAN interface must be configured.
WAN IP	(Appears when "IP Address Allocation" is Fixed.) A static IP address for the WAN interface must be configured. vCenter requires this property. The appliance will not use the WAN IP unless the "Enable WAN Interface" property is selected.

## Scanner

WINS 1	Enter an IP address to configure a primary WINS address. This is used only if you are running Windows Internet Naming Service and the virtual scanner needs to use it for name resolution.
WINS 2	Enter an IP address to configure a secondary WINS address. This is used only if you are running Windows Internet Naming Service and the virtual scanner needs to use it for name resolution.

**11) Ready to Complete.** Select "Power on after deployment" and then click Finish.



## What happens next

The virtual scanner powers up and the QualysGuard service completes the activation process. It may take a few minutes for this to occur. The virtual scanner attempts to make a connection to the QualysGuard platform using its current configuration (network and proxy settings).

## View the Console for the virtual scanner

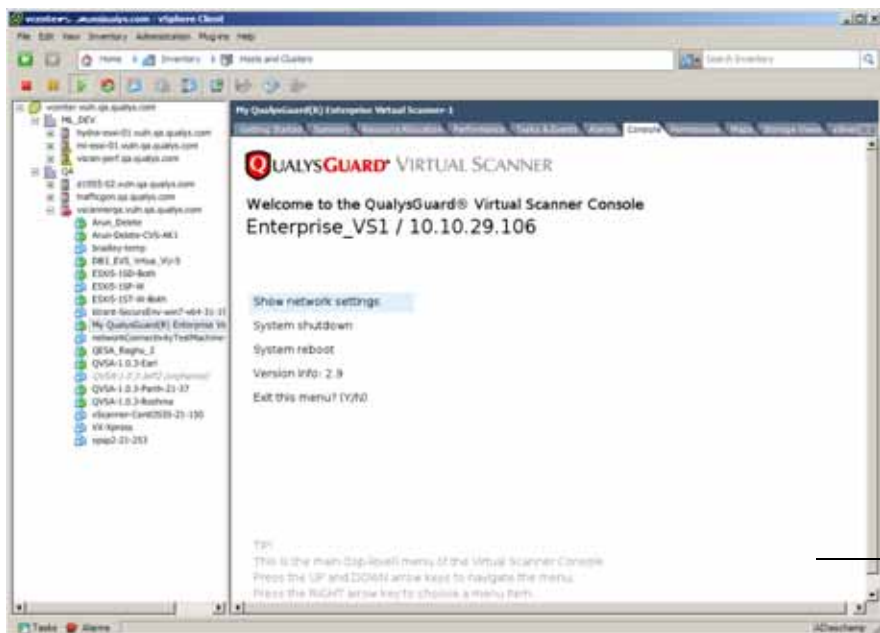
**1) Select the virtual scanner machine in the left panel.** The virtual scanner will be listed under the ESXi host where you deployed the virtual scanner.

**2) Select the Console tab.** System messages appear within the console during the startup and activation process.

**3) View Friendly Name and IP Address.** The appliances's friendly name and IP address appear when the appliance successfully connected to the QualysGuard platform and it has been activated. This also means the virtual scanner is ready to be used for scanning. If a network error appears, you need to troubleshoot the issue at this time. Be sure you followed the instructions for deploying the virtual scanner, as described in this document. See [FAQs](#) for assistance.



**4) Display the main menu.** Press Enter to display to the main menu. (Note: Use the Up and Down arrows to navigate the menu.)



**Tips:** Refer to this section on each screen for help.

5) **Check the network settings.** Press the Right arrow to display the network settings configured for the virtual scanner. Press the Left arrow to leave this screen and return to the main menu.



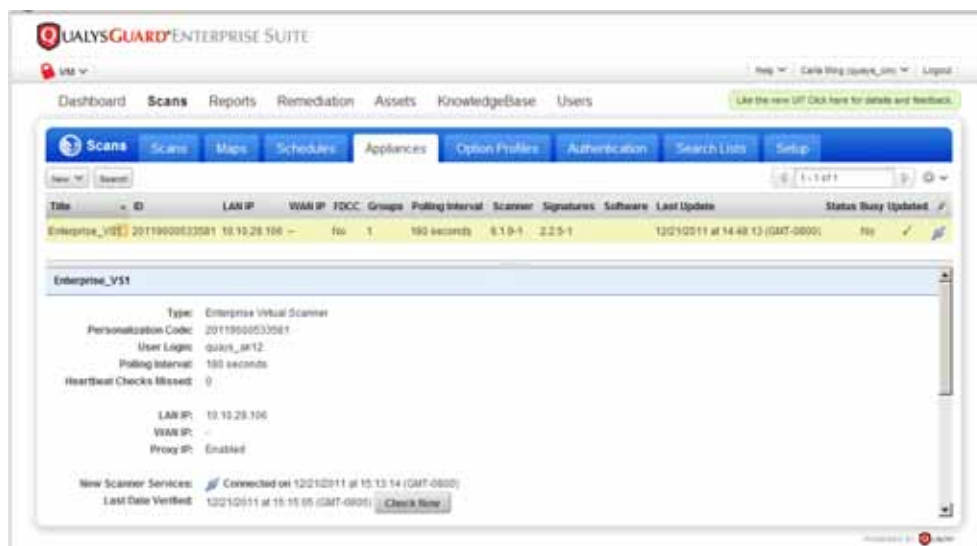
## Check the Scanner Appliance status in QualysGuard

We recommend you login to your QualysGuard account to view the virtual scanner appliance within your account.

**1) Go to the appliances list.** Log in to your QualysGuard account. Under VM go to Scans > Appliances.

**2) View the virtual scanner appliance information.** Select the row for your newly deployed virtual scanner and view its information in the preview pane. You'll see the Type field displays Enterprise Virtual Scanner along with the personalization code used to activate it.

Note: The virtual scanner should not be grayed out. A grayed out scanner indicates the scanner has been provisioned but not personalized yet, so it cannot be used for scanning your network.




**3) Check the New Scanner Services status.** The New Scanner Services status (🌐) column identifies whether the scanner appliance has connectivity to New Scanner Services at the SOC (Security Operations Center) and is ready to start processing new scans. New Scanner Services is a part of our global scanning infrastructure.

The status 🌐 (Connected) means the scanner appliance is ready to process new scans.


The status 🚫 (Not Connected) means the scanner appliance is not ready to process new scans. We recommend you check to be sure the appliance has network access to the scanning servers at the SOC. Appliances installed in your network must be able to send probes to target hosts from these URLs and you may need to whitelist them. Go to Help > About to see the list of scanning server URLs for your account. Please contact Support if you need help with troubleshooting this issue.

**Notice to Our Customers:** We are in the process of transitioning customers to use New Scanner Services. During the transition period, your subscription may not be configured to use New Scanner Services. If your account has not been configured yet, the status 🚫 (Not Used) appears, and this is no reason for concern. The appliance is ready to process scans. To see whether your subscription has been configured (enabled) for New Scanner Services, go to Help > Account Info > General Information.

**4) Check additional status.** Additional status is provided for your information.

Status. The heartbeat check status is online (blank) or offline (  ) based on the latest heartbeat check performed by the service (every 4 hours).

Busy. A scanner appliance is busy when it is processing one or more maps or scans. A newly installed scanner appliance will not be busy until a user launches a scan using the appliance.

Updated. The software is up to date when a  (green check) appears. The service will automatically update the software so you do not need to take any action. You have the option to request a software update by editing the scanner appliance (under Versions, click Update Now).

## Optional configuration for VLANs and static routes

It's possible to define VLANs and/or static routes for the virtual scanner appliance by editing the appliance's settings using the QualysGuard user interface when VLANs and Static Routes support is enabled for your subscription. To edit the appliance settings go to the scanner appliances list (under VM, go to Scans > Appliances). Select the row for your virtual scanner and then select Edit from the Quick Actions menu.



## FAQs

### How do I delete a virtual scanner?

Once provisioned, virtual scanners in your subscription appear in your scanner appliances list. Managers and Unit Managers have permissions to delete virtual scanners from their subscription. To delete a virtual scanner using the new user interface, select VM and go to Scans > Appliances, select the row for the virtual scanner you would like to delete, and then select Delete from the Quick Actions menu.

### What does the Network Error message mean?

The NETWORK ERROR message indicates the virtual scanner attempted to connect to the QualysGuard platform via HTTPS (port 443) and failed. The message appears with an error code (see below).

Important! The virtual scanner is not functional until the NETWORK ERROR message is resolved. Using the Virtual Scanner Console, make sure the network set up and/or proxy configuration is correctly defined.

The error code displayed with a network error message provides specific information on the error to assist with troubleshooting. If you need further assistance with troubleshooting the issue, please identify the error code when you contact Qualys Support.

Network Error Code	Description
E00	Internal error (NTLM Proxy error)
E01	
E02	Internal error (Proxy error)
E03	Proxy configuration error
E04	No connectivity after the Proxy was disabled
E05	DNS lookup of the QualysGuard server failed (maybe network connectivity problem)
E06	Cannot reach the QualysGuard server via HTTPS
E07	Invalid LAN IP address or LAN gateway address
E09	LAN IP address or LAN gateway address cannot be 127.0.0.1
E10	Could not configure the LAN interface
E13	DNS lookup of the QualysGuard server failed due to a network connectivity problem
E14	DNS lookup of the QualysGuard server failed during scanner activation due to a network connectivity problem

More general error codes may be overwritten by more specific ones. For example, the virtual scanner may return the error code E04 (No connectivity after the Proxy was disabled). After trying to connect for a while, the error code may be overwritten by E13 (DNS lookup of the QualysGuard server failed). When troubleshooting the network error, it's useful to watch these error codes scroll by.

## **What does the Communication Failure message mean?**

The COMMUNICATION FAILURE message appears if there is a network breakdown between the virtual scanner and the QualysGuard platform.

The communication failure may be due to one of these reasons: the local network goes down, Internet connectivity is lost for some reason, or any of the network devices between the virtual scanner and the QualysGuard platform goes down.

Note the sequence of events following a network breakdown:

If there are no scans and/or maps running on the appliance: The next time the virtual scanner sends a polling request to the QualysGuard platform, the polling request fails, and then the COMMUNICATION FAILURE message appears.

If there are scans and/or maps running on the appliance: The COMMUNICATION FAILURE message appears after the running scans and/or maps time out. In this case it is recommended you use the QualysGuard interface to cancel any running scans and/or maps and restart them to ensure that results are accurate.

After the network breakdown is resolved, the virtual scanner friendly name and IP address appear automatically. Then you can start scans and maps. The COMMUNICATION FAILURE message may not disappear right away for the reasons described below.

The COMMUNICATION FAILURE message remains until the next time the virtual scanner makes a successful polling request to the QualysGuard platform. There may be a lag time after the network is restored and before the scanner is back online, depending on when the next polling request is scheduled. Additional time is necessary for communications to be processed by a Proxy server if the virtual scanner has a Proxy configuration.

## **Please tell me more about proxy support using the virtual scanner.**

The virtual scanner does not support Proxy servers in networking environments where the Proxy server IP address is dynamically assigned. The virtual scanner does not support SOCKS proxies.

While using a virtual scanner with a Proxy configuration, you may notice the following:

Lag Time for Polling — There may be a lag time before virtual scanner configuration changes take effect. Changes may take effect after a period of time that is significantly longer than the polling interval. This is because there is additional time necessary for communications to be processed by the Proxy server.

No results or incomplete results — If the Proxy server sets limits for the absolute session timeout and/or the amount of outbound data that can be sent from the virtual scanner, you may receive no results or incomplete results. It's possible that the QualysGuard service terminates without completing a map or scan if these limits are set and a large number of IPs are scanned.