



QUALYSGUARD® CONSULTANT VIRTUAL SCANNER

USER GUIDE

January 10, 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

| | |
|--|-----------|
| Welcome to Consultant Virtual Scanner | 4 |
| Step 1: Provision a New Virtual Scanner | 5 |
| How to provision a new virtual scanner | 5 |
| Next steps | 6 |
| Step 2: Download and Save a Virtual Scanner Image | 7 |
| How to download and save a virtual scanner image | 7 |
| Next steps | 8 |
| Step 3: Install and Configure a Virtualization Platform | 9 |
| Install and configure VMware | 9 |
| Install and configure Oracle VirtualBox | 10 |
| Next steps | 10 |
| Step 4: Configure Your Virtual Scanner | 11 |
| Review network requirements | 11 |
| Scanning and firewalls | 11 |
| How to configure the virtual scanner | 12 |
| Customize the network set up | 14 |
| Enable proxy configuration | 15 |
| Check the Scanner Appliance Status in QualysGuard | 16 |
| Optional configuration for VLANs and static routes | 17 |
| FAQs | 18 |
| How do I remove virtual scanners? | 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 Consultant Virtual Scanner

QualysGuard® Consultant Virtual Scanner is now available. This user guide provides setup instructions using the original QualysGuard user interface.

The QualysGuard Consultant Virtual Scanner provides consultants with a convenient way to conduct security auditing engagements with their customers using QualysGuard IT Security and Compliance Suite. Consultants can complete virtual scanner setup before arriving at the customer location. Upon arrival consultant simply start the virtual scanner within the virtualization platform of their choice (VMware or Oracle VirtualBox) and then start scanning and reporting using the QualysGuard user interface.

QualysGuard Consultant Virtual Scanner supports the same global scanning capabilities as the QualysGuard Scanner Appliance, however certain network configurations are not supported at this time. The virtual scanner has one network configuration (split network configuration is not supported), and it does not support configuration for VLANs or Static Routes.

Availability

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



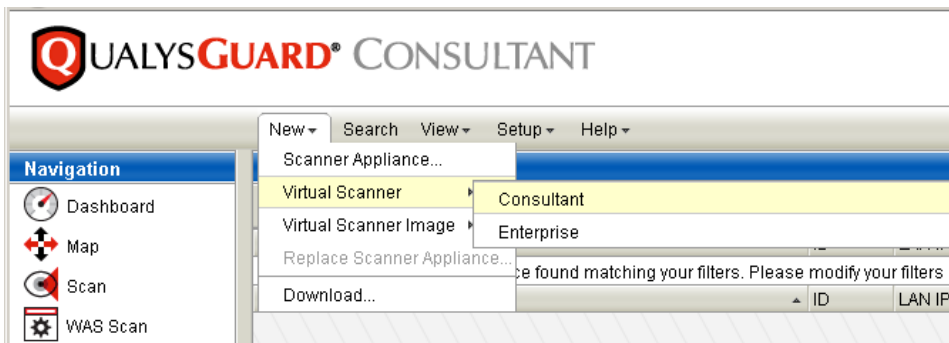
Step 1: Provision a New Virtual Scanner

Provision a new virtual scanner after you have registered for the Consultant Virtual Scanner. Once provisioned, you must download a virtual scanner image and configure the virtual scanner by running the Virtual Scanner Console on VMware or Oracle VirtualBox.

How to provision a new virtual scanner

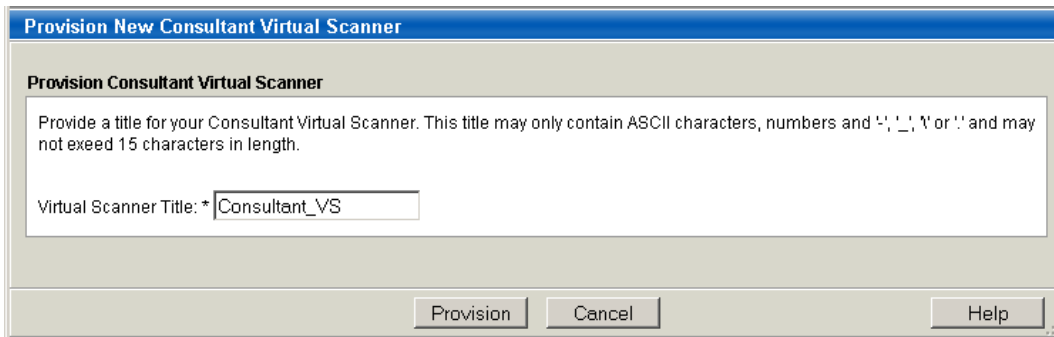
Login to your QualysGuard account to complete these steps.

1) From the scanner appliances list, go to New > Virtual Scanner > Consultant. (This option is available to Managers and Unit Managers).



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

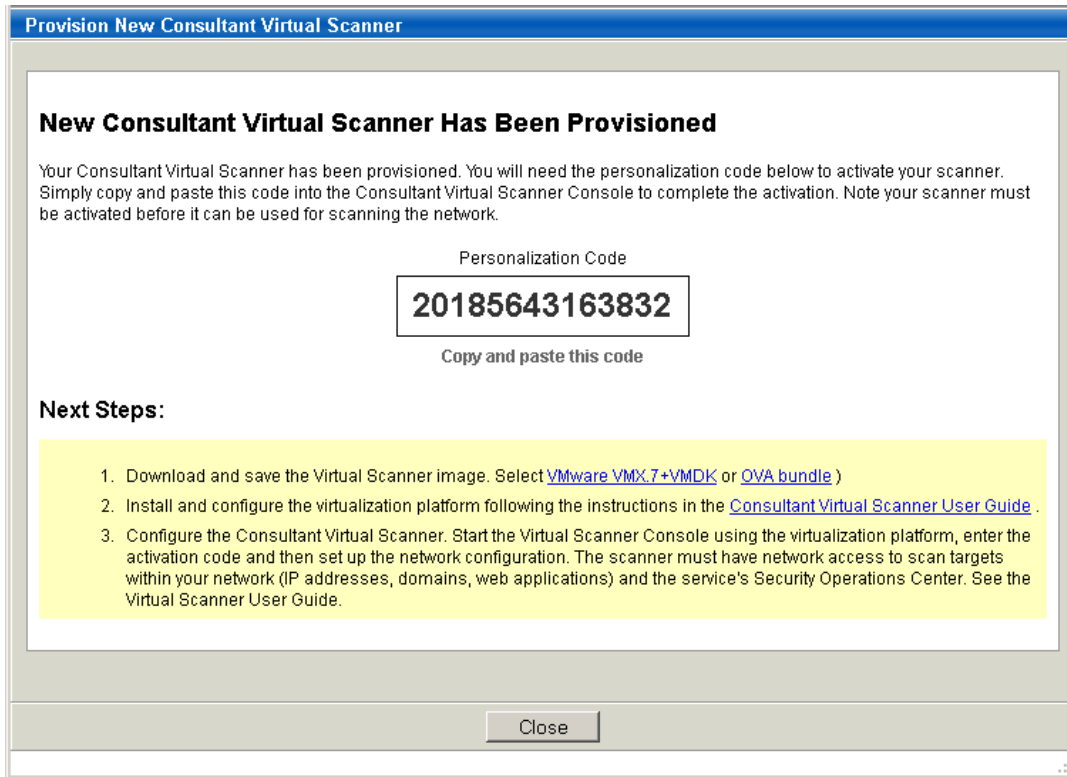
The friendly name can contain a maximum of 15 characters. These characters are allowed: ASCII characters, numbers and these special characters: - (dash), _ (underscore), \ (backslash), and period (.).



(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 the Virtual Scanner Console.

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



4) Review Next Steps. Click the “Consultant 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: Install and Configure a Virtualization Platform](#)

[Step 4: Configure Your Virtual Scanner](#)



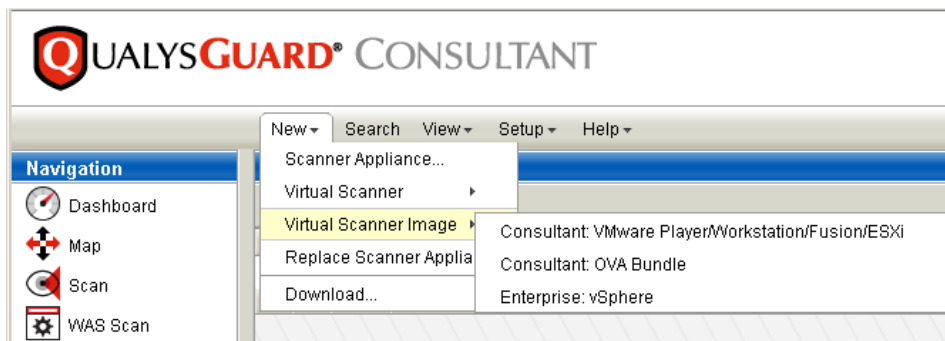
Step 2: Download and Save a Virtual Scanner Image

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

How to download and save a virtual scanner image

Login to your QualysGuard account to complete these steps.

1) Select a virtual scanner image. You may select an image from the Provision New Virtual Scanner workflow (see Step 1) or by selecting New > Virtual Scanner Image. (This option is available to Managers and Unit Managers). Select one of the Consultant images, depending on which virtualization platform you'd like to use.



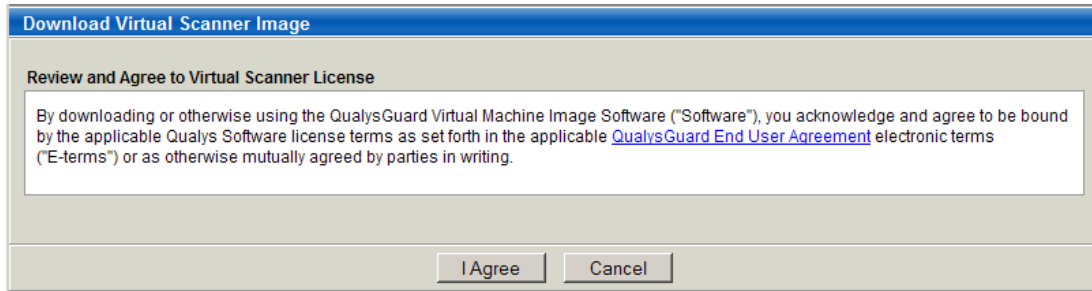
Your Consultant image options are:

Consultant: VMware Player/Workstation/Fusion/ESXi. A VMware virtual machines .zip image. These products are supported: VMware Player, Workstation, Fusion and ESXi.

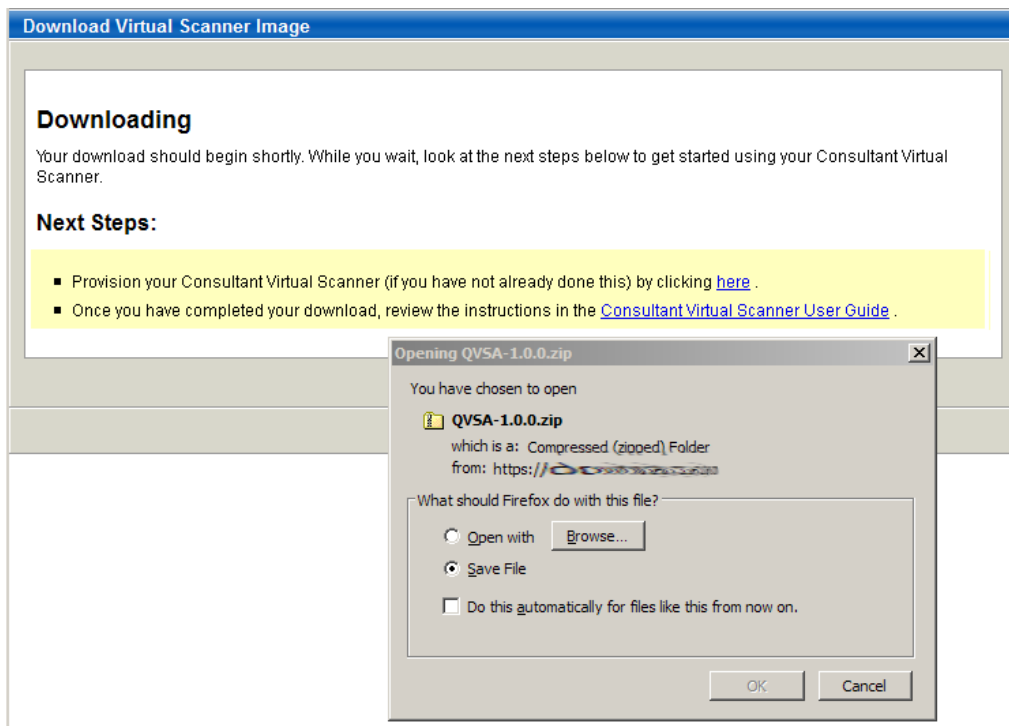
Consultant: OVA Bundle. A OVF + VMDK image for Oracle VirtualBox or manual conversion tool with VMware OVFTool.

Note: The Enterprise: vSphere option only appears if your account is also registered for the Enterprise Virtual Scanner. This option only works for Enterprise virtual scanners.

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(s). For the VMware image, unzip the archive. Two files are included: QVSA-<version>.vmx and QVSA-<version>-disk1.vmdk. For the OVA Bundle, one file is downloaded: QVSA-<version>.ova.

Next steps

[Step 3: Install and Configure a Virtualization Platform](#)

[Step 4: Configure Your Virtual Scanner](#)



Step 3: Install and Configure a Virtualization Platform

Install and configure one of the supported virtualization platforms to be used to run the virtual scanner image you've saved on your system.

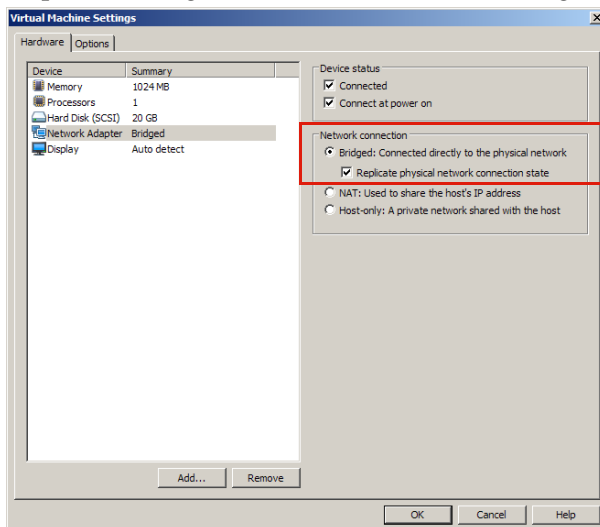
Install and configure VMware

- 1 Install a VMware product on your local machine. These products are supported: VMware Player, Workstation, Fusion and ESXi.
- 2 Start the VMware platform and open the virtual scanner machine.
- 3 Navigate to the network settings. Go to Virtual Machine > Virtual Machine Settings. In the settings window on the Hardware tab, select the device "Network Adapter".
- 4 Under Network connection, check to be sure "Bridged" is selected. The "Bridged" setting is required. Make changes if needed, and then click OK.

Bridged: Connected directly to the physical network (Required) Select this radio button.

Replicated physical network connection state (Recommended) Select this check box if you use virtual machines on a laptop or virtual device. As you move from one wired or wireless network to another, the IP address is automatically renewed.

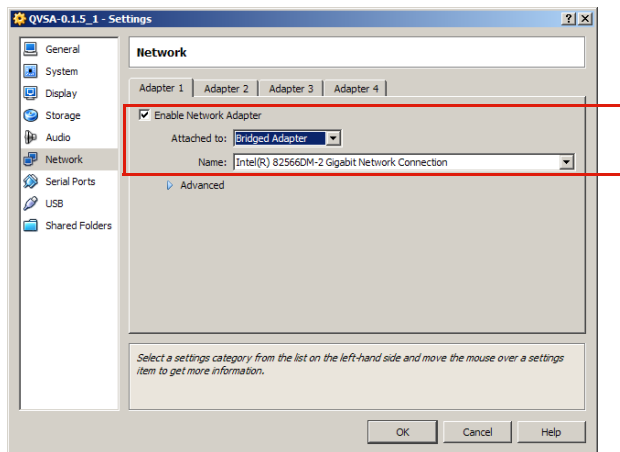
Required "Bridged" network connection setting:



Install and configure Oracle VirtualBox

- 1 Download VirtualBox and save to your local machine. VirtualBox may be downloaded from: <http://www.virtualbox.org/wiki/Downloads>
- 2 Run the VirtualBox download file and complete the VirtualBox Setup Wizard.
- 3 Open Oracle VM VirtualBox Manager, select File > Import Appliance to start the Import Appliance Wizard. Using the wizard, click the Choose button and select the QVSA-<version>.ova file to import. Click Next and then Finish to import the scanner.
- 4 Navigate to the network settings. Select the appliance from the list. Right click and select "Settings". In the settings window, select "Network" on the left to view the network settings group.
- 5 Check to be sure "Bridged Adapter" is enabled for the virtual scanner appliance. The "Bridged Adapter" setting is required. On the Adapter 1 tab make sure you've selected "Enable Network Adapter" and "Attached to: "Bridged Adapter"". Make changes if needed, and then click OK.

Required network settings:



- 6 Start the virtual scanner appliance. Select the appliance from the list. Right click and select "Start".

Next steps

[Step 4: Configure Your Virtual Scanner](#)



Step 4: Configure Your Virtual Scanner

After completing the previous steps, you are ready to configure the virtual scanning using start the Virtual Scanner Console. You must activate the virtual scanner by entering the personalization code you received when you provisioned the virtual scanner in Step 1. Optionally, you can configure network settings. By default DHCP is enabled unless you choose to configure a static IP configuration. Proxy configuration is also supported.

Review network requirements

| | |
|--|---|
| Outbound HTTPS Access | 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. |
| Accessibility of Target IP Addresses | The IP addresses for the hosts to be scanned must be accessible to the virtual scanner. |
| Virtualization Platform using “Bridge” Mode | <p>These virtualization platforms are supported: VMware Player, Workstation and Fusion, and Oracle VirtualBox. See Step 3 for instructions on how to install and configure the virtualization platform.</p> <p>IMPORTANT: Due to limitations of the NAT implementation of the VMware products and Oracle VirtualBox, it is strongly recommended not to use “NAT mode” in these products, but “Bridge mode” instead. Otherwise, depending on manufacturer and product, the NAT tables may be exhausted after scanning as few as two (2) hosts, leading to truncated and erroneous scan results.</p> |
| Bandwidth | Minimum recommended bandwidth connection of 1.5 megabits per second (Mbps) to the QualysGuard platform. |
| DHCP or Static IP | 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. |
| Proxy Support | 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.

How to configure the virtual scanner

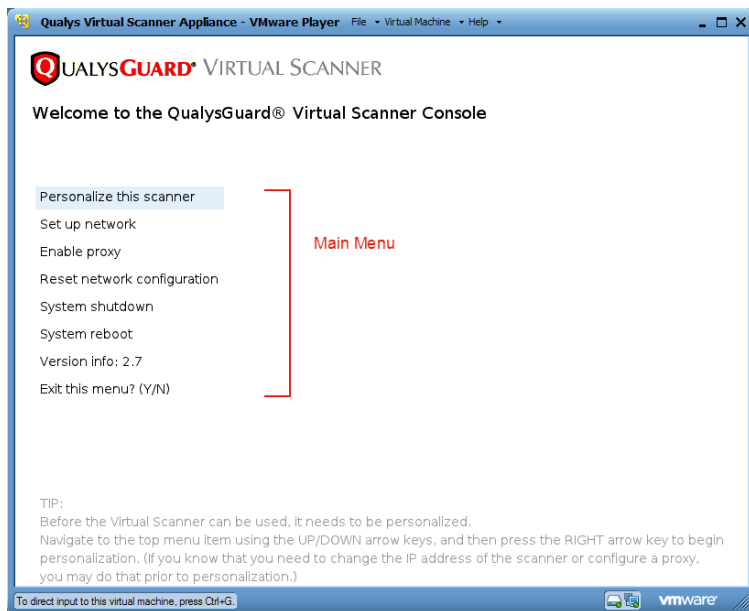
1) Start the Virtual Scanner Console using the virtualization platform.

Using VMware, start the platform and run the .vmx executable.

Using Oracle VirtualBox, start Oracle VM VirtualBox Manager and open the virtual scanner (appliance).

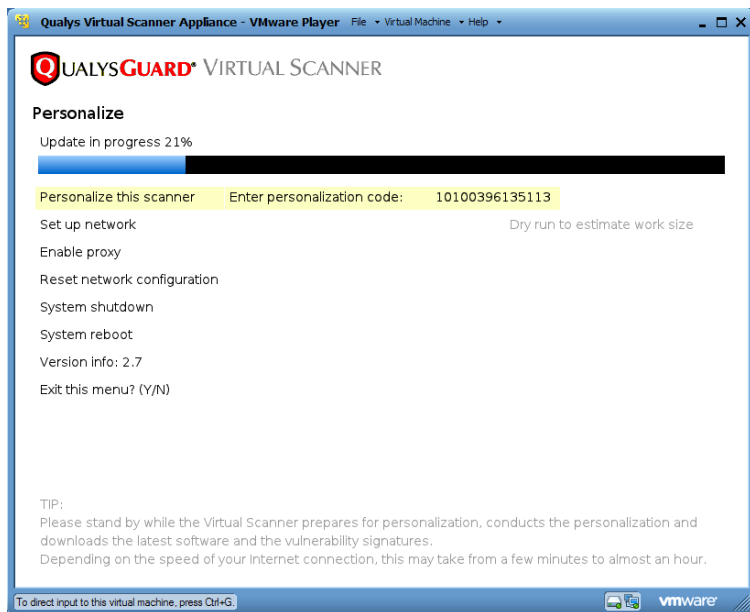
2) Select "Personalize this scanner". To use DHCP without proxy configuration, select "Personalize this scanner" by pressing the Right arrow. To use a static IP address and/or proxy configuration, enable these configurations first from the main menu.

For custom configuration: To configure a static IP, go to "Set up network" by pressing the Down arrow one time and then the Right arrow one time (see [Customize the network set up](#)). To enable a proxy, go to "Enable proxy" using the Up/Down arrows. When highlighted, press the Right arrow (see [Enable proxy configuration](#)). After making configuration settings, use the Up/Down arrows to navigate to "Personalize this scanner" and then press the Right arrow.

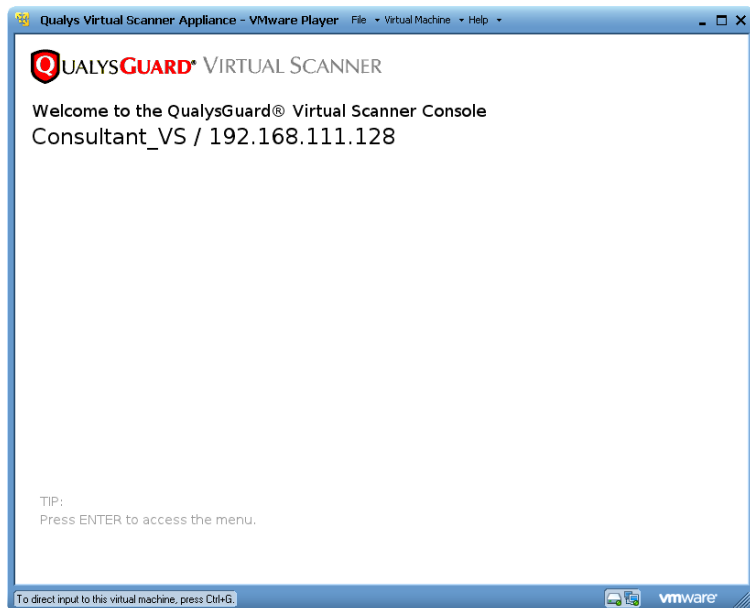


Help Tips: Refer to this section on each screen for help with navigation and making settings.

3) Enter a personalization code. You obtained a personalization code when the virtual scanner was provisioned. One activation code may be used to activate one virtual scanner. After entering the code activation starts and the service reports the progress. Activation may take a few minutes to complete.



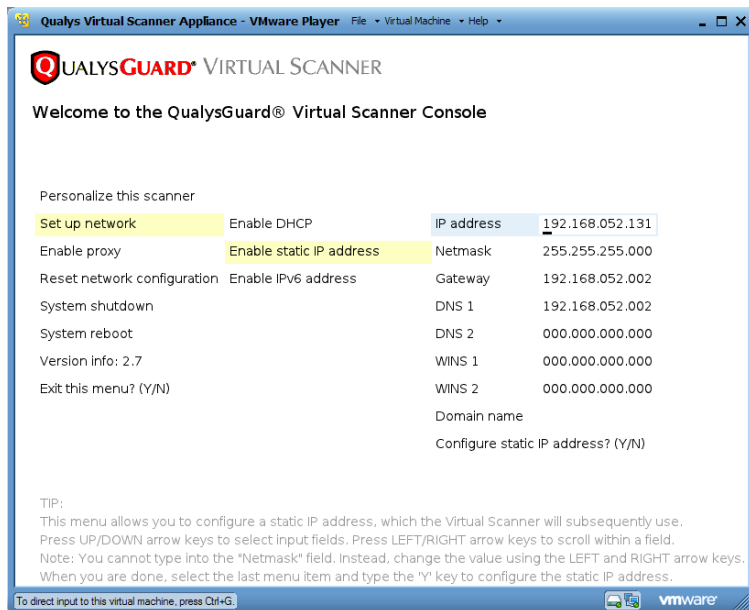
4) Wait until the activation completes. During activation, the virtual scanner attempts to make a connection to the QualysGuard platform using its current configuration (network and proxy settings). Upon success, the scanner's friendly name and IP address appear and the scanner is ready to be used for scanning. Press Enter to go to the main menu.



Customize the network set up

If you wish to enable a static IP address, go to the main menu (on the left) press the Down arrow to select “Set up network”. Then press the Right arrow one time, followed by the Down arrow one time to select “Enable static IP address”. Press the Right arrow to view the static IP settings.

How to enter settings: Press Up and Down arrows to select input fields. Press the Right and Left arrows to scroll within a field. When you are done, select the last item, in this case “Configure static IP address?” and type “Y” to configure the IP address (or type “N” to cancel and return to the main menu).

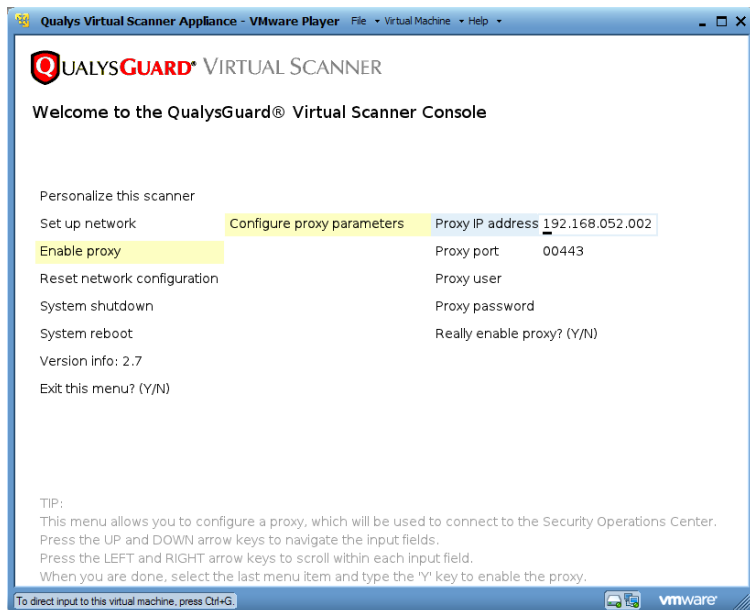


What happens next: After you type “Y” to configure the IP address the virtual scanner attempts to connect to the QualysGuard platform using its current configuration (network set up and proxy settings). Upon success, the friendly name and IP address for the scanner appear. If not, a network error appears and you need to troubleshoot the configuration. See [FAQs](#) for assistance.

Enable proxy configuration

If you wish to enable a proxy configuration, go to the main menu (on the left) and use the Up and Down arrows to select “Enable proxy”. Then press the Right arrow one time to select “Configure proxy parameters” and press the Right arrow another time to view the proxy settings.

How to enter settings: Press Up and Down arrows to select input fields. Press the Right and Left arrows to scroll within a field. When you are done, select the last item, in this case “Really enable proxy?” and type “Y” to enable the proxy configuration (or type “N” to cancel and return to the main menu).



What happens next: After you type “Y” to enable the proxy configuration the virtual scanner attempts to connect to the QualysGuard platform using its current configuration (network set up and proxy settings). Upon success, the friendly name and IP address for the scanner appear. If not, a network error appears and you need to troubleshoot the configuration. See [FAQs](#) for assistance.

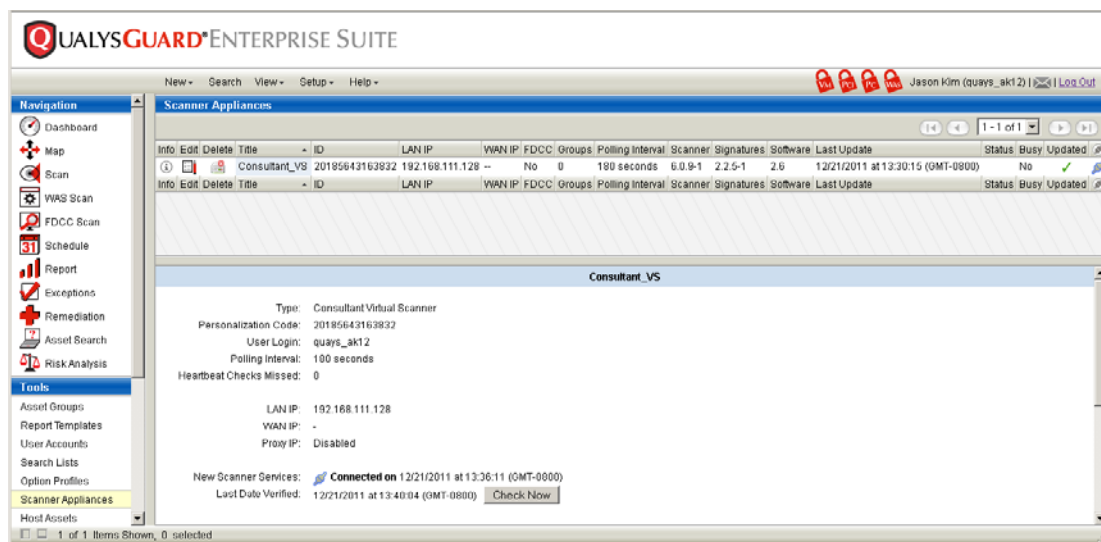
Check the Scanner Appliance Status in QualysGuard

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

1) Go to the appliances list. Log into your QualysGuard account. On the left menu go to Scanner Appliances, under Tools.

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 Consultant Virtual Scanner along with the personalization code used to activate the appliance.

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 (on the left menu go to Scanner Appliances, under Tools). Identify the virtual scanner you want to edit and click .



FAQs

How do I remove virtual scanners?

Once provisioned, virtual scanners appear in your scanner appliances list. Managers and Unit Managers can remove a virtual scanner from their subscription. To do this, using the original user interface, go to Scanner Appliances on the left menu, under Tools. Identify the virtual scanner you would like to delete and click  next to the scanner appliance title.

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.

Using the Virtual Scanner Console you can enable a proxy configuration for 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 performance issues:

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.