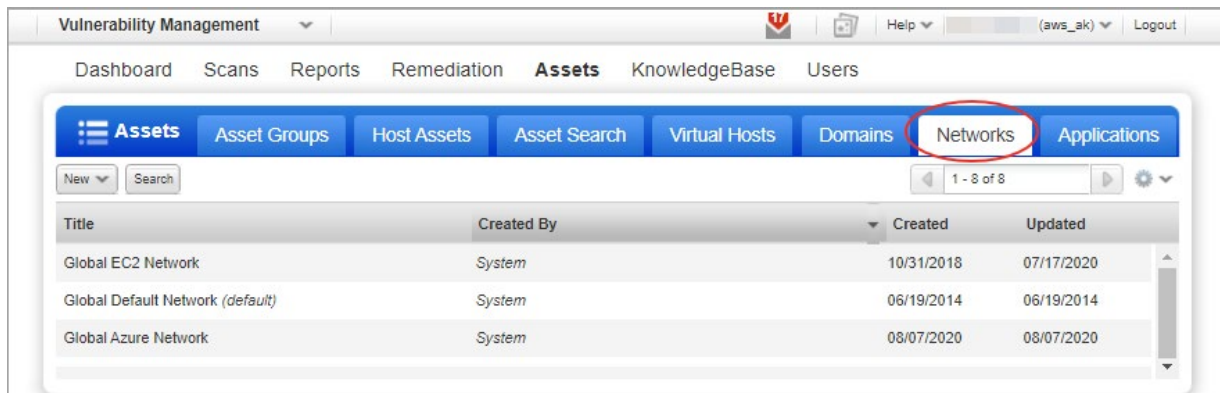


Network Support Quick Start

Customers can now manage overlapping IP ranges within a single Qualys subscription, giving you the ability to define discrete private networks to keep overlapping blocks isolated from each other. This is a common need that appears in many use cases including:

- M&A events
- Air gap networks
- Business continuity/disaster recovery
- Development/test environments
- IaaS environments
- “Cloned” small office environments

These different network zones can now be easily defined and separated within Qualys through the UI and API using custom networks. To take advantage of this, the administrator uses the new “Networks” tab under Assets, defines a new network, and assigns it a scanner appliance. Once defined, you can perform asset discovery, launch scans, run reports, and track mitigation on that network as a specific entity. Assigning scanners to networks resolves the issue of duplicate IP addresses occurring in different networks, but allows the administrator to maintain centralized management across the organization.



Tip - You'll see the Networks tab only when this feature is turned on for your subscription.

Good to Know

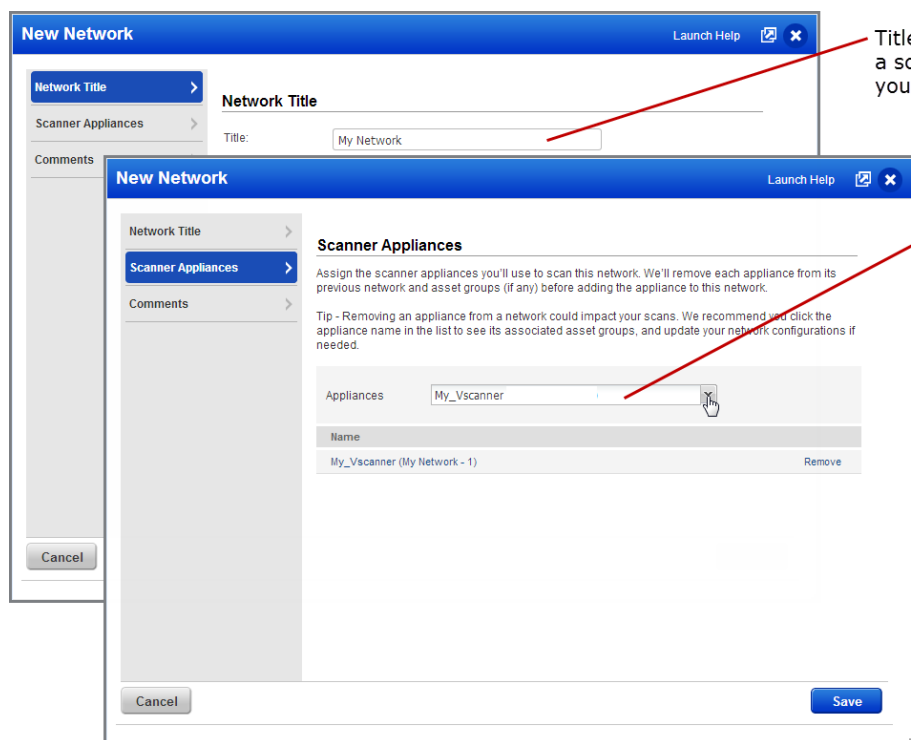
- You'll create custom networks to group one or more scanner appliances.
- The Global Default Network, provided by Qualys, is used to scan assets that do not belong to custom networks.
- The Global EC2 Network, provided by Qualys, is used for all the assets that are detected by the Amazon Web Services (AWS) EC2 connector and that do not belong to custom networks.
- The Global Azure Network, provided by Qualys, is used for all the assets that are detected by the Microsoft Azure connector and that do not belong to custom networks.

- What about my configurations? Initially your existing configurations (asset groups, schedules, appliances) will be assigned to the Global Default Network and schedules will continue to run.

Note you can change the network for an appliance and schedule but not for an asset group.

Create a custom network

Just go to Assets > Networks and select New > Network (Manager only). Then assign one or more scanner appliances. These appliances will be used to scan the IPs/ranges associated with the network.



The screenshot displays the 'New Network' configuration window. The top section is titled 'New Network' and includes a 'Network Title' field with the value 'My Network'. Below this is the 'Scanner Appliances' section, which contains a list of appliances. One appliance, 'My_Vscanner', is selected and added to a table. The table has columns for 'Name' and 'Remove'. The name 'My_Vscanner (My Network - 1)' is listed, with a 'Remove' button next to it. A 'Save' button is located at the bottom right of the window, and a 'Cancel' button is at the bottom left. A red arrow points from the 'Title' field to the text 'Title - When you launch a scan, you'll select your network.' Another red arrow points from the 'Appliances' list to the text 'Appliances - Add as many as you like. Each appliance can be in only one network.'

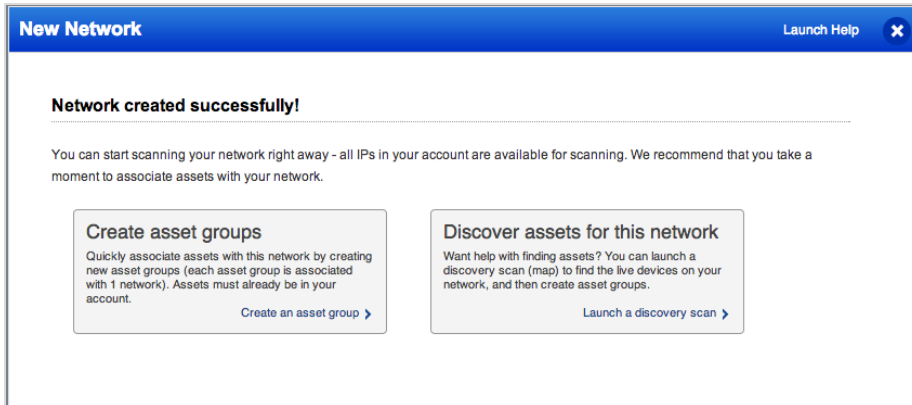
Title - When you launch a scan, you'll select your network.

Appliances - Add as many as you like. Each appliance can be in only one network.

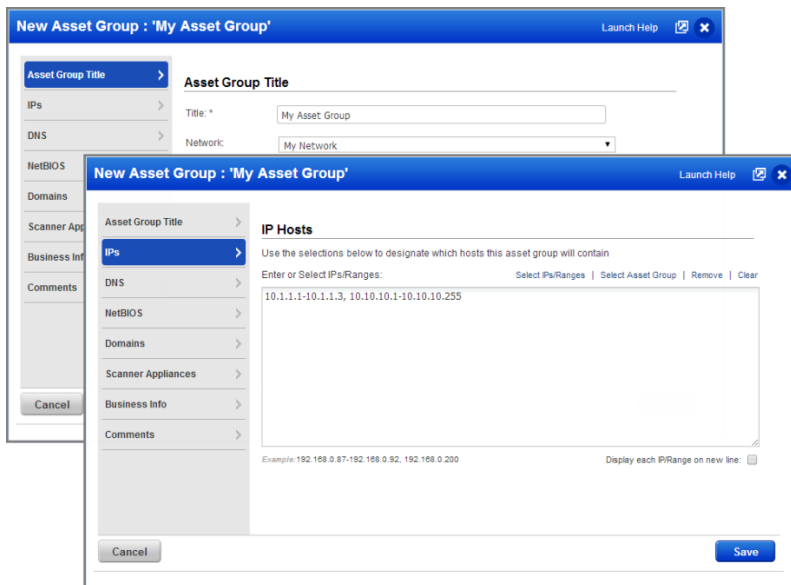
When you're done, click Save. That's it – your custom network is created and you can start scanning it.

Organize your assets by network (recommended)

We recommend you take a moment to discover assets on your new network and organize them into asset groups. This will help you to select them as targets for scans and reports.



You'll create an asset group by 1) assigning it to a network, and 2) selecting IPs/domains.



Each asset group can be in only one network. Once you save an asset group, you can't change its network association.

The IPs/domains in your account can still be assigned to multiple asset groups.

Scan your custom network

You'll start a scan using the same familiar scan workflows. Select your custom network and All Scanners in Network (or an appliance name in your custom network).

Launch Vulnerability Scan Turn help tips: On | Off Launch Help

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:

Option Profile: * [Select](#)

Processing Priority:

Network: [View](#)

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

Assets Tags

Asset Groups: [Select](#)

IPs/Ranges: [Select](#)

Example: fe80:012e:21f8:887e:ff1, fe80:012e:21f8:887e:ff2

Exclude IPs/Ranges: [Select](#)

Example: fe80:012e:21f8:887e:ff1, fe80:012e:21f8:887e:ff2

FQDN(s):

Example: Separate entries using commas. www.abc.com, www.xyz.com

Temporarily add agent addresses
Select this option to add the IP addresses of any agents in your target when those IPs are not already in your subscription. They'll be added for this scan only.

Notification

Send notification when this scan is finished

Want to scan hosts outside of your custom network? No problem, just pick the network called Global Default Network and we'll scan hosts not associated with any custom networks.

Good to Know

Your host based vulnerability findings will be stored in your account - per network and per host.

Report on your network

Your report target can include a mix of asset groups, IP/ranges and asset tags - for one network or multiple networks.

How do I report on IPs in one network only?

There's a couple ways to do this.

Option 1 - Enter the IPs/ranges you want to report on and select a network name from the drop-down. Your report will be filtered to the selected network only (this only applies to the IPs/Ranges selection).

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: * [Select](#)

Report Format: *

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Option 2 - Select only asset groups that belong to the network you're interested in.

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: * [Select](#)

Report Format: *

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Select Asset Groups

Search

1 - 4 of 4

Title	IPs	User	Network
<input type="checkbox"/> Asset Group - 1	10.10.10.2-10.10.10.255, 10.10.24.2-10.10.24...	Keyser	Global Default Network
<input checked="" type="checkbox"/> My Asset Group	10.10.26.2-10.10.26.255	Keyser	My Network

Can I create a report including IPs on different networks?

Yes this is easy to do. Enter the IPs/ranges you want to report on and select the "All" network option.

What about vulnerability details?

We'll display the network name next to each IP address in your report for quick identification.

This report is sorted by host. Is your report sorted by vulnerability? If yes, you'll see vulnerabilities and the IPs for each vulnerability along with their networks.

Sample report

We'll show you the network name next to each IP address in your reports.

Patch Report

Report Summary
 Company: Quays
 Created on: 04/14/2014

Total Patches	Hosts Requiring Patches	Vulnerabilities Addressed
27	4	42

[View Report Targets...](#)

HOSTS							PATCHES required on 192.168.1.82 (18)				
IP	Network	DNS Name	NetBIOS	OS	OS CPE	Patches	Vendor ID	Severity	Title	Published	Val...
192.168...	Global Default Network		NEWMINI	MacOS X 13.1.0	cpe:/o:apple:mac_os_x:13.1.0	18	APSB14-09	4	Adobe Flash Player Multiple Vuln...	6 days ago	6
192.168...	Global Default Network	vm-xp	VM-XP	Windows XP Service Pack 0-1		4	RHSA-20...	4	CUPS UDP Packet Remote Denial...	9 years ago	1
192.168...	Global Default Network			IBM Tape Library		3	gcmrekey...	4	OpenSSH AES-GCM Cipher Remo...	157 days ago	1
192.168...	Global Default Network			VxWorks Based Device		2	APSB12-19	5	Adobe Flash Player and AIR Mult...	1 year ago	1
							APSB12-22	4	Adobe Flash Player and AIR Mult...	1 year ago	1
							APSB12-24	4	Adobe Flash Player and AIR Mult...	1 year ago	1
							APSB12-27	4	Adobe Flash Player and AIR Mult...	1 year ago	1
							APSB13-01	4	Adobe Flash Player and AIR Rem...	1 year ago	1
							APSB13-04	5	Adobe Flash Player Multiple Cod...	1 year ago	1

Where else can I see scan findings?

Go to Assets > Host Assets. You'll see that all IPs in your account are listed for every network you have. Expand a network to view the IP addresses in that network. Click any host to view the host information with the current findings (latest host scan data).

Vulnerability Management

Dashboard Scans Reports Remediation **Assets** KnowledgeBase Users

Assets < Asset Groups Host Assets Asset Search Virtual Hosts Domains Networks Application >

Network: nw2_BU2 Hosts: 10.10.25.105-10.10.25.110

Info	Tracking	IP	DNS	NetBIOS	OS	
<input type="checkbox"/>	<input type="checkbox"/>	IP	10.10.25.105	vsener-2005-u	VSERVER-2005-U	Windows XP
<input type="checkbox"/>	<input type="checkbox"/>	View host information	105			
<input type="checkbox"/>	<input type="checkbox"/>	IP	10.10.25.107			
<input type="checkbox"/>	<input type="checkbox"/>	IP	10.10.25.108			
<input type="checkbox"/>	<input type="checkbox"/>	IP	10.10.25.109			
<input type="checkbox"/>	<input type="checkbox"/>	IP	10.10.25.110			Windows 2003

If the same IP address is scanned in multiple networks, you'll see a separate set of scan data for each network.