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.
- 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.

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.

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).

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).

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

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).

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