Vulnerability Management
Lab Tutorial Supplement

Please be advised that all labs and tests are to be conducted within The parameters outlined within the text. The use of other domains or IP addresses is prohibited.

Contents

Account & Application Setup

VM and VMDR will provide you with the tools and features needed to successfully manage and mitigate vulnerabilities. To assess host assets for vulnerabilities, you must first add them to your Qualys subscription.

You can accomplish this task by deploying Qualys Cloud Agents or by adding host IPs to the "Address Management" or "Host Assets" tabs. The "Host Assets" tab is replaced by the "Address Management" tab, when Asset Group Management Service (AGMS) is enabled.

IPs that you add to the "Address Management" or "Host Assets" tabs are "Scannable" and may be targeted in successive vulnerability scans.

Navigate to the following URL to view the "Add Host Assets" tutorial:

LAB 1 - https://ior.ad/7ecA

Tracking Methods

When adding host assets to your account, three basic methods are available for tracking their vulnerability findings:

- Host IP Address
- Host DNS Name
- Host NetBIOS Name

IP Tracked Hosts

The "IP Address" tracking method works best when used with hosts that have "static" IP addresses. If host IPs change frequently, it is typically better to use DNS or NetBIOS tracking.

DNS Tracked Hosts

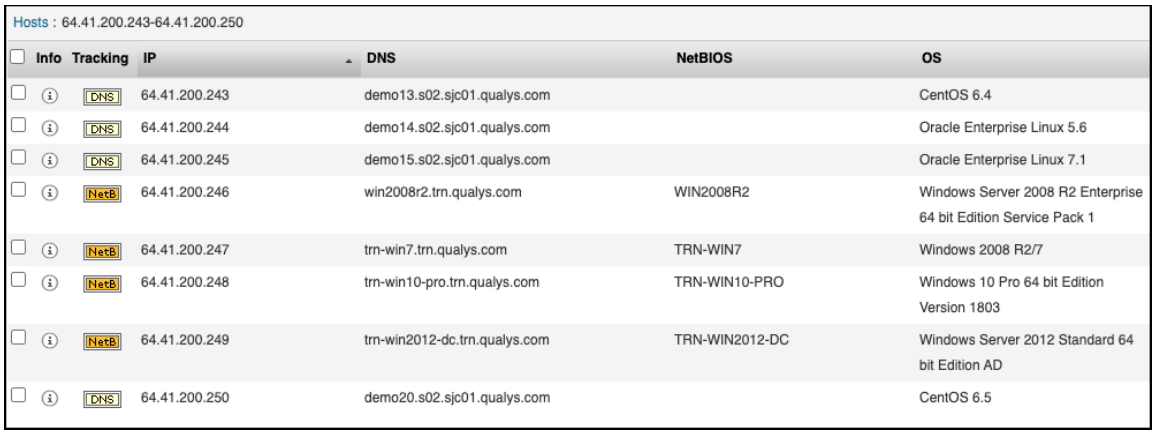
The Linux-based hosts in the Qualys Training Lab are configured to track vulnerabilities by host DNS name.

NetBIOS Tracked Hosts

The Windows-based hosts in the Qualys Training Lab are configured to track vulnerabilities by host NetBIOS name.

A fourth tracking method, the Qualys Host ID, is used by default, for all "Cloud Agent" host assets. The Qualys Host ID is universally unique (i.e., UUID) and is only available for "scannable" host assets, when the "Agentless Tracking" feature is enabled.

A good tracking method is one that is both unique and persistent, for each host.



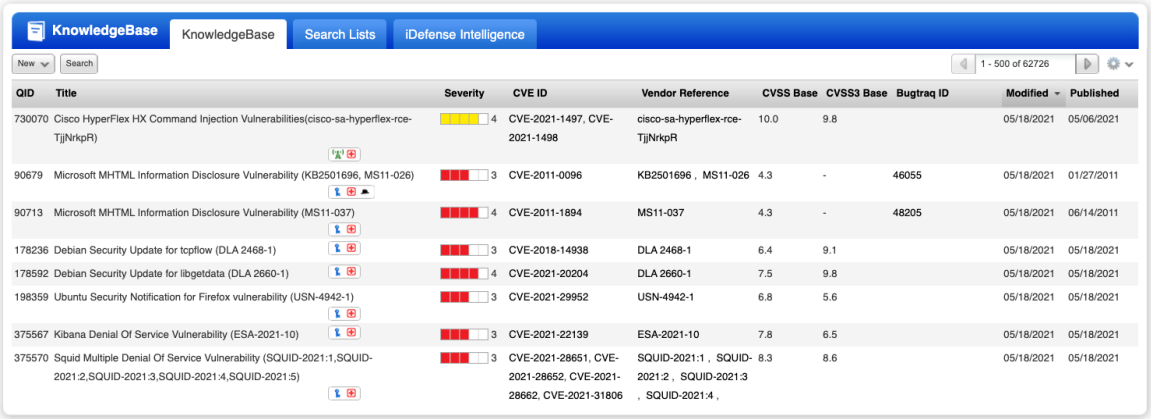
Hosts : 64.41.200.243-64.41.200.250

Info	Tracking	IP	DNS	NetBIOS	OS
	DNS	64.41.200.243	demo13.s02.sjc01.qualys.com		CentOS 6.4
	DNS	64.41.200.244	demo14.s02.sjc01.qualys.com		Oracle Enterprise Linux 5.6
	DNS	64.41.200.245	demo15.s02.sjc01.qualys.com		Oracle Enterprise Linux 7.1
	NetB	64.41.200.246	win2008r2.trn.qualys.com	WIN2008R2	Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1
	NetB	64.41.200.247	trn-win7.trn.qualys.com	TRN-WIN7	Windows 2008 R2/7
	NetB	64.41.200.248	trn-win10-pro.trn.qualys.com	TRN-WIN10-PRO	Windows 10 Pro 64 bit Edition Version 1803
	NetB	64.41.200.249	trn-win2012-dc.trn.qualys.com	TRN-WIN2012-DC	Windows Server 2012 Standard 64 bit Edition AD
	DNS	64.41.200.250	demo20.s02.sjc01.qualys.com		CentOS 6.5

The illustration above depicts the Windows and Linux host targets in the Qualys Training Lab environment (64.41.200.243 – 64.41.200.250). All lab targets in this course have public IP addresses and will be scanned using Qualys' pool of Internet-based scanners.

KnowledgeBase & Search Lists

The Qualys KnowledgeBase provides the most current and comprehensive vulnerability and threat intelligence information.



QID	Title	Severity	CVE ID	Vendor Reference	CVSS Base	CVSS3 Base	Bugtraq ID	Modified	Published
730070	Cisco HyperFlex HX Command Injection Vulnerabilities(cisco-sa-hyperflex-rce-TjjNrkpR)	4	CVE-2021-1497, CVE-2021-1498	cisco-sa-hyperflex-rce-TjjNrkpR	10.0	9.8		05/18/2021	05/06/2021
90679	Microsoft MHTML Information Disclosure Vulnerability (KB2501696, MS11-026)	3	CVE-2011-0096	KB2501696 , MS11-026	4.3	-	46055	05/18/2021	01/27/2011
90713	Microsoft MHTML Information Disclosure Vulnerability (MS11-037)	4	CVE-2011-1894	MS11-037	4.3	-	48205	05/18/2021	06/14/2011
178236	Debian Security Update for tcpflow (DLA 2468-1)	3	CVE-2018-14938	DLA 2468-1	6.4	9.1		05/18/2021	05/18/2021
178592	Debian Security Update for libgetdata (DLA 2660-1)	4	CVE-2021-20204	DLA 2660-1	7.5	9.8		05/18/2021	05/18/2021
198359	Ubuntu Security Notification for Firefox vulnerability (USN-4942-1)	3	CVE-2021-29952	USN-4942-1	6.8	5.6		05/18/2021	05/18/2021
375567	Kibana Denial Of Service Vulnerability (ESA-2021-10)	3	CVE-2021-22139	ESA-2021-10	7.8	6.5		05/18/2021	05/18/2021
375570	Squid Multiple Denial Of Service Vulnerability (SQUID-2021:1,SQUID-2021:2,SQUID-2021:3,SQUID-2021:4,SQUID-2021:5)	3	CVE-2021-28651, CVE-2021-28652, CVE-2021-28662, CVE-2021-31806	SQUID-2021:1 , SQUID-2021:2 , SQUID-2021:3 , SQUID-2021:4 ,	8.3	8.6		05/18/2021	05/18/2021

Each vulnerability has a unique Qualys ID (QID). CVE and Bugtraq IDs are also provided. Click any of the column headers to sort the list of QIDs. Use the "Quick Actions" menu of any QID to view vulnerability details, including threat, impact, and solution information.

Click the "Search" button (in the upper-left corner) to select from dozens of criteria, to locate specific types of vulnerabilities.

Navigate to the following URL to view the "Vulnerability KnowledgeBase" tutorial:

PLAY LAB 2 - https://ior.ad/7ecB

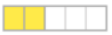
Color Codes & Severity Levels

Color codes allow you to easily distinguish between confirmed (red) and potential (yellow) vulnerabilities.

	Confirmed Vulnerability	Security weakness verified by an "active test"
	Potential Vulnerability	Security weakness requiring manual verification
	Information Gathered	Configuration Data

Qualys scanners and agents also collect configuration data, which is color coded blue.

Severity levels indicate the potential impact of a compromised or exploited vulnerability.

Confirmed	Potential	Severity Level	Description
		Minimal (1)	Intruders can collect information about the host via open ports or services, which can lead to the disclosure of other vulnerabilities.
		Medium (2)	Intruders can collect sensitive information from the host, such as software versions installed, which can reveal known vulnerabilities.
		Serious (3)	Intruders can gain access to security settings on the host, which could lead to: access to files and disclosure of file contents, directory browsing, denial of service attacks, and unauthorized use of services.
		Critical (4)	Intruders can potentially gain control of the host, or collect highly sensitive information including: read access to files, potential backdoors, or a listing of all user accounts on the host.
		Urgent (5)	Intruders can easily gain control of the host, which can lead to the compromise of your entire network. Vulnerabilities include: read and write access to files, remote execution of commands, and backdoors.

Severity level 5 is the most urgent, while level 1 is the least urgent. Common Vulnerability Scoring System (CVSS) scores are also provided.

Search List

A “Search List” allows you to create a custom list of QIDs from the Qualys KnowledgeBase.

A “dynamic” Search List is automatically updated by the Qualys service when new QIDs are added to the Qualys KnowledgeBase. A “static” Search List does not receive automatic updates, but can be updated manually.

With a static or dynamic search list you can:

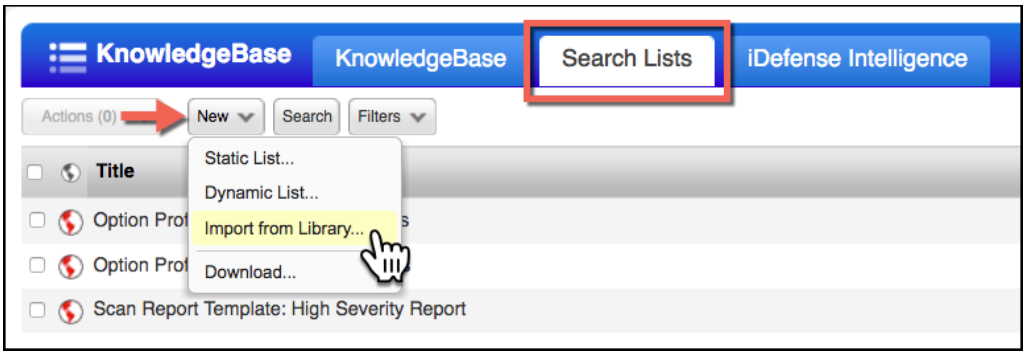
- Build a report to focus on specific vulnerabilities.
- Launch a scan that targets a specific type or group of vulnerabilities.
- Build a Remediation Policy to automatically assign or ignore vulnerabilities.

Navigate to the following URL to view the “Knowledge Base Search Lists” tutorial:

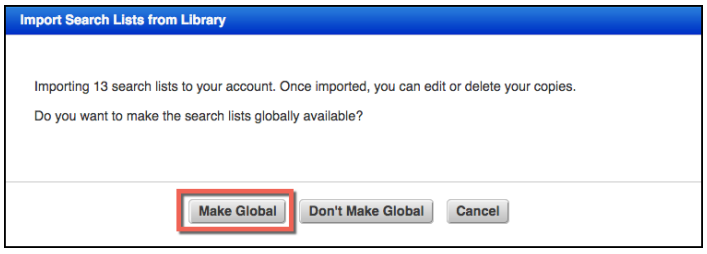
PLAY LAB 3 - https://ior.ad/7ecF

Search List Library

Qualys has a library of some very useful Search Lists.



You’ll find a “Search Lists” tab under the Scans, Reports, and KnowledgeBase sections of VM and VMDR. All three tabs perform the same function.



The “Global” option allows you to control the visibility of the objects you create or import. If you make an object “Global” it will be visible to other users (Scanners, Readers, etc…) within your Qualys subscription.

Organize & Manage Assets

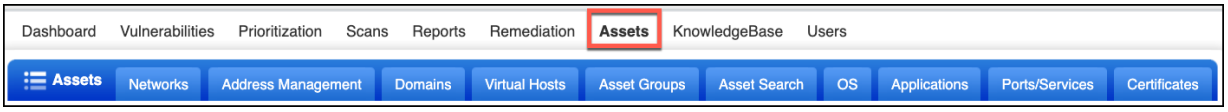
Qualys VM, VMDR, AssetView, and Asset Inventory provide different tools and options for managing the assets within your account.

Asset Search

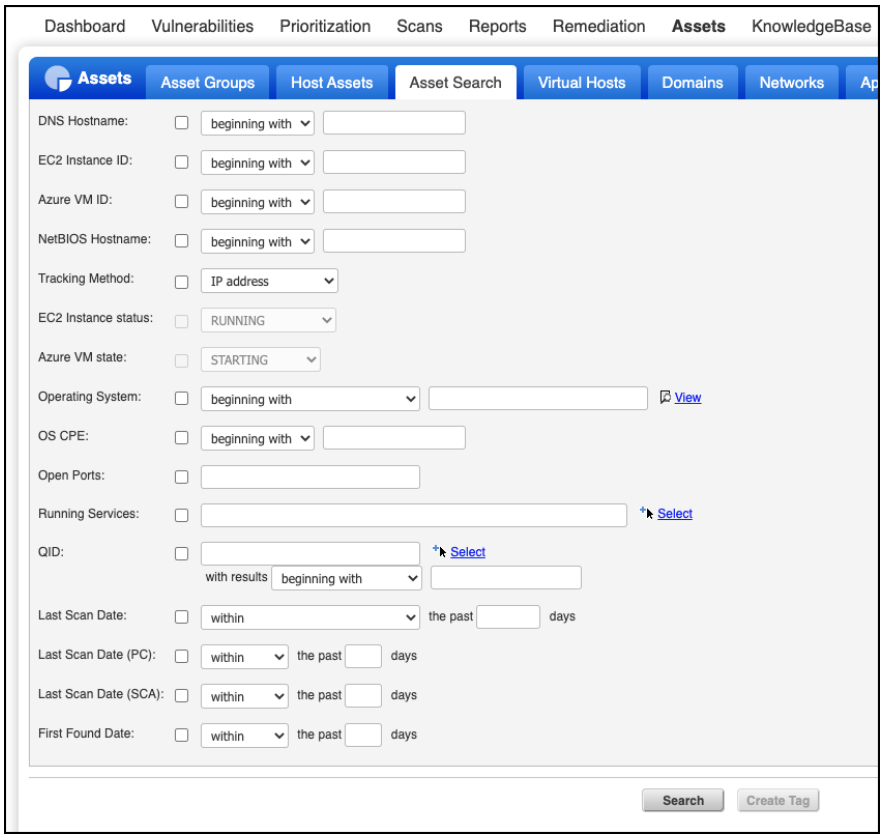
The "Assets" section of the Qualys Vulnerability Management application provides an excellent source of host asset data and information. Here you will find multiple tabs that will allow you to monitor and manage your asset inventory.

Navigate to the following URL to view the "Search for Assets" tutorial:

PLAY LAB 4 - https://ior.ad/7esx

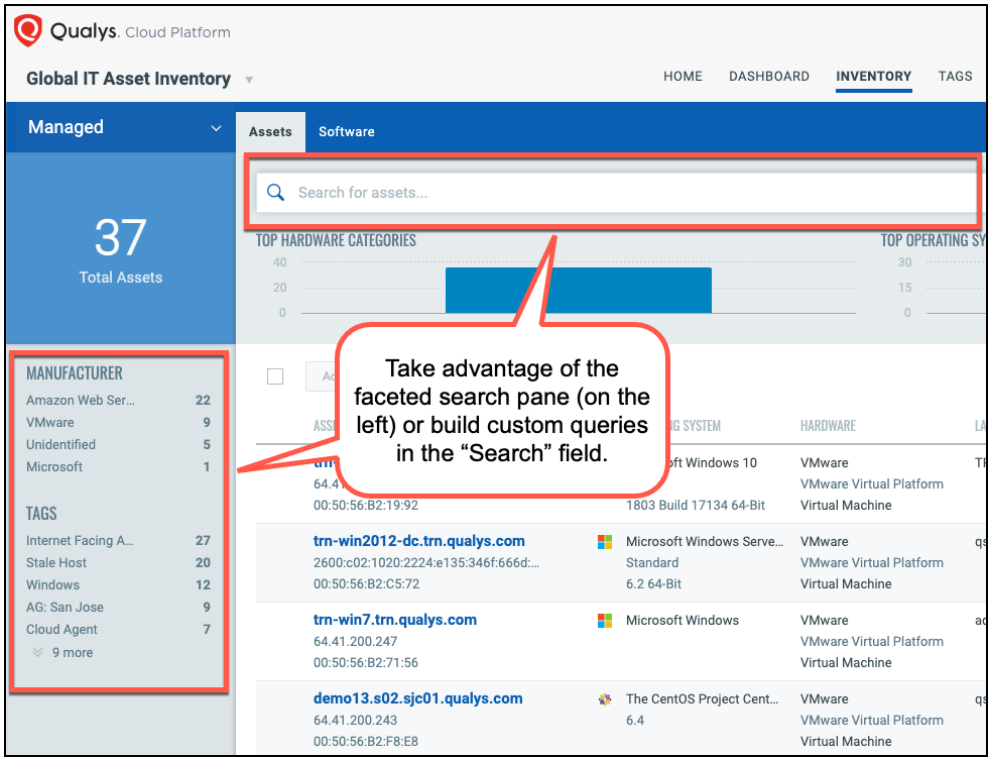


Navigate to the "Assets" section and the "Asset Search" tab, to utilize VM and VMDR's search capabilities.

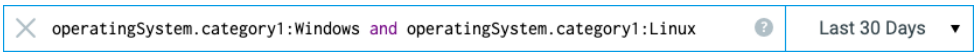


Use the various criteria and options to perform a search or even create an Asset Tag.

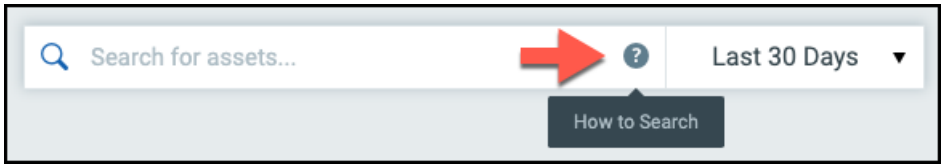
Qualys Global IT Asset Inventory provides useful tools to query your asset data.



Perform searches with a click of your mouse, using the faceted search pane or build custom queries using the "Search" field.



Combine query tokens, values, and Boolean operators to create more complex search queries.



Click the "Help" icon (at the right-side of the "Search" field) for information, syntax, and examples on how to search.

Asset Groups

Asset Groups were the first asset management tool provided by Qualys VM. Simply create an Asset Group, give it an appropriate name, and manually add host IP addresses. Alternatively, hosts can be added to Asset Groups by their DNS or NetBIOS names. Here are some important characteristics of an Asset Group:

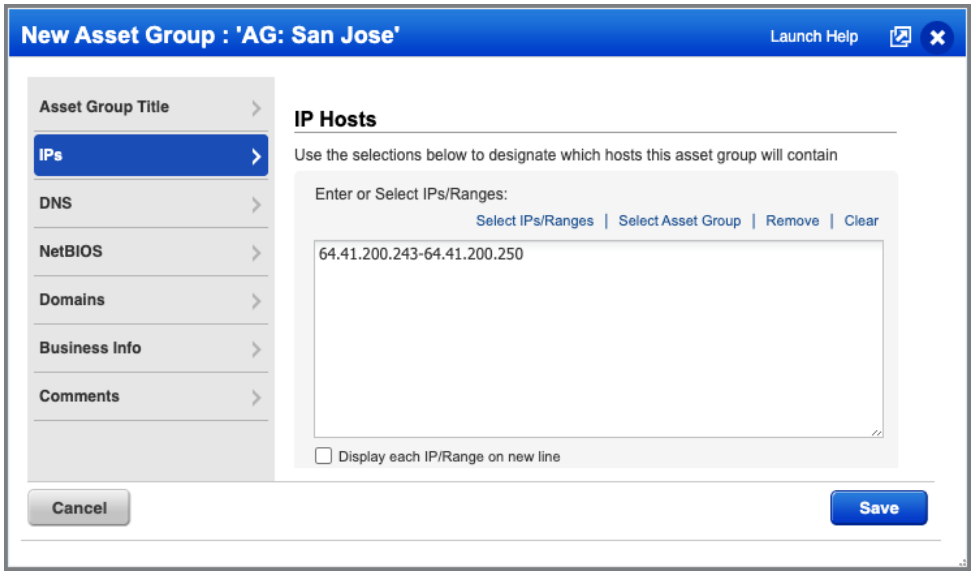
- Used to assign access privileges to user accounts.
- Contains a "Business Impact" setting that is used to calculate Business Risk.
- Can be used as a target for mapping, scanning, reporting, and remediation.
- A single host can be a member of multiple Asset Groups.
- Nesting one Asset Group inside another is not supported. *
- Created and updated manually. *

* The last two items in this list, will be addressed using Asset Tags. Asset Tags are updated automatically and dynamically. Asset Tag "nesting" is the recommended approach for designing functional Asset Tag "hierarchies" (parent/child relationships).

Navigate to the following URL to view the "San Jose Asset Group" tutorial:

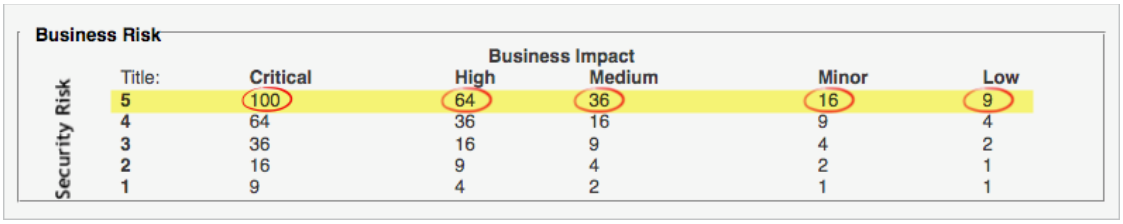
LAB 5 - https://ior.ad/7eiB

Qualys recommends adding the "AG:" prefix to Asset Group names. Other naming conventions that help to distinguish Asset Group members (such as location, function, device type, etc…) will make it easier for other Qualys users in your account to identify and use Asset Groups, effectively.



IP addresses are often associated or directly linked to some domain name (s). You may associate domain names with the IP addresses in your Asset Groups.

Business risk is the product of an Asset Group's "Average Security Risk" and its "Business Impact" setting. Once an Asset Group's Average Security Risk is calculated, its associated Business Risk can then be determined.



Business Risk

Security Risk	Business Impact					
Title:	Critical	High	Medium	Minor	Low
5	100	64	36	16	9
4	64	36	16	9	4
3	36	16	9	4	2
2	16	9	4	2	1
1	9	4	2	1	1

A “Critical” Asset Group will receive a higher Business Risk score than a “High” or “Medium” Asset Group that has the same security risk average. Asset Groups with a “Minor” or “Low” impact, will receive even lower Business Risk scores, helping you to prioritize patching and remediation tasks for your most important assets. By default, Asset Groups are created with “Business Impact” set to High.

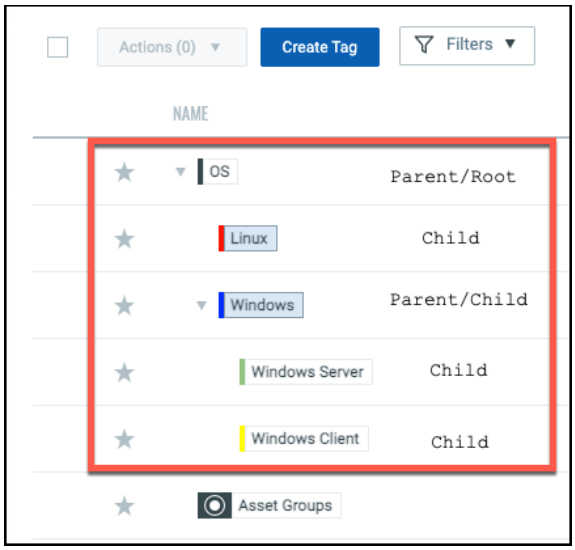
Asset Tags

Asset Tags provide a flexible, scalable, and dynamic solution to help you label and identify hosts. Asset tags are continuously updated, when new data and information is provided by Qualys Sensors, including Scanner Appliances and Cloud Agents.

Asset Inventory is a core component of the Qualys Cloud Platform and it provides a centralized location for creating and managing Asset Tags.

Create Operating System Hierarchy

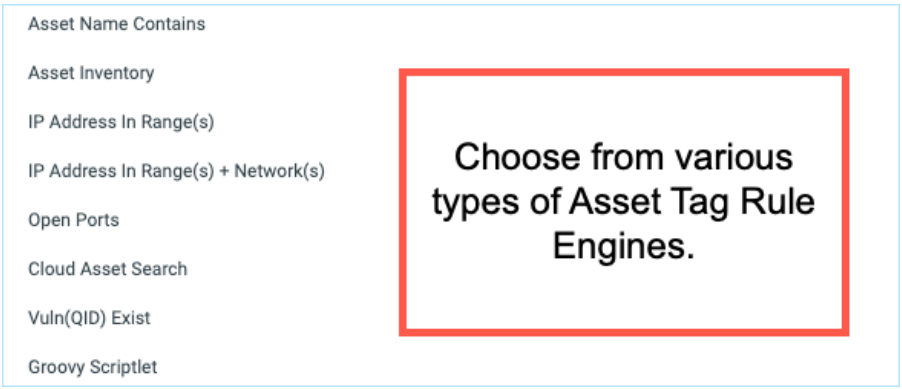
Asset Tags are organized into hierarchical structures or parent/child relationships. Some tags serve both a Parent and Child role.



Many tag hierarchies begin with a static “parent” that serves as a “placeholder” for its dynamic “child” tags. Tags located at higher levels of the hierarchy reflect a broader scope of host assets, while tags at lower levels of each hierarchy represent a more finite set of assets. A single host asset can have multiple tags, simultaneously.

Navigate to the following URL to view the “OS Asset Tag Hierarchy” tutorial:

PLAY LAB 6 - https://ior.ad/7emE

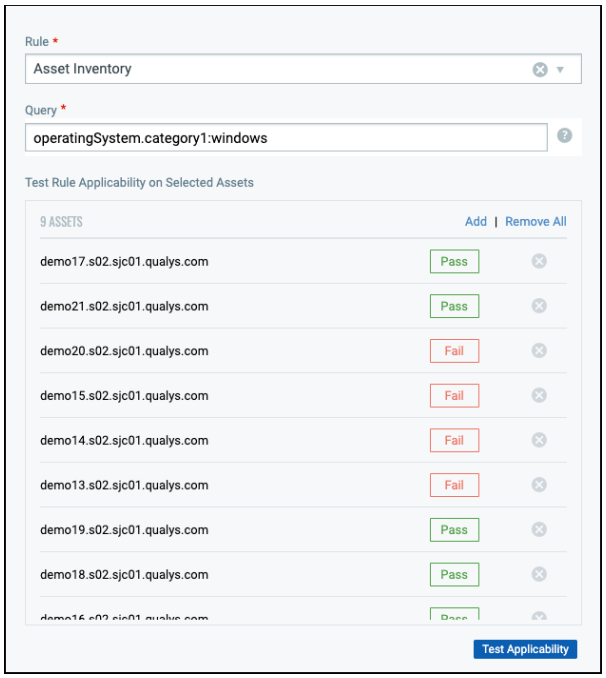


Dynamic Asset Tags are created using various types of Asset Tag Rule Engines. These tags are automatically updated as new information is received from Qualys Sensors.

Windows Tag

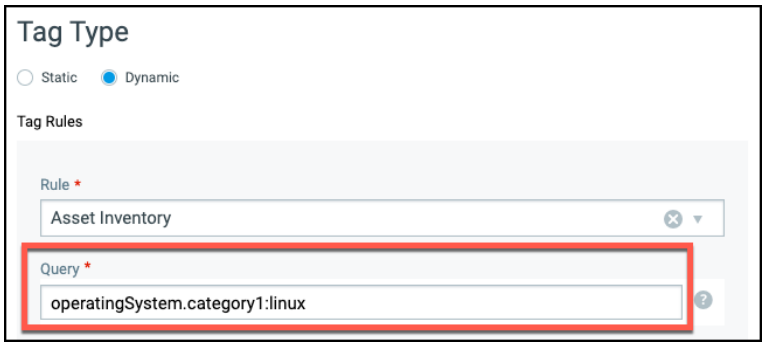
The “Asset Inventory” rule engine and the “operatingSystem query token provide a convenient way to label host by their OS.

When testing your queries, hosts that meet the query conditions(s) will Pass, while all other hosts will Fail.

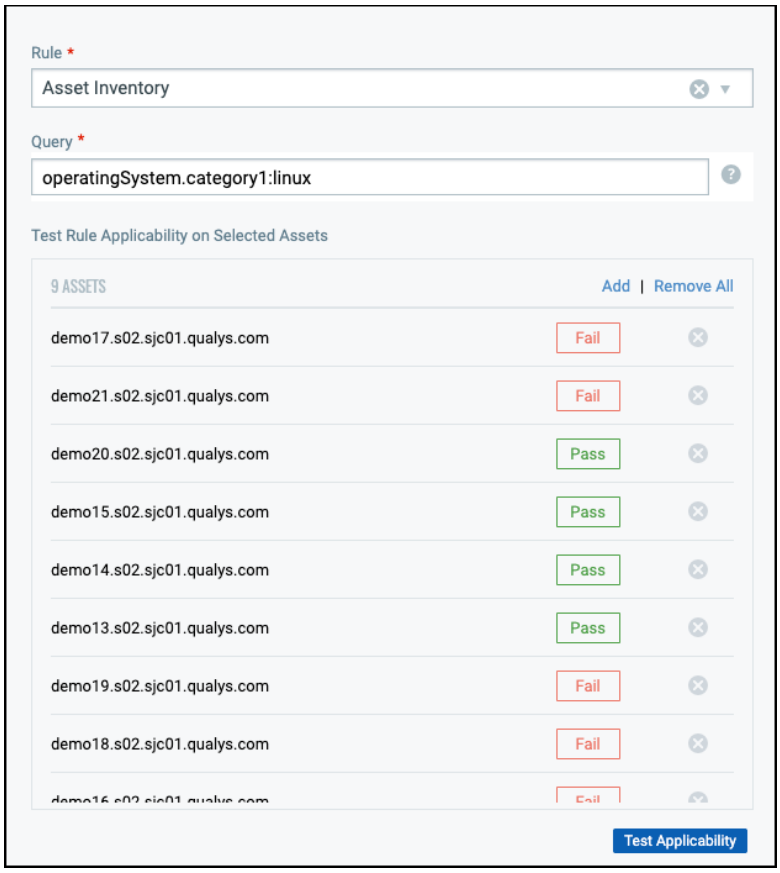


Linux Tag

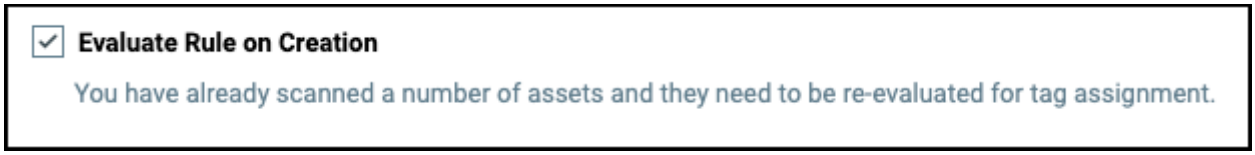
Linux hosts are easily tagged using the “Asset Inventory” rule engine and “operatingSystem” query token.



Now, all Linux host assets produce a Pass, while other hosts Fail.



Using the "Evaluate Rule on Creation option (while building or editing a tag) will add the tag to host that have already been scanned.



Vulnerability Assessment

Vulnerability assessments are performed within Qualys VM and VMDR, using data collected from Qualys Scanner Appliances and Qualys Cloud Agents.

The exercise steps in this lab are designed to collect assessment data, using the Qualys External Scanner Pool. Any user with scanning privileges has access to the Qualys pool of External Scanners.

Best Practice - Before you start scanning with Qualys, always be sure to get approval to scan IP addresses and/or web applications. It is your responsibility to obtain this approval.

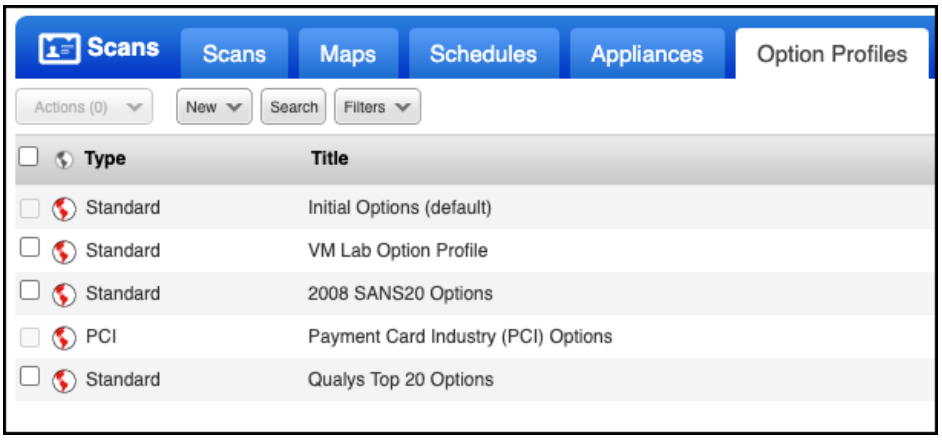
Option Profile

Every scan must include an Option Profile that specifies your preferred scanning options. In this tutorial you'll create an option profile with the following settings:

- Standard TCP and UDP Port Numbers
- Normal Overall Performance (balances scan performance with bandwidth usage)
- Complete Vulnerability Detection
- Windows and Unix Authentication

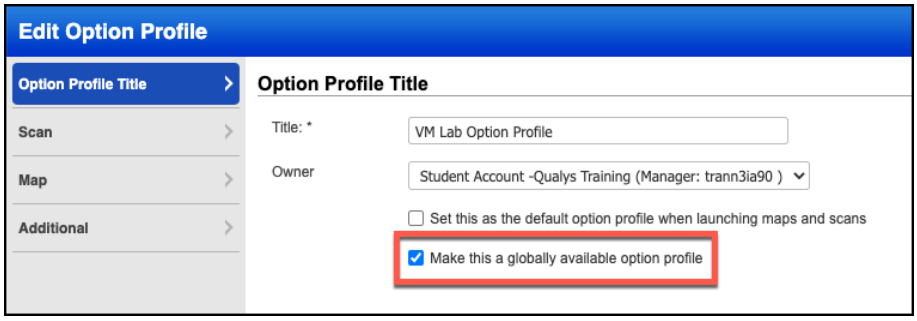
Navigate to the following URL to view the "Scanning Options" tutorial:

PLAY LAB 7 - https://ior.ad/7edH



Qualys VM and VMDR provide many "out-of-box" Option Profiles that are ready to use. Create custom profiles to meet your specific scanning objectives.

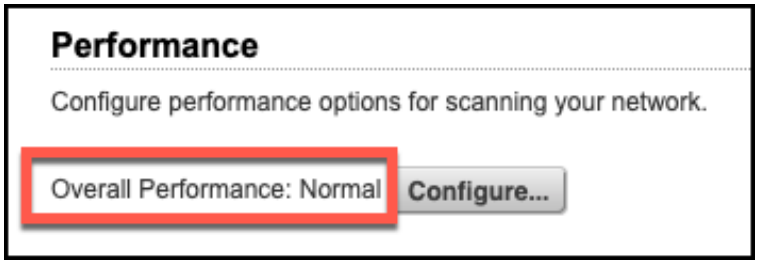
Make an Option Profile “global” to allow other Qualys users to see and use it.



The “Standard Scan” port setting contains the most commonly used port numbers (about 1,900) found in a typical network environment.

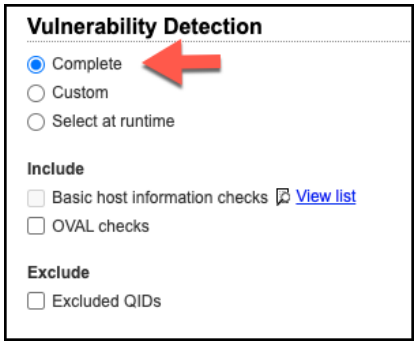
Click the “View list” link to see the specific port numbers included.

The preset configuration options for scan performance include High, Normal, and Low. A “Custom” setting is also available and will allow you to adjust individual performance settings and options.



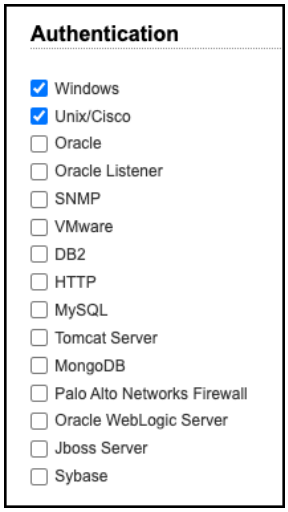
The “Normal” options provides a good balance between scan performance and bandwidth usage.

Qualys recommends using the “Complete” Vulnerability Detection option whenever possible.



This will provide the best possible vulnerability detection findings.

As a best practice, perform scans in "authenticated" mode, to get the most thorough and accurate results.



The lab targets in our training lab use both Windows and Unix authentication.

Authentication Records

Performing a "trusted" scan requires one or more authentication records. Alternatively, a Qualys Scanner Appliance can use authentication credentials collect from multiple types of authentication vaults

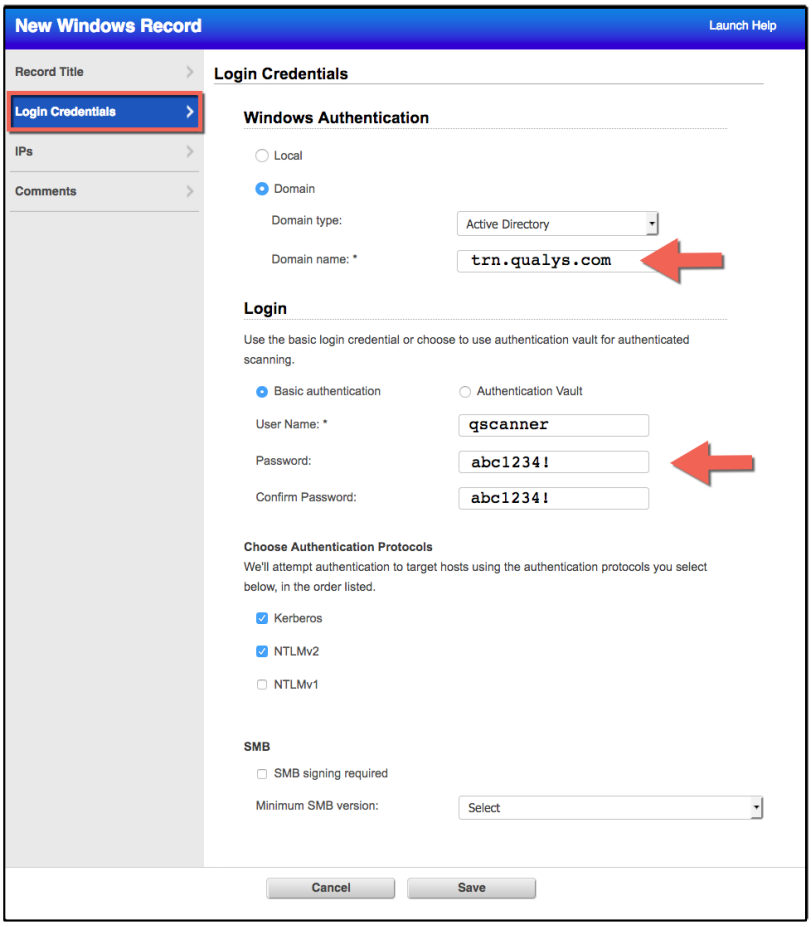
In this exercise, you'll create authentication records for the Window and Linux hosts in our training lab environment.

Navigate to the following URL to view the "Windows & Linux Authentication Records" tutorial:

LAB 8 - https://ior.ad/7ecH

Windows Authentication Record

Windows authentication records can be configured for both "Local" and "Domain" user accounts

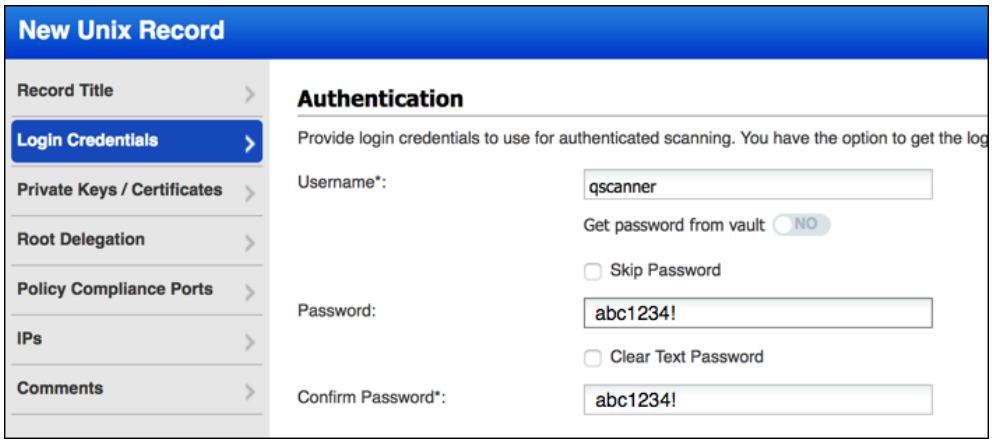


The "qscanner" user account is a member of the Domain Admins user group within the "trn.qualys.com" domain. At least on authentication protocol is required.

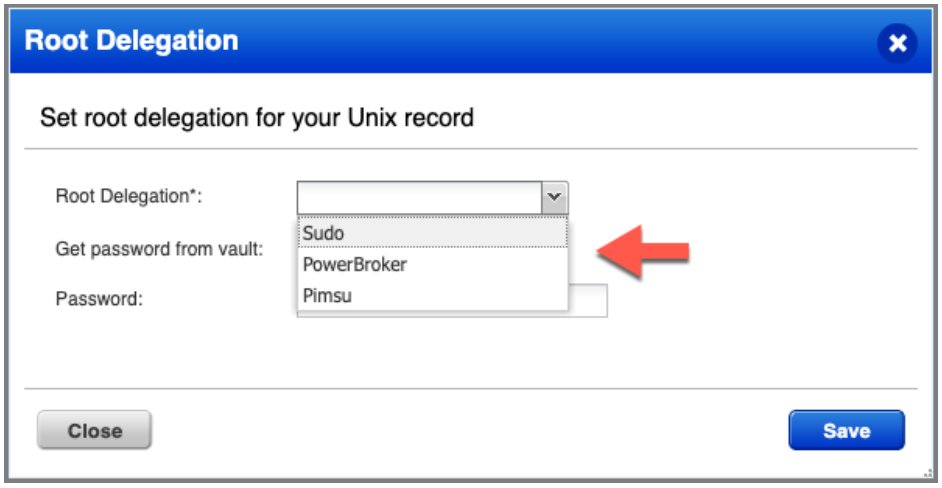
IP addresses are not required for Active Directory authentication records. This information will be collected at scan-time, from the Windows Domain service.

Unix Authentication Record

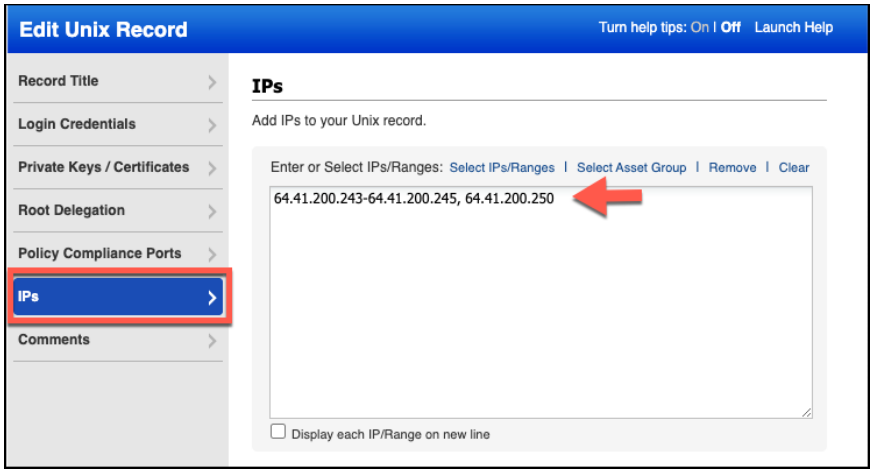
Unix authentications records can be created with a standard user account (avoid using the 'root' account).



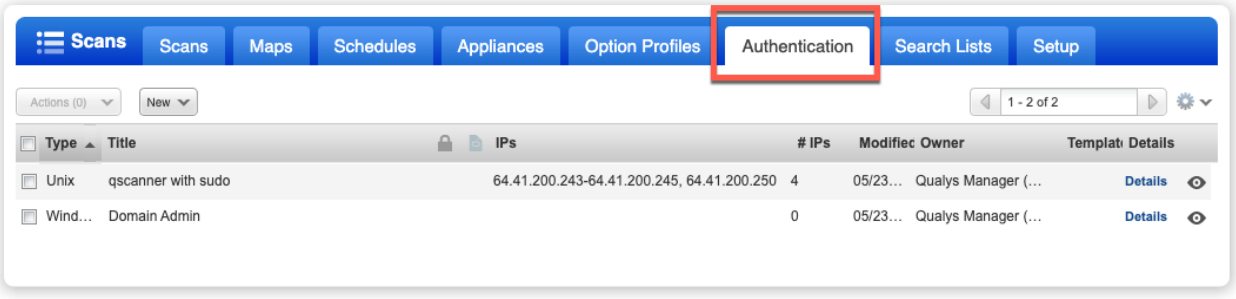
Root Delegation can then be used to provide elevated privileges to the scanning user account, via Sudo, PowerBroker or Pimsu.



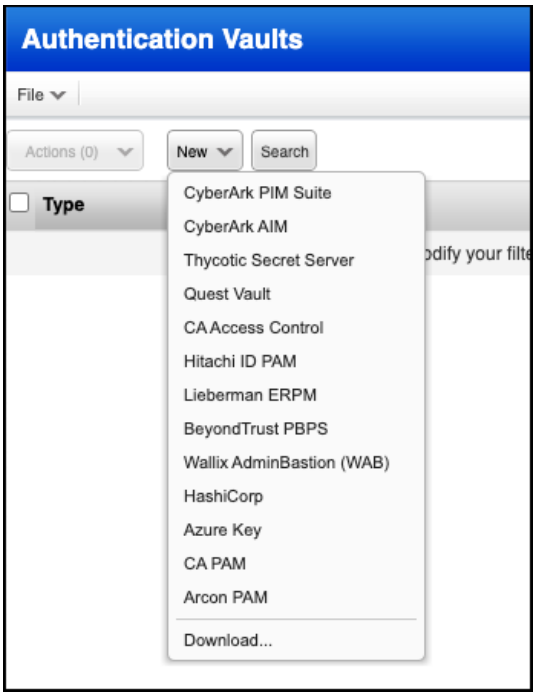
IP addresses are required for all Unix-based authentication records.



Click the "Create" button to complete the creation of your new Authentication Record.



These two authentication records will be used by Option Profiles that have Window and/or Unix authentication enabled.

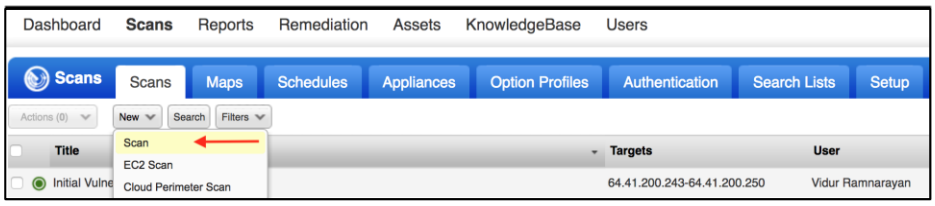


Alternatively, a Qualys Scanner Appliance can use authentication credentials collected from one of the supported authentication vaults.

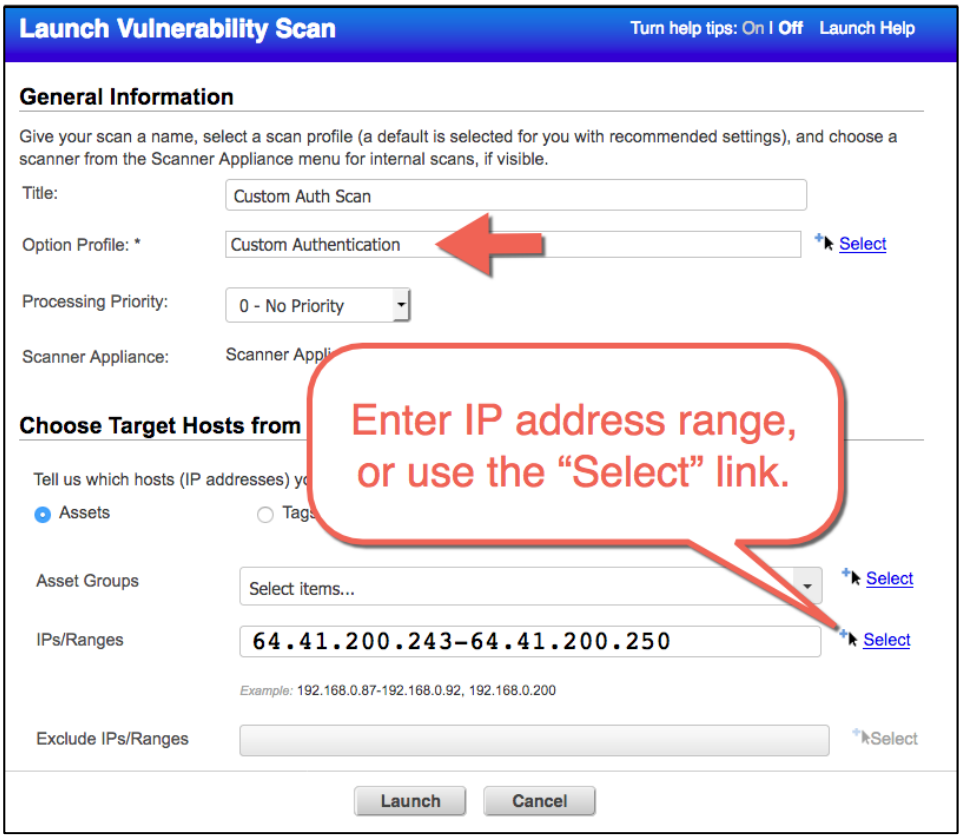
Launch Scan

Navigate to the following URL to view the "Launch Scan & View Results" tutorial:

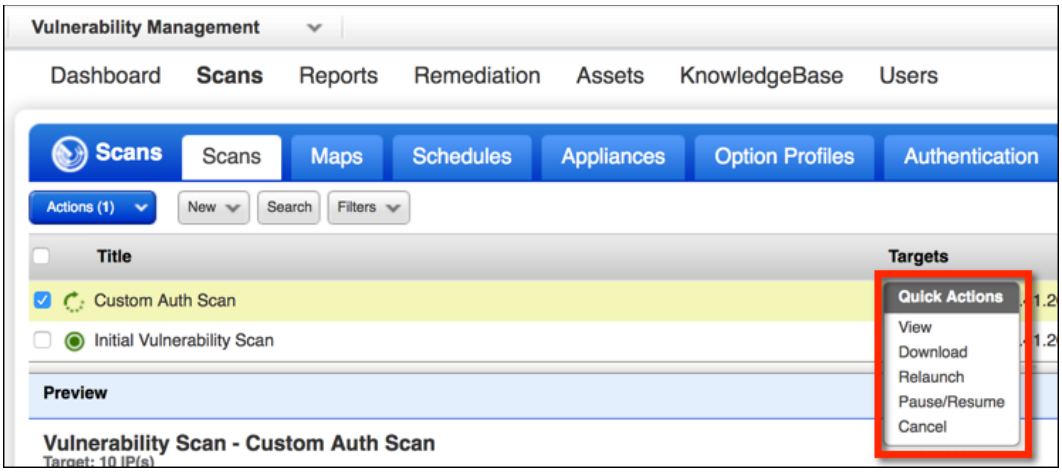
PLAY LAB 9 - https://ior.ad/7edJ



1. **Navigate to the "Scans" tab, click the "New" button and select the "Scan" option.**



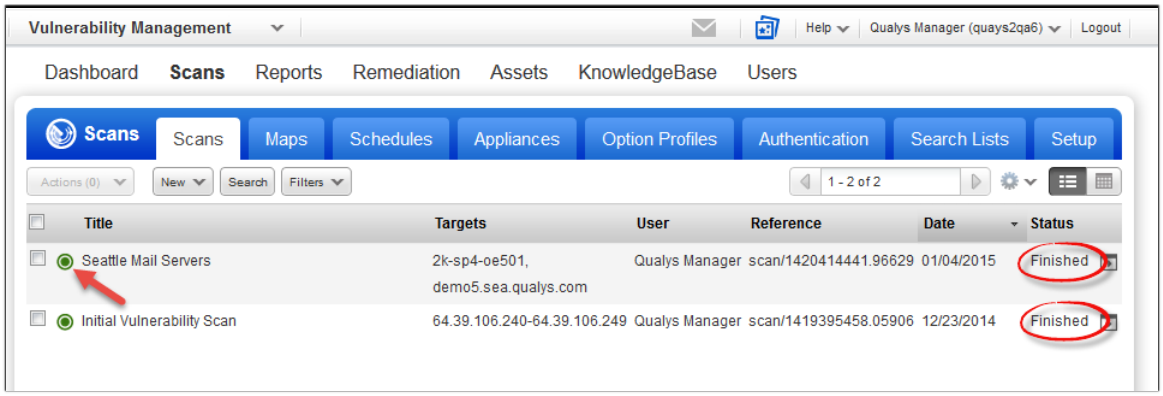
2. **Enter the Title: Custom Auth Scan.**
3. **Select the "Option Profile" you just created (Custom Authentication).**
4. **In the "Choose Target Hosts from" section, enter the IP address range for all host IPs (64.41.200.243-64.41.200.250), or click the "Select" link to select all IPs from a list.**
5. **Click the "Launch" button to launch the scan.**
6. **Click the "Close" button to close the "Scan Status" window, when it is displayed.**



From the "Scans" tab, you can use the "Quick Actions" menu to cancel or pause running scans. To delete a scan, simply place a check in the box next to the Title, and choose the Delete option from the Actions button.

Processed vs. Unprocessed Scans

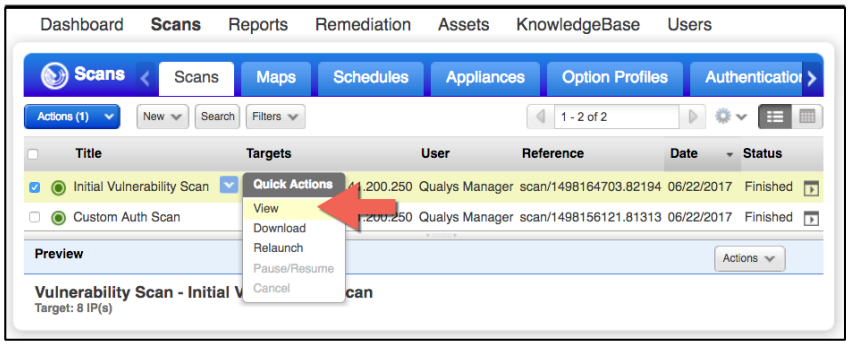
When a Scanner Appliance has finished performing a vulnerability scan, the scan results are sent to the Qualys Secure Operations Center (SOC). The raw scan data is then processed and integrated with the "Host Based Findings" within your subscription.



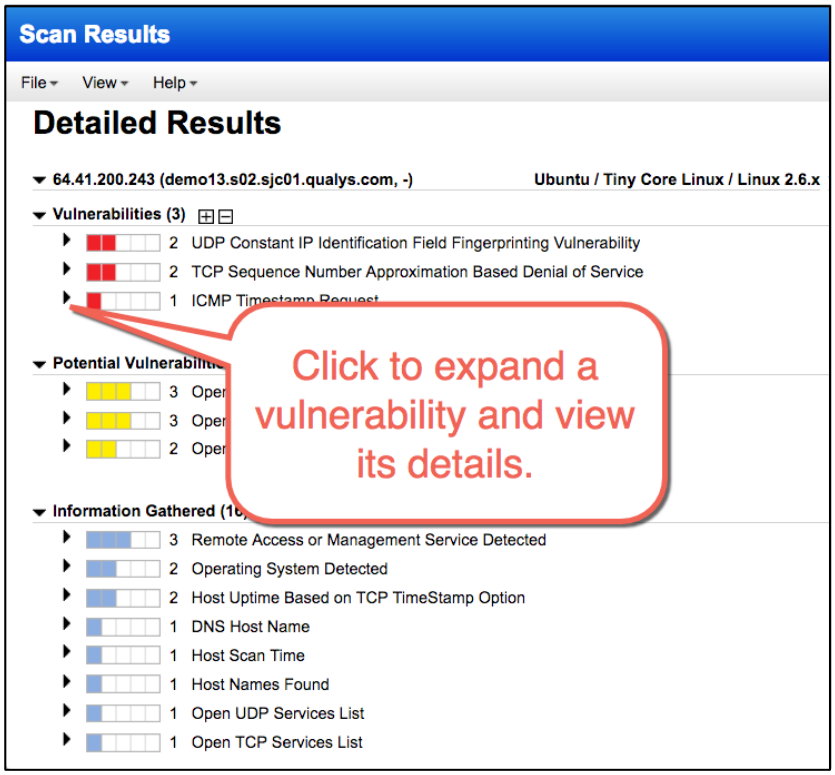
Although the "Status" column may display the "Finished" status, your scan results will not be available for use until the ○ icon changes to the ◉ icon (as illustrated above).

View Scan Results

When a scan is finished, the "raw" scan results can be analyzed.



Choose any "Finished" scan and use its "Quick Actions" menu to select the "View" option.



Here you will find a list of all host assets targeted by the scan, and for each host a list of confirmed vulnerabilities, potential vulnerabilities, and configuration data. Click the ▶ icon to expand any section or expand a specific vulnerability to view its details. You'll find a list of color codes and severity levels on the next page.

Color Codes

Each detected vulnerability can be analyzed by examining its associated color code and severity level.

	Confirmed Vulnerabilities	Security weaknesses verified by an "active test"
	Potential vulnerabilities	Security weaknesses that need manual verification
	Information Gathered	Configuration data

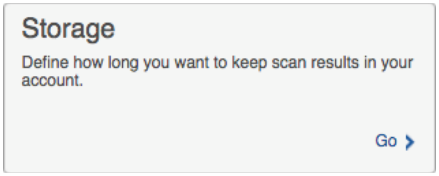
Severity Levels

Level 5	Remote root/administrator	Remote control over system with Admin privileges
Level 4	Remote user	Remote control over system with user privileges
Level 3	Leaks critical sensitive data	Remote access to services or applications
Level 2	Leaks sensitive data	Determine precise system/service versions
Level 1	Basic information	Open ports and other easily deduced data

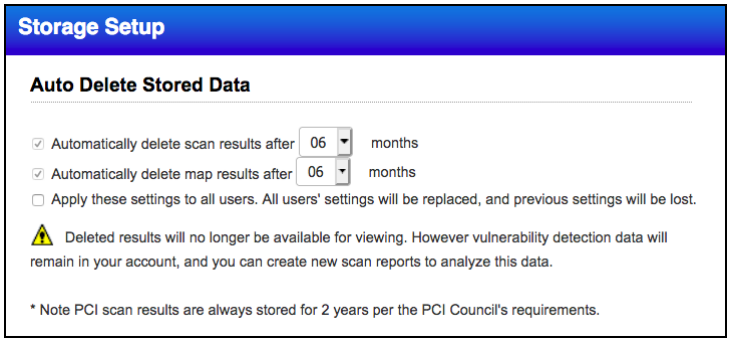
Storage

By default, the Qualys service deletes scan and map results, when they reach the age of six months. You may extend this to thirteen months or reduce it to one month using the "Storage" setup option.

1. **From the "Scans" section, navigate to the "Setup" tab.**



2. **Click the "Storage" option.**



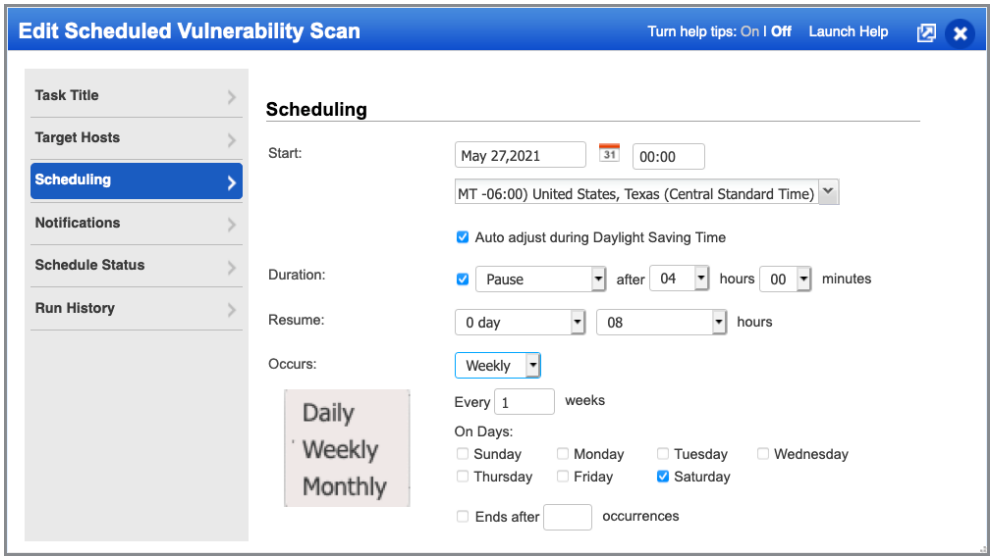
3. **Use either drop-down menu to view the available range of storage time frames.**

   The Storage "Auto Delete" feature will help you keep your scan and map results to a manageable size.

4. **Click the "Save" or "Cancel" button to return to the "Setup" tab.**

Scheduled Scans

As a best practice, schedule scans to run at regular and predictable intervals. The "Schedules" tab (within the "Scans" section) provides option to schedule scans to run at daily, weekly, and monthly intervals.



Navigate to the following URL to view the "Scheduled Scans" tutorial:

PLAY LAB 10 - https://ior.ad/7edW

Reporting

The raw Scan Results (from a completed vulnerability scan) contain a comprehensive account of the data and metadata collected during the course of the scan. The type and amount of information found in the Scan Results, typically exceeds that which is required by your target audiences.

Qualys VM and VMDR provide Report Templates that effectively remove and filter unwanted or unnecessary data and findings from your reports, leaving only the information that is useful to those who will view it.

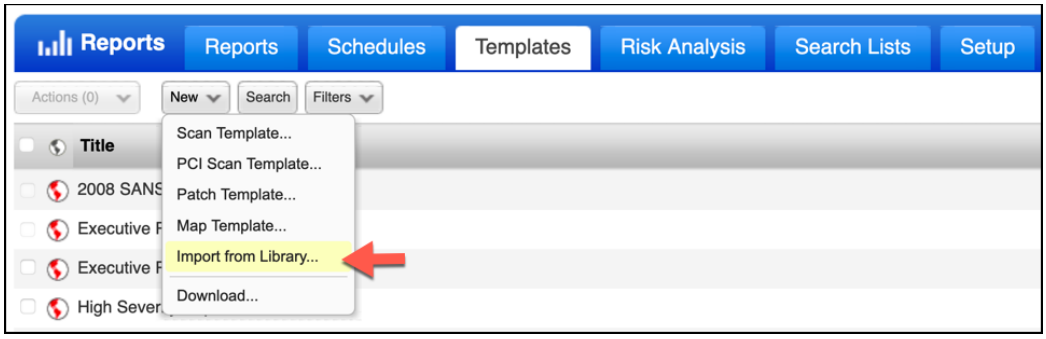
Report Template Library

Qualys provides many "out-of-box" Report Templates designed to meet common reporting tasks and objectives.

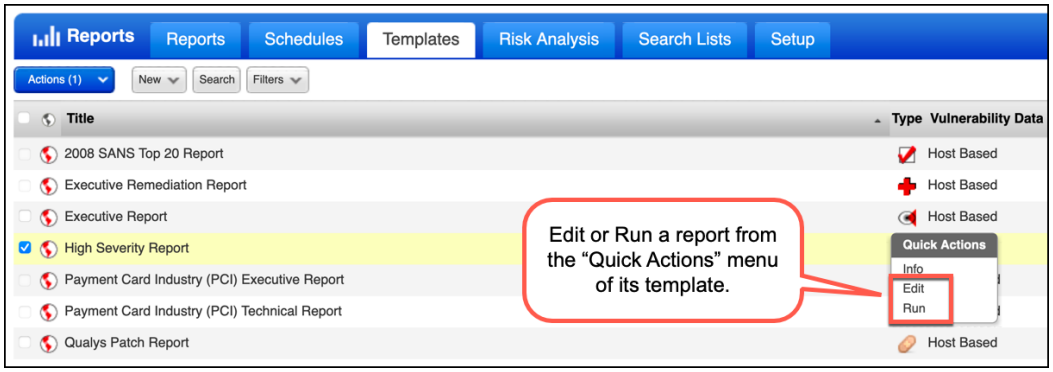
Navigate to the following URL to view the "High Severity Report" tutorial:

PLAY LAB 11 - https://ior.ad/7emY

Import additional templates into your Qualys account from the Report Template Library.

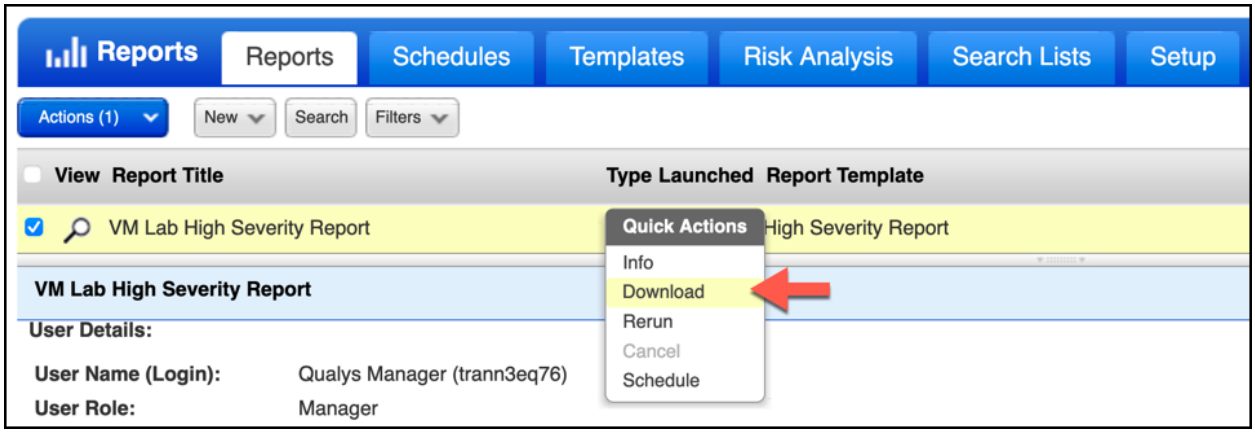


You can edit the "out-of-box" templates to meet your unique reporting needs and objectives.



Edit or Run a report from the "Quick Actions" menu of its template.

All reports have an active life of seven days under the "Reports tab.



Use the "Quick Actions" menu of any report to download and permanently add it to an archive or repository.

Custom Report Template

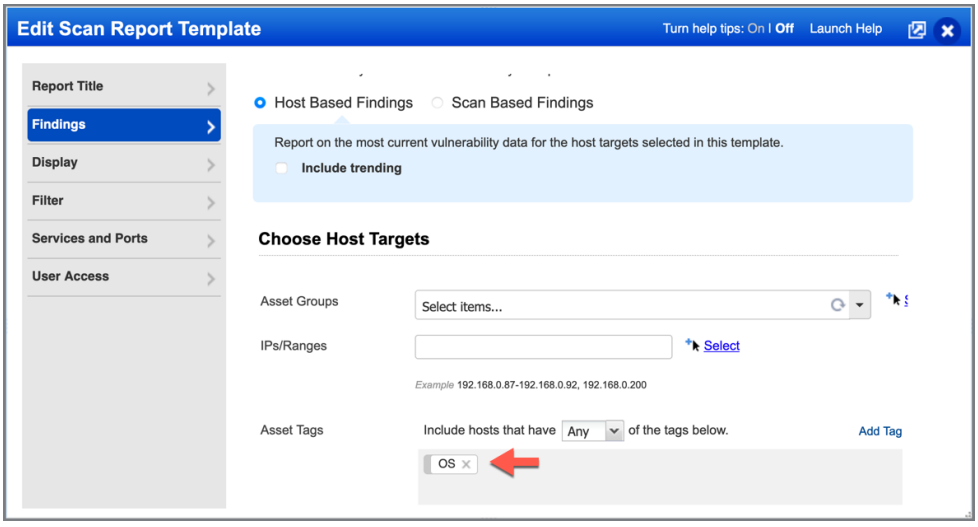
While the "out-of-box" templates are convenient and easy to use, you'll typically want to design and build your own Report Templates to meet your organization's custom reporting objectives. Each template is organized by Findings, Display, Filters, Services and Ports, and User Access.

Navigate to the following URL to view the "Custom Report Template" tutorial:

PLAY LAB 12 - https://ior.ad/7eDm

Findings

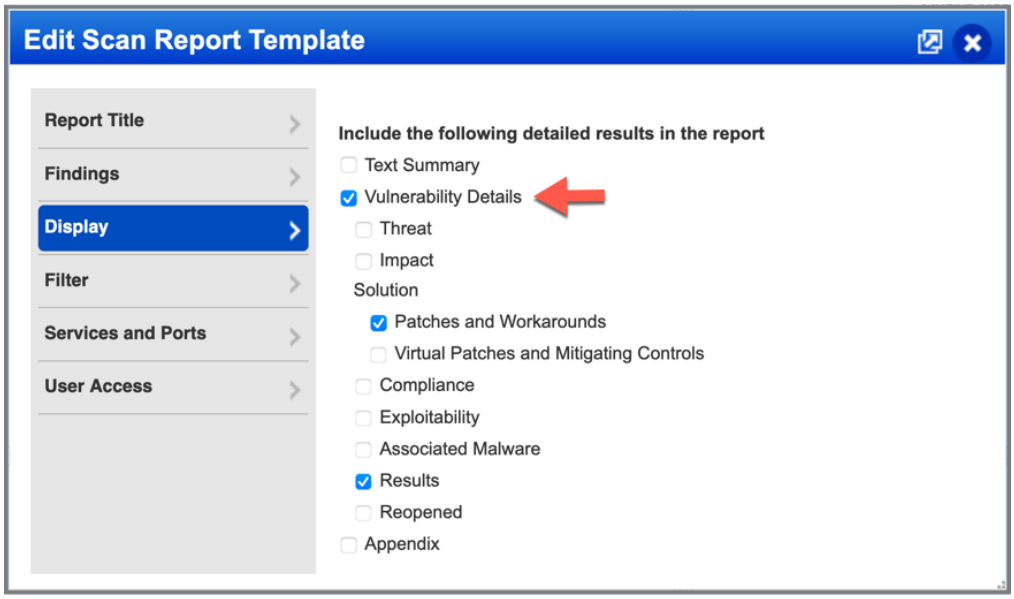
Select Findings in the navigation pane to choose between host-based or scan-based findings.



The "Host Based Findings" option provides vulnerability history and status information and is required to include trending.

Display

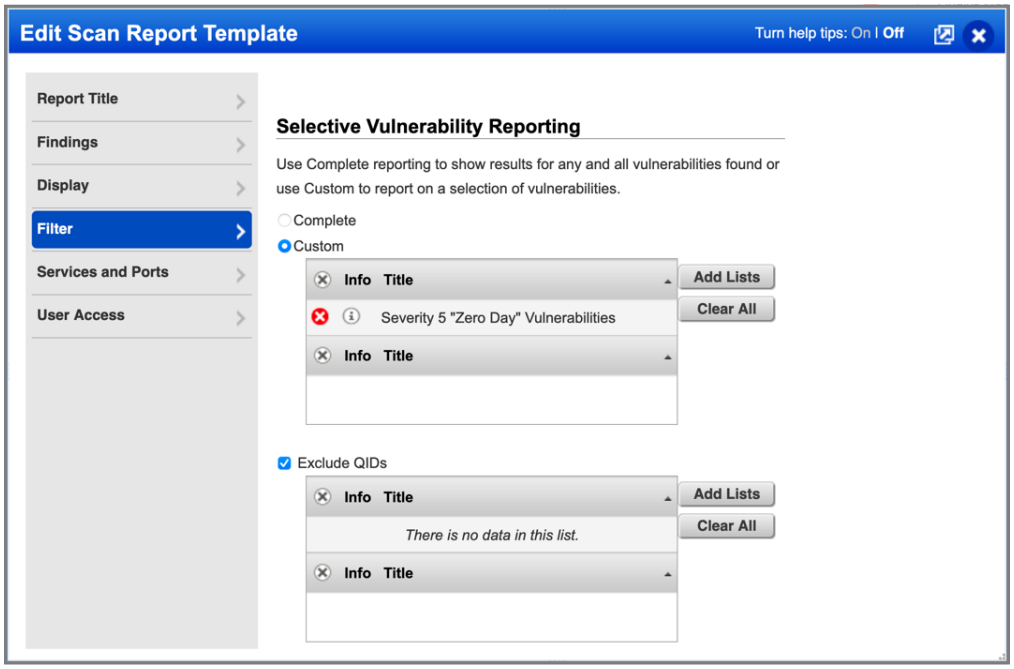
Select Display in the navigation pane to choose amongst various graphics and details settings and options.



As a "best practice" choose the display options that are appropriate for your target audience and do not include information that is not needed.

Filter

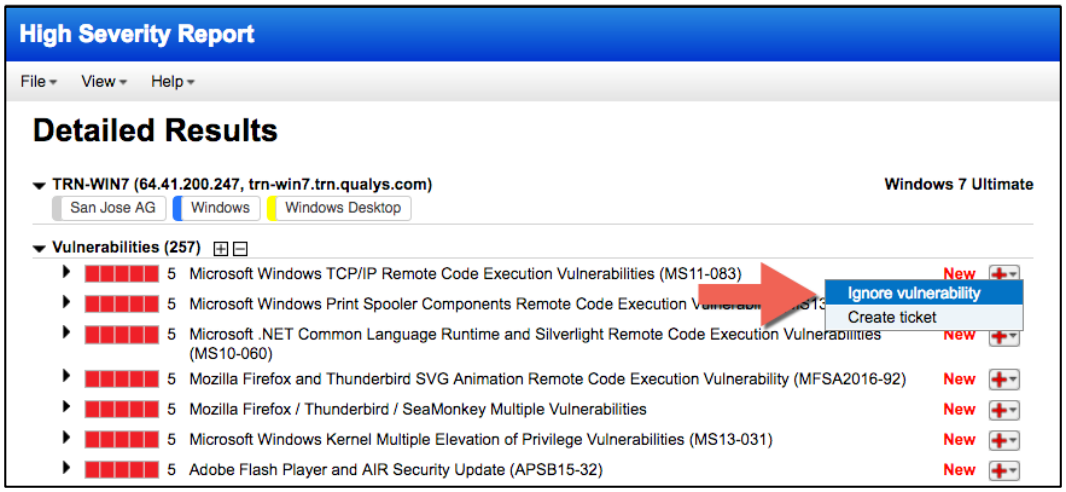
To focus report on a specific list of vulnerabilities, select Filter in the navigation pane and then click the "Custom" radio button to add one or more Search Lists.



Use the "Exclude QIDs" check box to exclude a specific list of vulnerabilities from the report.

Integrated Workflow Actions

When the "HTML pages" report format is used, additional functionality is integrated into a report via the icon. Using "workflow actions" you can ignore vulnerabilities, create remediation tickets, or view remediation tickets that already exists.



The first time a vulnerability is found the word "New" will appear in the report. When a vulnerability is discovered two or more times (in succession), its status will change to "Active." If the vulnerability has been fixed, the word "Fixed" appears.

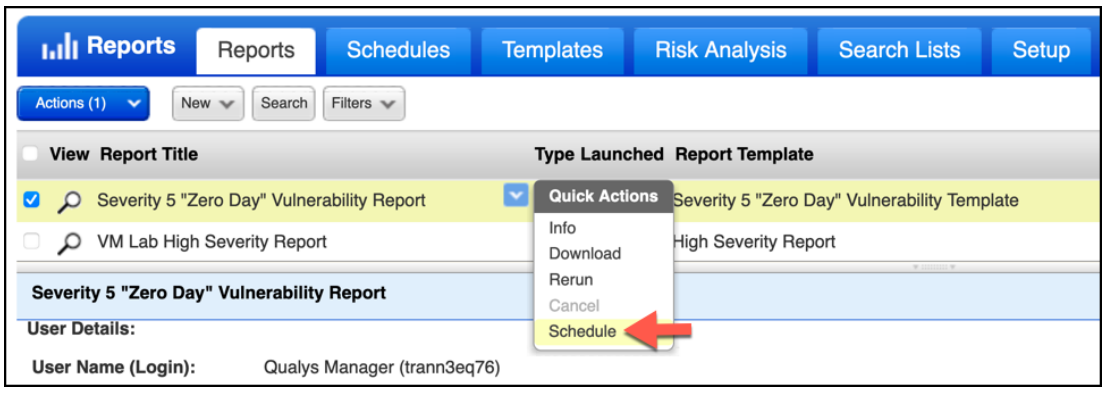
Scheduled Reports

In the same way that scans are scheduled to run at regular intervals, reports can be scheduled run immediately following or soon after scanning intervals have completed.

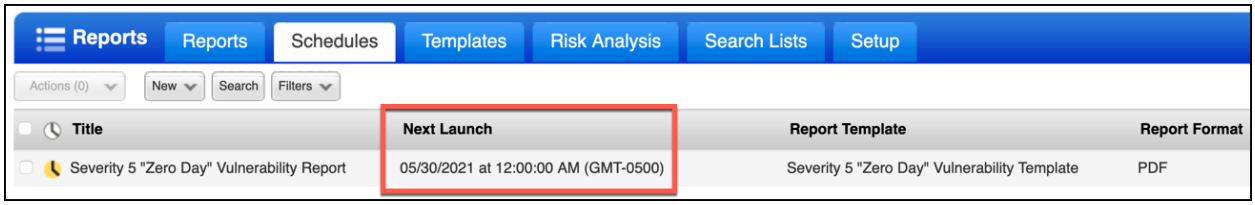
Navigate to the following URL to view the "Scheduled Report" tutorial:

PLAY LAB 13 - https://ior.ad/7eEx

Use the "Quick Actions" menu of any completed report to schedule it to run at a future date or regular intervals.



Scheduled report can be edited and managed from the "Schedules" tab.



User Management

User accounts form the basis for privileges and access control within Qualys. This section will explore creating users and the various levels of user privileges.

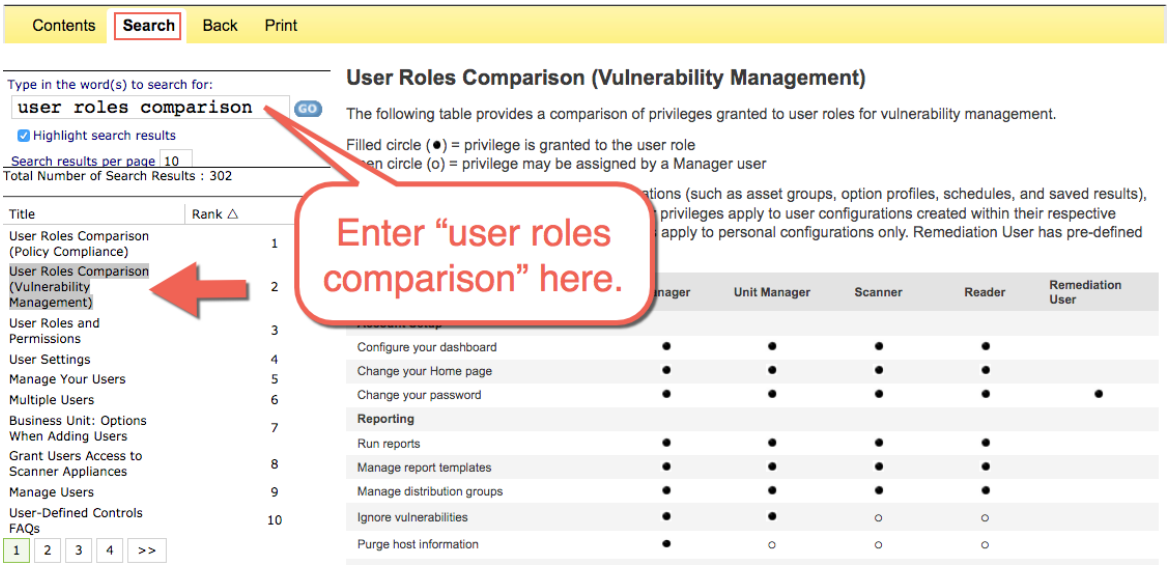
User Roles

User privileges are assigned and identified using various "User Roles". Your Qualys student account has the role of "Manager".

The "Scanner" role carries the primary responsibility of mapping and scanning network resources.

The "Reader" role can create custom reports from existing scan and map data but cannot launch scans or maps.

The "Remediation User" role provides the least privileges of all user roles It was designed for assigning detected vulnerabilities to a specific person.



Navigate to the following URL to view the "Create User Account" tutorial:

PLAY LAB 14 - https://ior.ad/7eFw

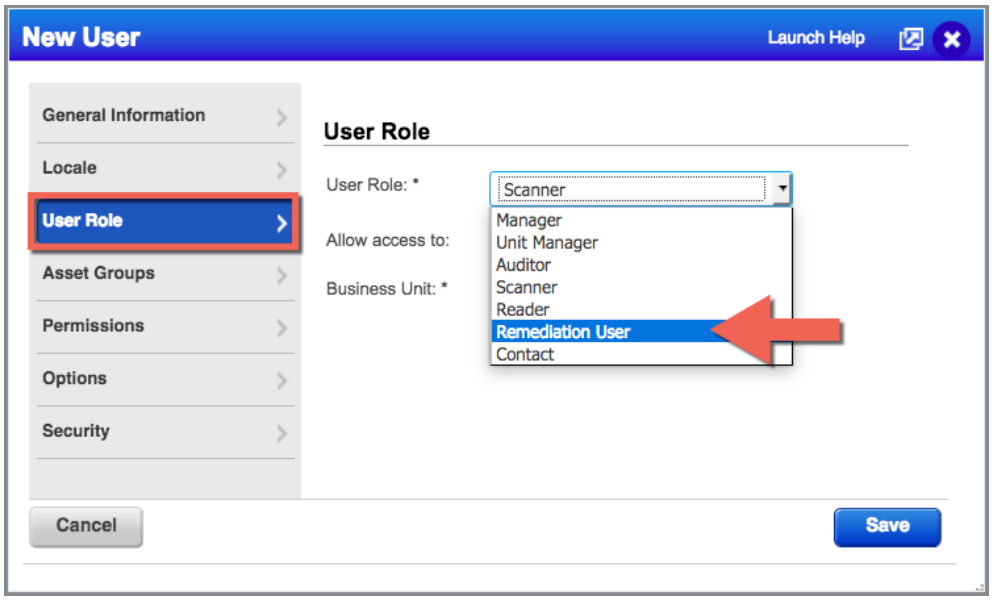
To view a comprehensive comparison of all Vulnerability Management user roles:

1. **Click the "Help" button and select the "Online Help" option.**
2. **Click the "Search" menu, enter "user roles comparison" in the "Search" field, and click GO.**
3. **Click "User Roles Comparison (Vulnerability Management)" in the search results, to view the VM comparison chart.**

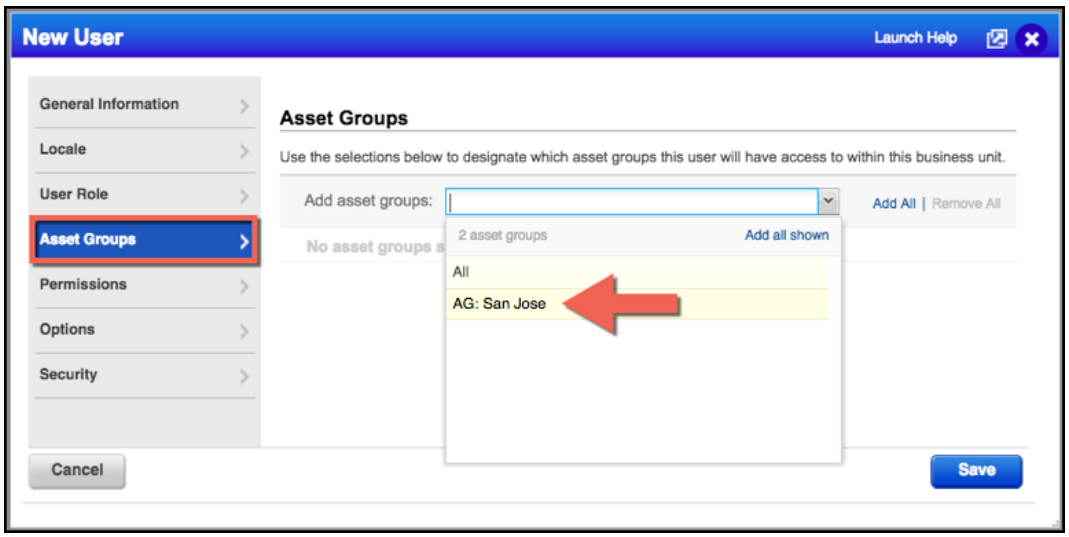
Create User Account

The next few steps will create a new user account, with a specific user roll and some basic privileges.

1. **Navigate to the "Users" section, followed by the "Users" tab.**
2. **Click the "New" button and select the "User..." option.**
3. **Fill in the blank fields in the "General Information" section with your info. Use a valid email address that you can get to from the computer you are seated at.**

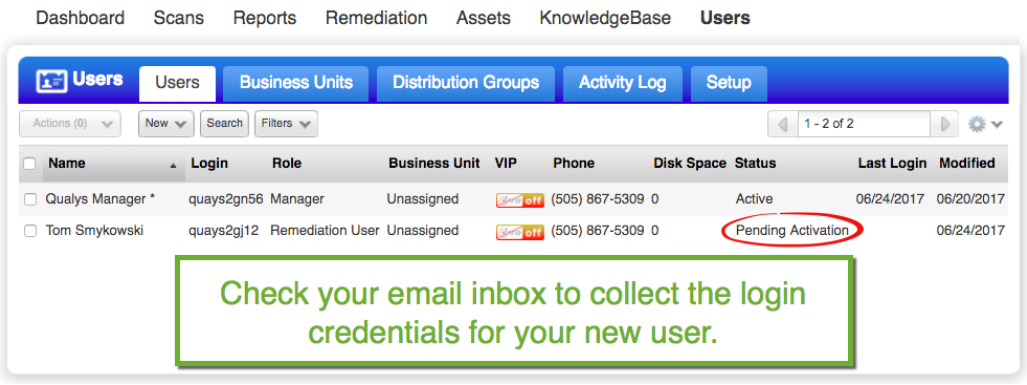


4. **Click "User Roles" in the navigation pane (left) and choose "Remediation User" as your User Role.**



5. **Click "Asset Groups" in the navigation pane and add "AG: San Jose" to this account.** Presently, access permissions are provided to user accounts, using Asset Groups. This includes scanning, reporting and remediation access privileges.
6. **Click the "Save" button.**

Your new user account is created in the "Pending Activation" status. To activate a new user account, login to the new account using the credentials delivered to your email inbox.



7. **Activate this account by opening the email sent by Qualys (subject: Qualys Registration – Start Now) and using the provided credentials to login.**

Remediation

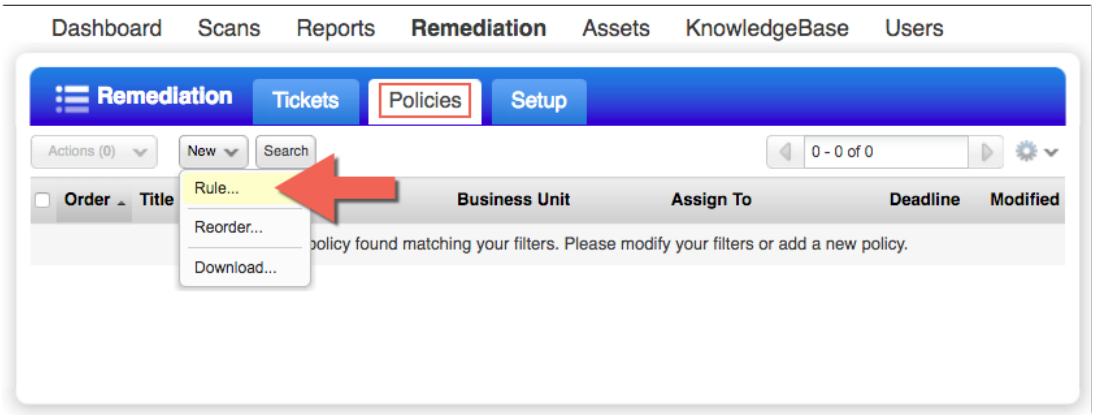
In this lab, you will create a Remediation Policy that assigns vulnerabilities to a specific user, and a second policy that ignores vulnerabilities that will not be addressed or resolved.

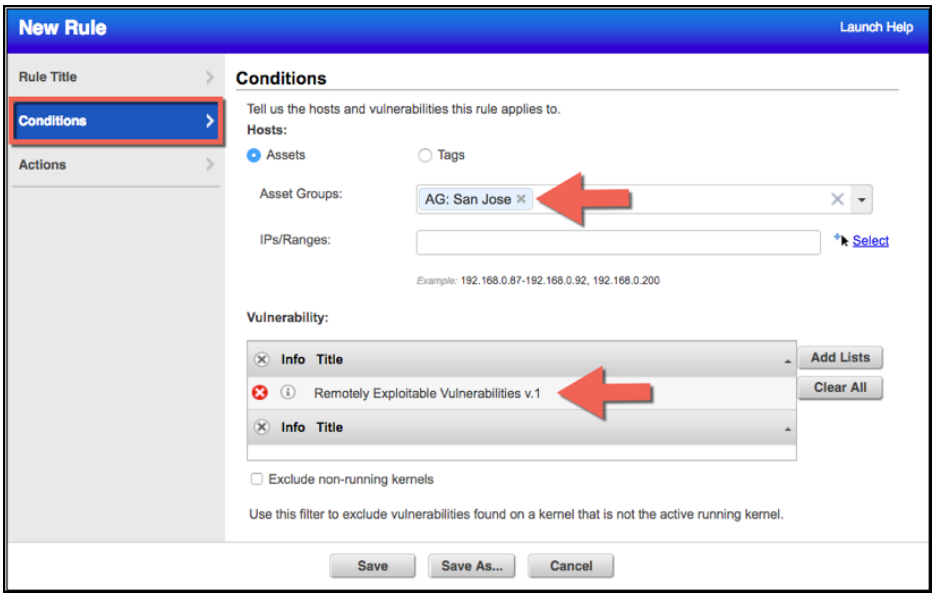
Assign Vulnerability to User

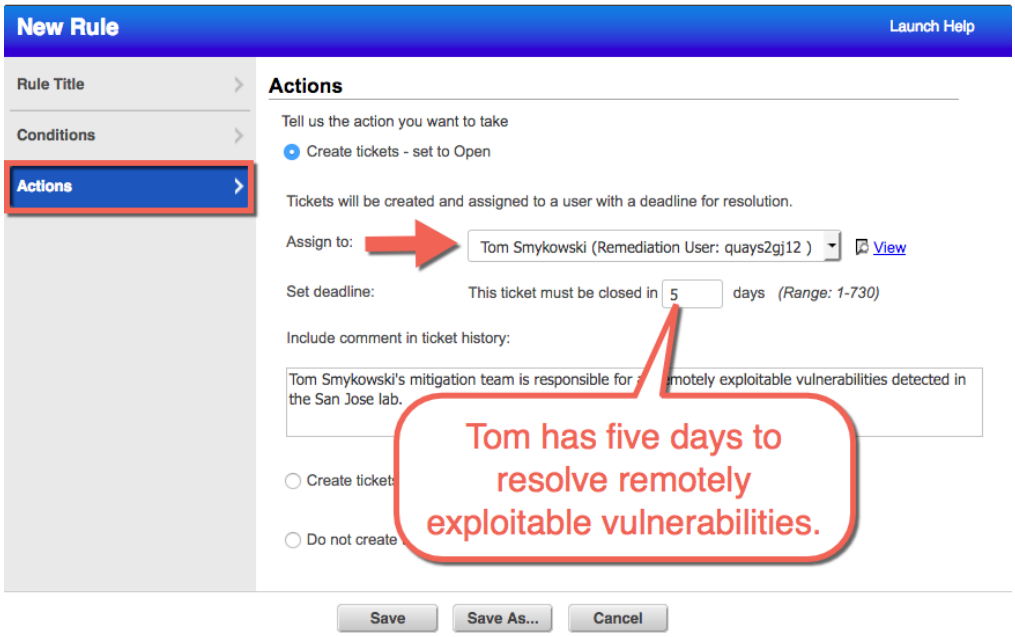
This first policy will be used to assign remotely exploitable vulnerabilities, to the “Remediation User” account created in the “User Management” lab.

Navigate to the following URL to view the “Assign Vulnerabilities” tutorial:

PLAY LAB 15 - https://ior.ad/7eMh





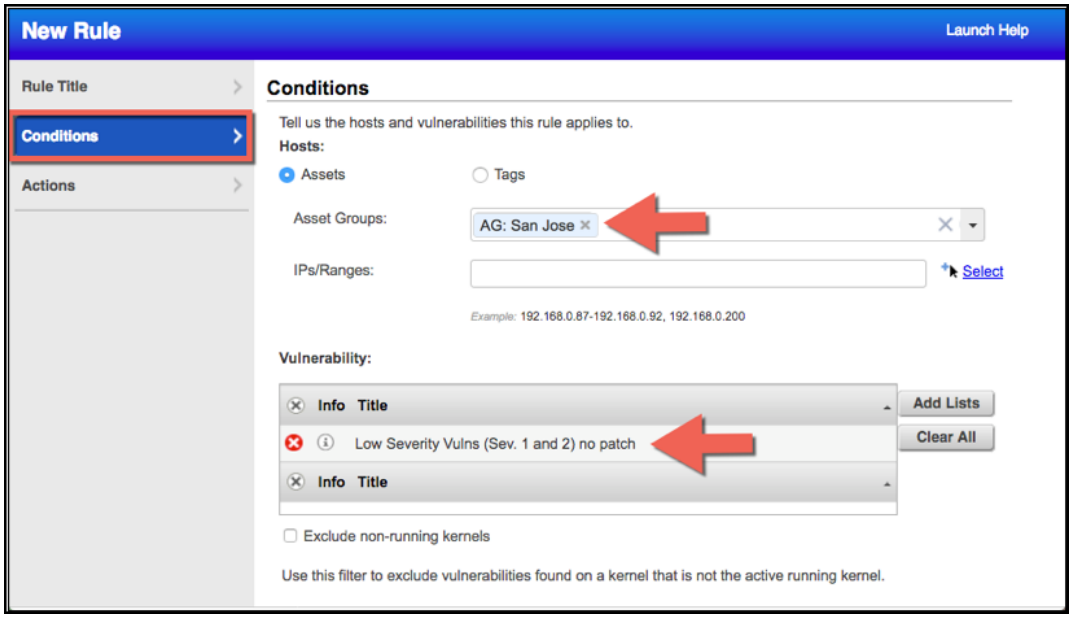


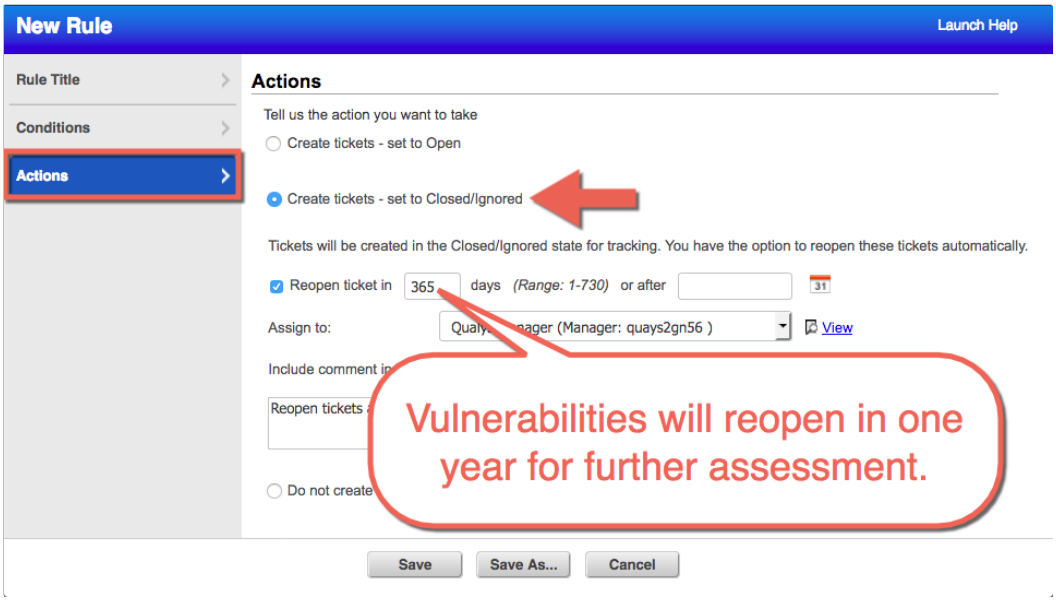
Ignore Vulnerabilities

Remediation Policies can be used to automate the process of ignoring vulnerabilities that you do not plan to address or resolve.

Navigate to the following URL to view the "Ignore Vulnerabilities" tutorial:

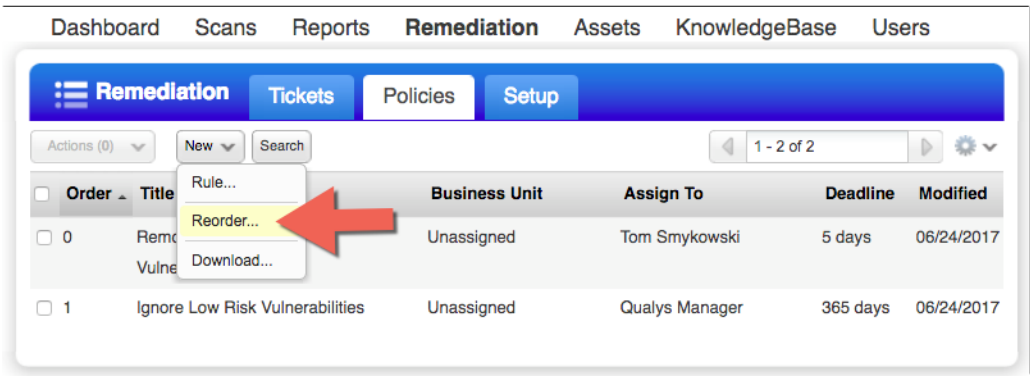
PLAY LAB 16 - https://ior.ad/7ecB



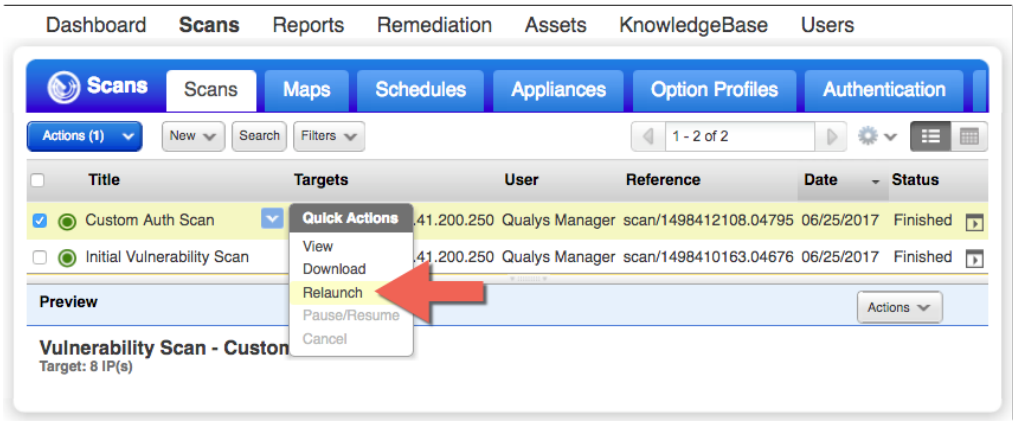


Configure the option to reopen vulnerabilities. This option is convenient for those who wish to re-assess the risk of ignored vulnerabilities at regular intervals.

Remediation Policies are evaluated in order from top to bottom. Place the most important policies at the top of the list.



An additional vulnerability scan will be required here, to see the results of the Remediation Policies just created.

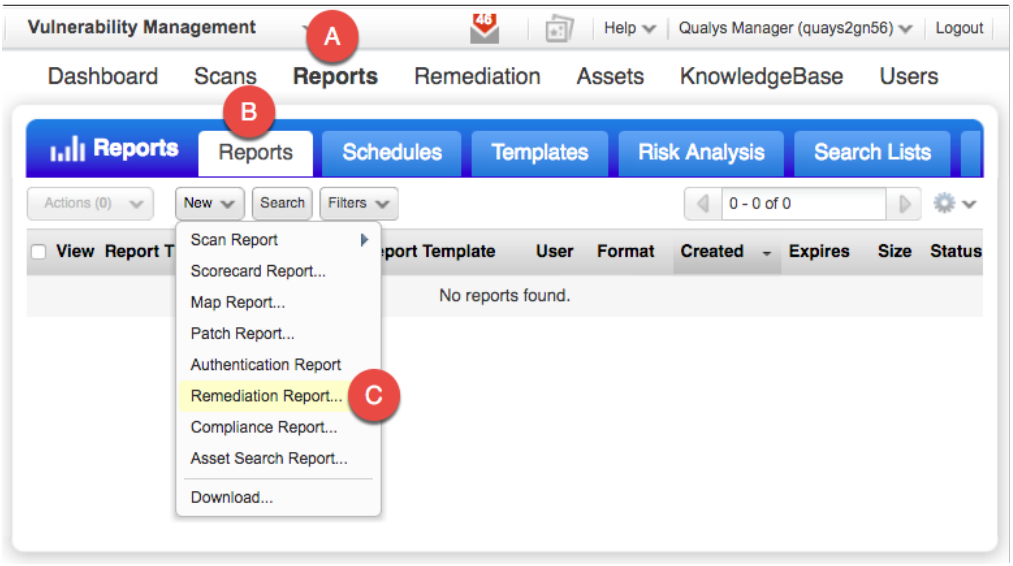


Create Remediation Report

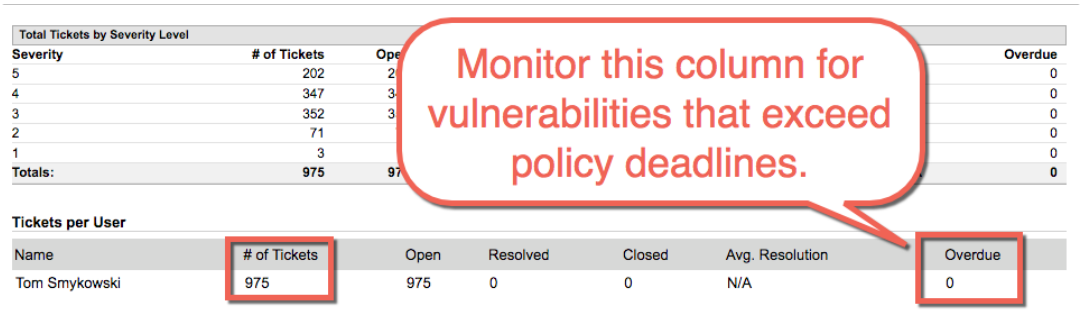
With the creation of at least one remediation policy, you can build reports to monitor the progress of your patching and mitigation activities.

Navigate to the following URL to view the "Remediation Report" tutorial:

PLAY LAB 17 - https://ior.ad/7eXH



Along with some useful statistics, the real beauty of this report is the "Overdue" column which tracks the number of vulnerabilities that have exceeded policy due dates.



This type of information can be very useful for identifying bottlenecks in your mitigation processes and activity.

Appendix A: Mapping

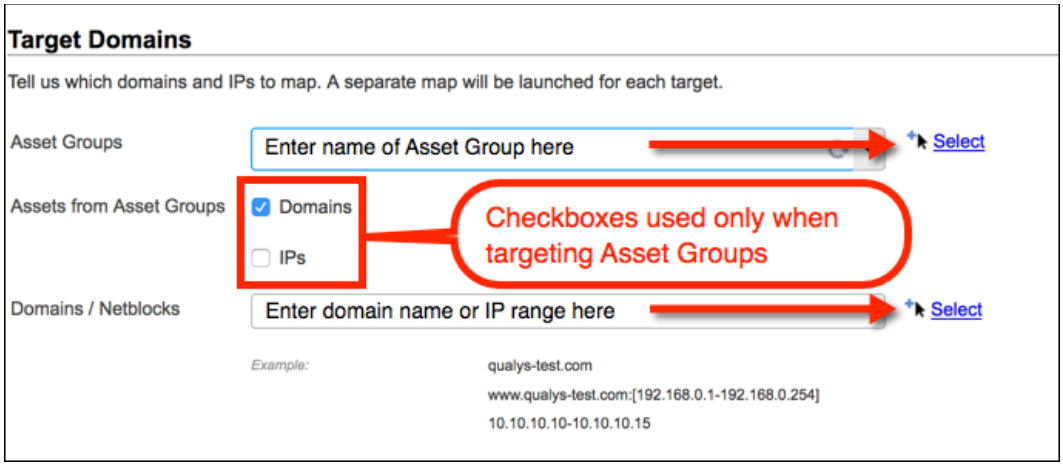
Map reports are very useful tools when managing all host assets within your company or enterprise architecture. Only mapping provides "discovery" data that will allow you to distinguish between authorized and unauthorized hosts. When used properly, mapping can help you add a new host to your Vulnerability Management subscription, approve other hosts that will not be added to your subscription, and even find "rogue" devices within your network.

Mapping Targets

Unless you manage a limited number of hosts, it is considered a "best practice" to map you network or enterprise architecture in small segments. You can accomplish this task using any of the basic mapping targets:

- Asset Group
- Domain
- Netblock

Understanding the proper use of mapping targets will lead to the creation of successful map reports.



Asset Group

Although Asset Groups will be defined in detail later, within the Asset Management lab, a couple of key points are required here in the discussion of mapping:

- Asset Groups only contain hosts that have already been added to your Vulnerability Management subscription.
- The "Domains" and "IPs" checkboxes are used only when an Asset Group has been selected as a target.

Domain

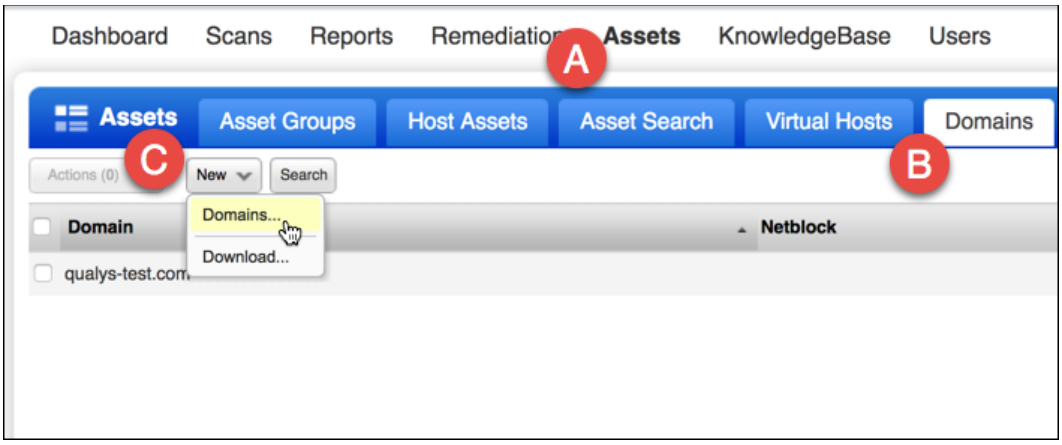
Another target option for mapping involves using a domain name. A domain name must be added to the "Domains" tab, before it can be used as a target for mapping. Basic DNS reconnaissance is used to collect information from a domain target. Additionally, TCP, UDP, and ICMP probes are used to validate the DNS reconnaissance findings.

Netblock

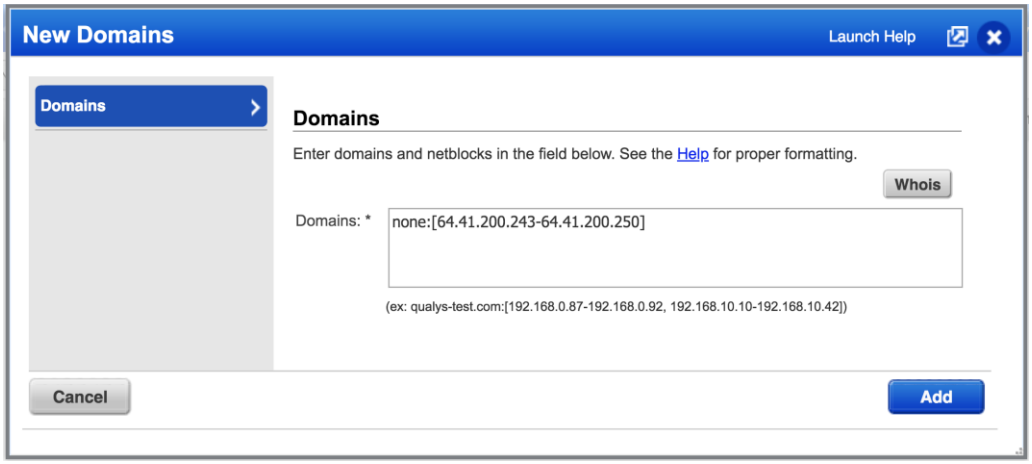
A netblock must also be added to the "Domains" tab, before it can be used as a mapping target. The "none" Domain is a special domain, used to add netblocks to the "Domains" tab. Various probes such as TCP, UDP, and ICMP are used to locate LIVE hosts within the targeted netblock.

Add Mapping Target

To use any of the target types listed above, it must first be added to your account. The "Domains" tab is used for adding mapping targets to the Vulnerability Management application (Asset Groups can also serve as mapping targets).



1. **Navigate to the 1) "Assets" section, 2) "Domains" tab, click on the 3) "New" button and select the "Domain" option.**



2. **Add the following netblock to the "Domains" field:**

   `none:[64.41.200.243-64.41.200.250]`

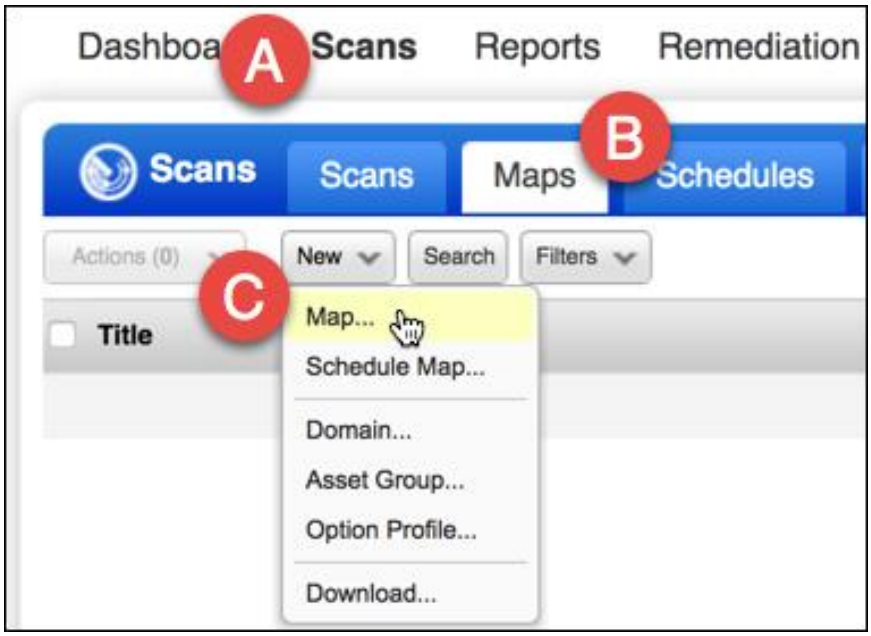
   DO NOT USE COPY AND PASTE (there is no blank space in the "none" domain).

The "none" domain can be used to target any netblock within your organization. Notice that the netblock listed above contains two more IP addresses than the number of IPs already within your subscription. It is a "Best Practice" recommendation to add all reserved IP address netblocks (RFC 1918) to the "none" domain.

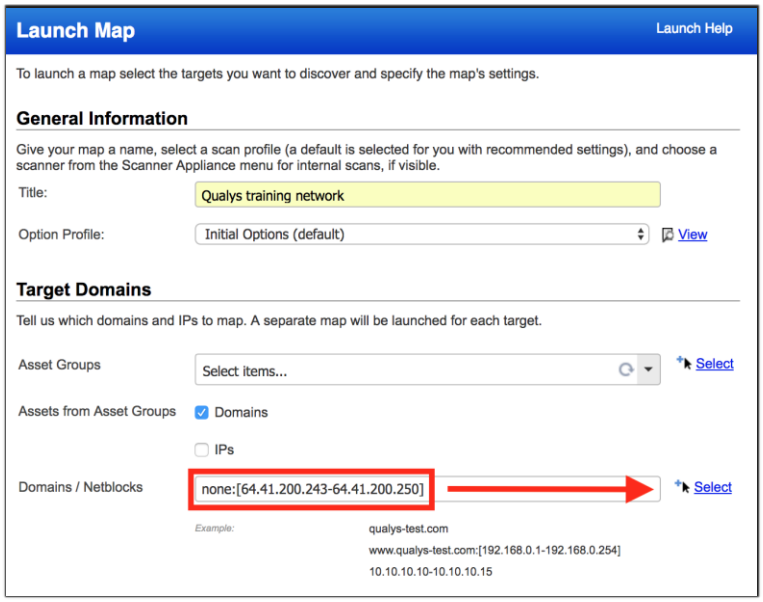
3. **Click the "OK" button to acknowledge your scanning permission.**

Launch Map

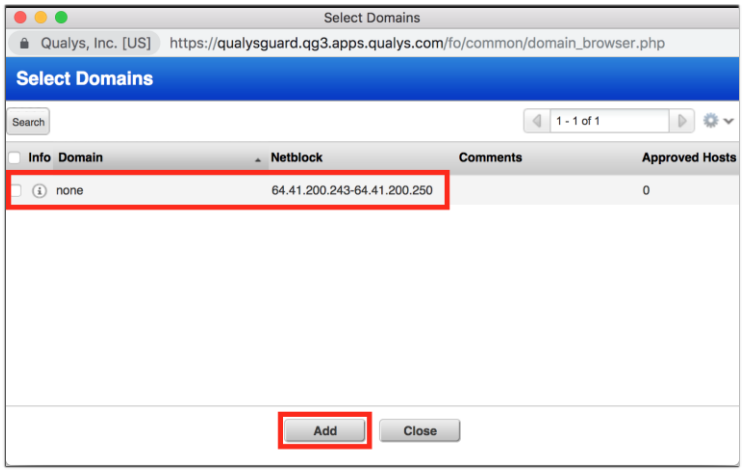
In the next few exercise steps, you will use the "none" domain target to create a Map Report of the hosts within the Qualys Training Network.



1. **Use your mouse to navigate to the 1) "Scans" section, 2) "Maps" tab, click on the 3) "New" button and select the "Map" option.**



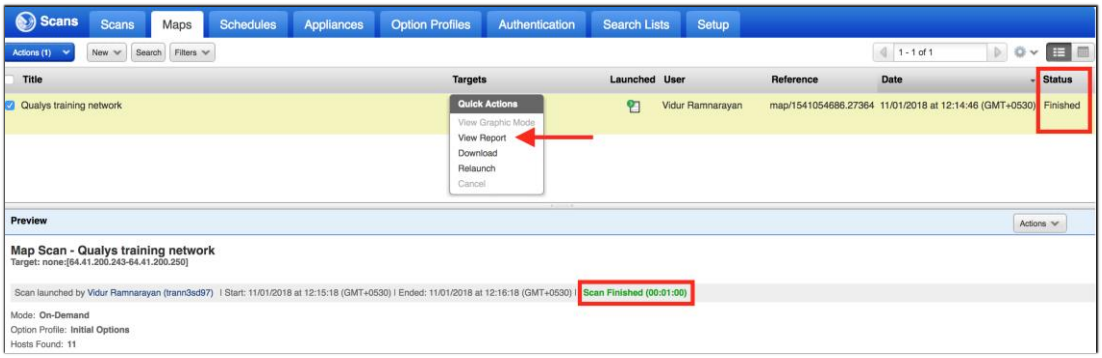
2. **In the "Title" field type: "Qualys Training Network".**
3. **Leave the Option Profile set to: Initial Options (default).**
4. **Under "Target Domains" click the "Select" link just to the right of the "Domains/Netblocks" field.**



5. **Check the "none" Domain and click the "Add" button.**
6. **Click the "Launch" button to begin mapping. It is normal for your map task to display the "Queued" status, before changing to the "Running" status.**

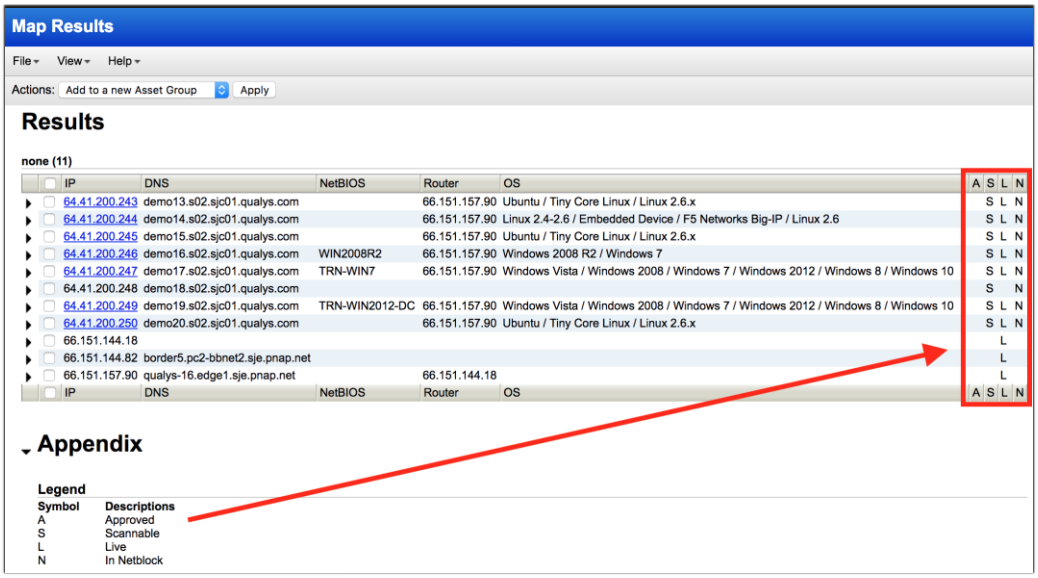
View and Use Map Results

When a map reaches the "Finished" status, you may view its results. Do not attempt to view map results while the Status column displays the "Queued" or "Running" status.



1. **To view your finished map results, open the Quick Action menu and select the "View Report" option.**

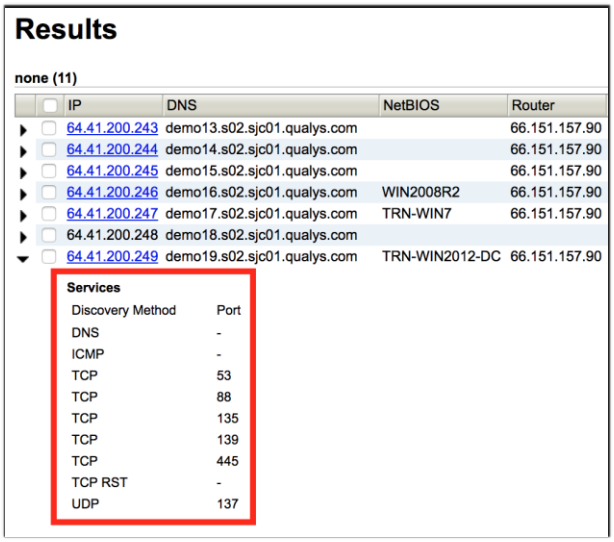
LOOK *If the "View" option is grayed-out, try refreshing your browser.* LOOK



2. **Scroll down to the "Results" to view the hosts that were discovered.**

   Each host is identified by its IP address and name (DNS or NetBIOS). If "Basic Information Gathering" is enabled the map will also provide Router and OS information.

   The columns that appear on the right side of the report are used to identify Approved hosts (A), Scannable hosts (S), Live hosts (L), and Netblock hosts (N). A host is considered "scannable" if it has already been added to your Vulnerability Management subscription. The "netblock" symbol is only relevant when a netblock is selected as the mapping target.

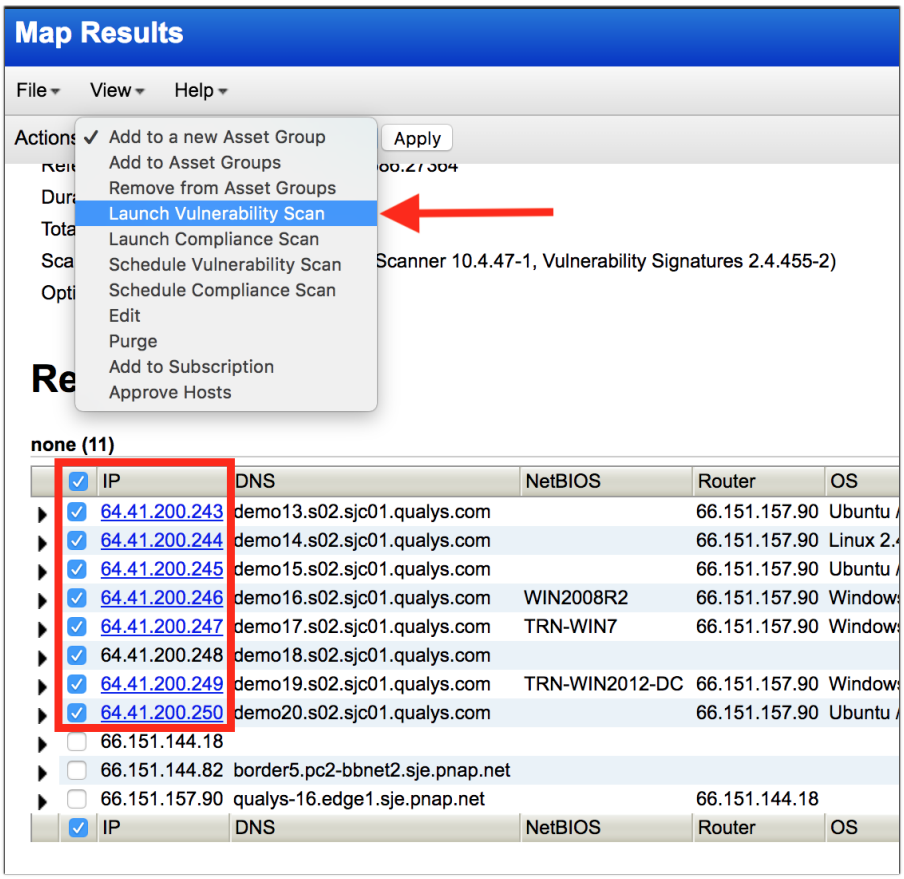


3. **Click the arrow icon ▶ to the left of a host to view its discovery method.**

   Notice there may be some host(s) that are outside of the IP range you mapped. They are not members of the target netblock. They are typically discovered via traceroute. Hosts inside the IP range you mapped were discovered in various ways (common TCP ports, UDP ports, and/or ICMP).

Actions Menu

The "Actions" drop-down menu is provided to perform various actions on any host that appears in the Map Results. To use the "Actions" menu: 1) use a checkbox to select a host, 2) choose an action from the "Actions" menu, and 3) click the "Apply" button.

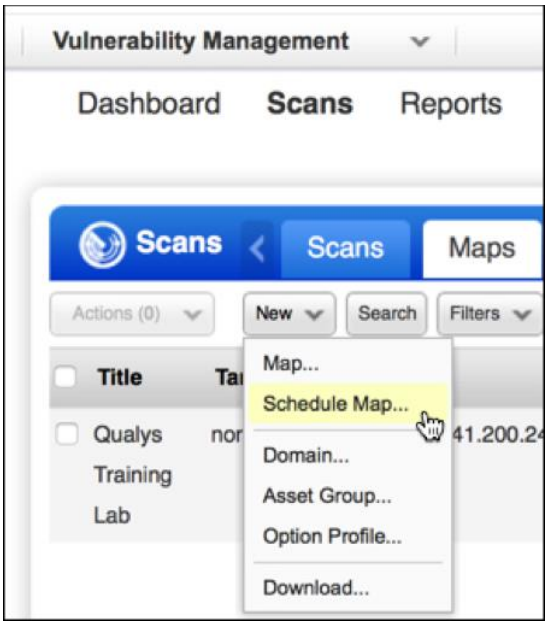


1. **Close the Map Results (File > Close).**

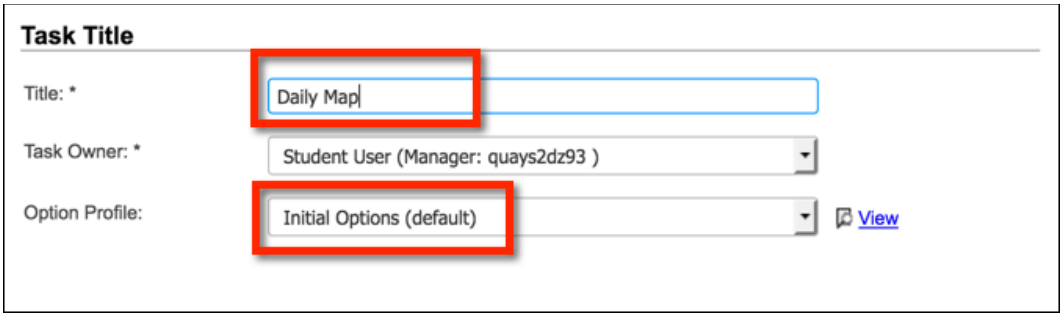
Scheduled Maps

You can use "differential reporting" to compare two maps to identify new hosts introduced into the network, as well as retired hosts that have been removed.

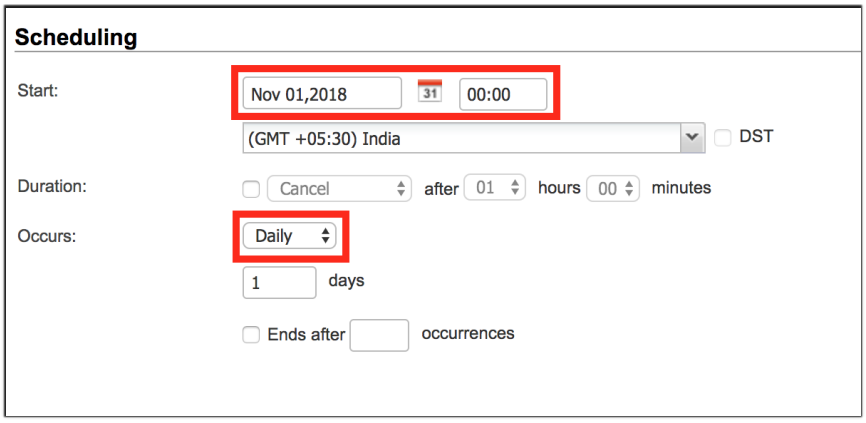
Reporting like this relies on having regular snapshots of the network from which to make a comparison. The next lab steps are designed to schedule a Map Report to run every day.



1. **Navigate to the "Scans" section, followed by the "Maps" tab, click the "New" button and select the "Schedule Map" option.**
2. **Configure the schedule with the following details:**



- **Title: Daily Map**
- **Option Profile: Initial Options (default)**
- **Target Domains: none:[64.41.200.243-64.41.200.250]**



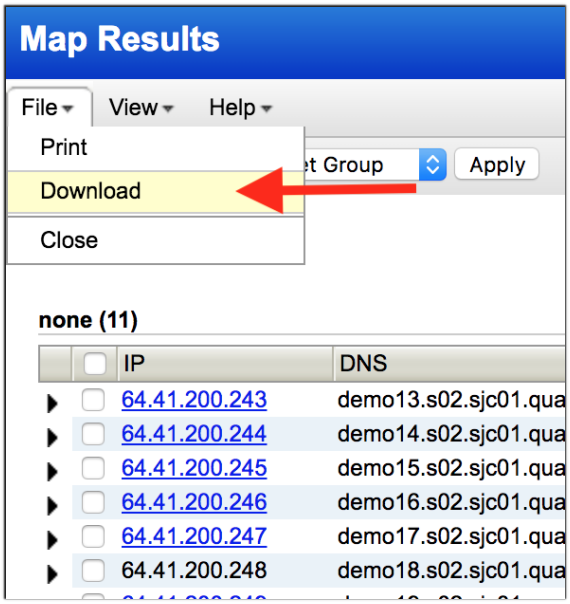
- **Scheduling: Start the scheduled task at a future date and time (time zone is required)**
- **Occurs: Daily**

3. **Click "Save".**

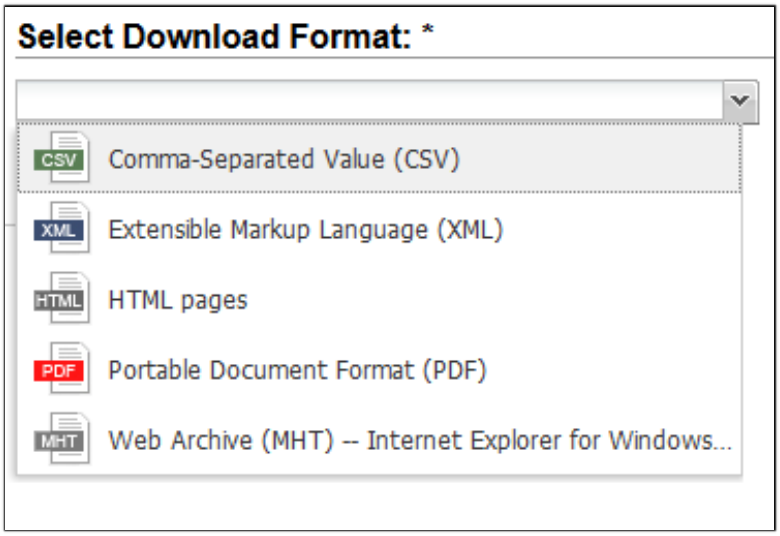
Export and View Map Results

Any Map Report can be downloaded using multiple file format options. Additionally, all maps can be viewed in a "Graphic" mode.

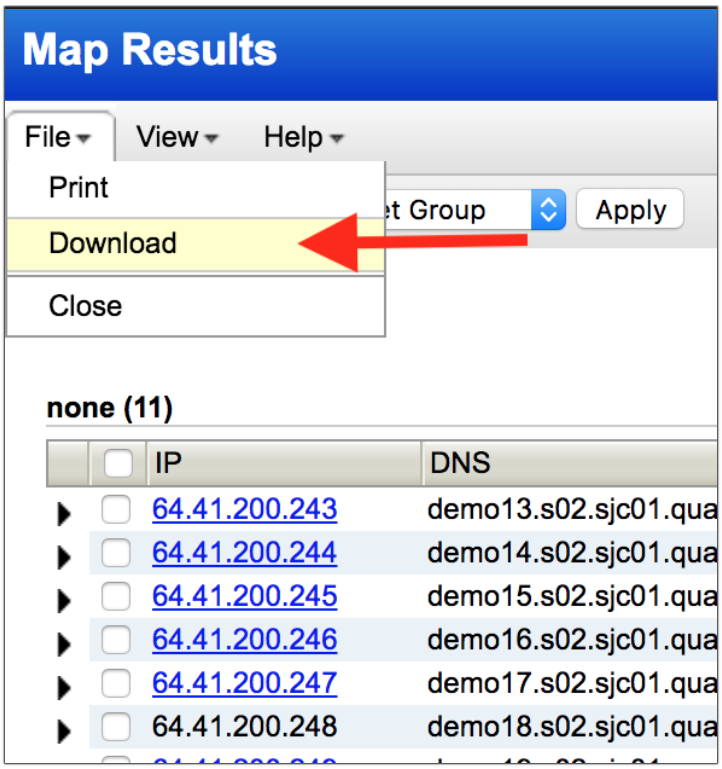
1. **Navigate to the "Maps" tab within the "Scans" section.**
2. **Use the Quick Actions menu to open up and view a Map that you have already created.**



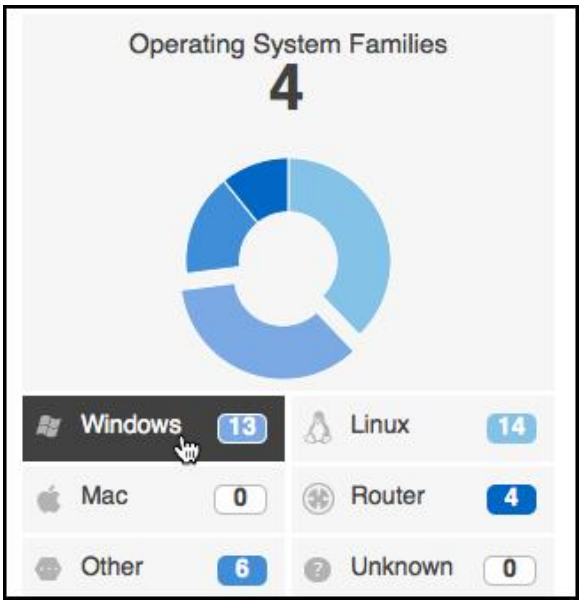
3. **While viewing the map results, click the "File" menu and select the "Download" option.**



Experiment with different file formats. A CSV file can be easily imported into a spreadsheet.



4. **While viewing the same map results, click the "View" menu and then select the "Graphic Mode" option.**



5. **Use the filters on the left to locate the Windows assets in the map results (right). Experiment with different OS options.**
6. **Click the icon over any host to view its information in the preview pane.**

   You can also toggle the "Summary" and "Results" tabs at the top of the window to view a list of assets discovered in the map.

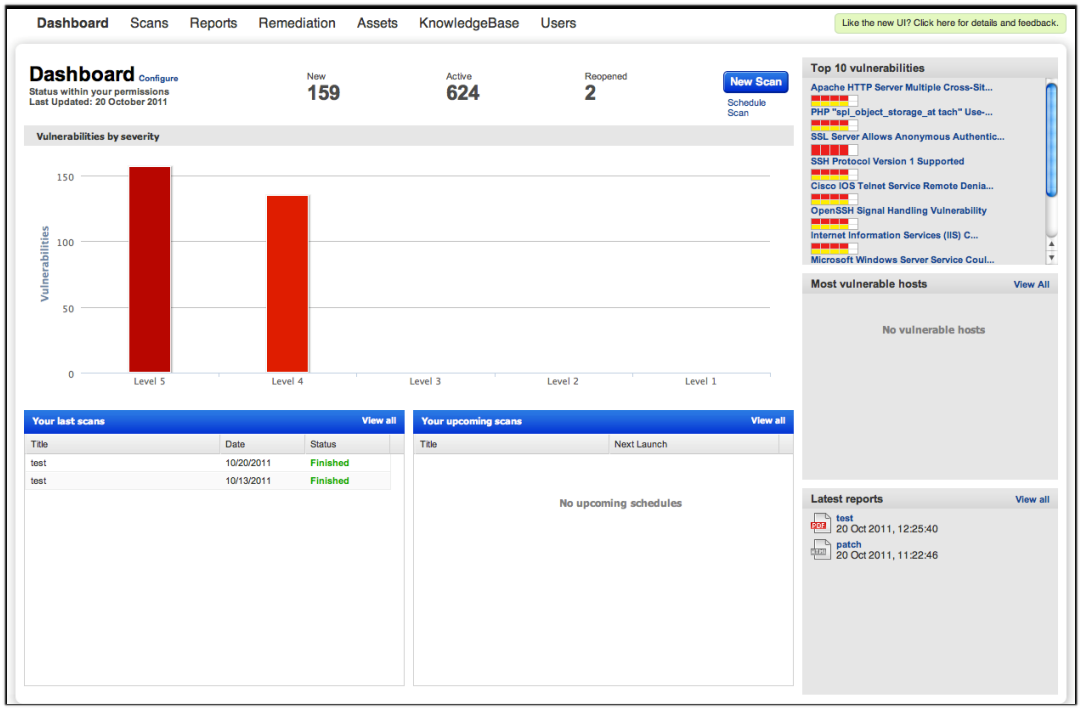
Appendix B: Account Configuration

Before ending the training, it's important that we cover some less conspicuous setup configurations of Qualys. These are items that aren't essential, but may be needed here and there.

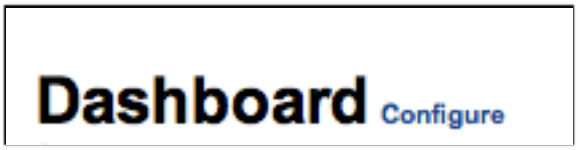
Dashboard

Because we've mapped and scanned, some information will be populated in our Dashboard.

1. **Navigate to the "Dashboard" section.**



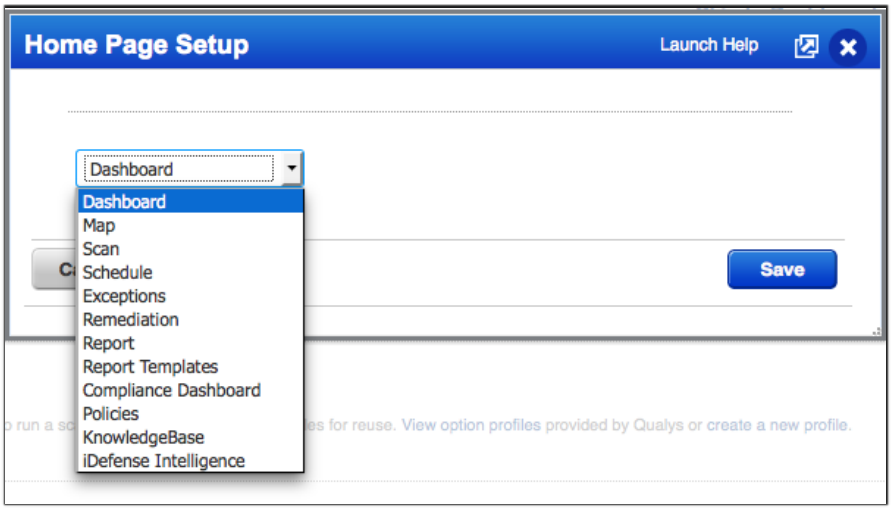
2. **Customize some items on the Dashboard by clicking on the "Configure" link.**



Qualys Home Page

What do you want to see when you login?

1. **Click on your Qualys User ID (located just to the right of the Help button) and select "Home Page".**



2. **Select the home page that best suits your needs, and click the "Save" button.**

Excluding Hosts from Scans

In some cases, you may have IP addresses within a segment that do not need to be scanned, and they will never need to be scanned. In this case, the "Excluded Hosts" section of the Setup menu comes in handy.

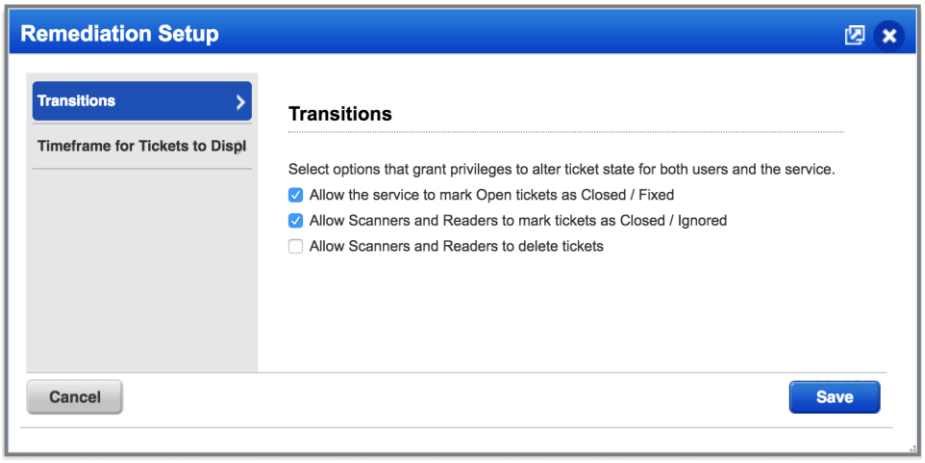
1. **Navigate to the "Setup" tab in the "Scans" section, and click on Excluded Hosts section.**
2. **A new screen will appear.**
3. **Click the "Edit" button.**
4. **Add the IP 64.41.200.243 to the list. Click "Add".**
5. **Add a comment (the Comment field is required).**
6. **Click "Close".**

Tip: it's a good practice to add comments about "why" this is excluded in the event of an audit.

7. **Rerun a light scan over the IP Segment containing the IP address you just excluded. You should not see the .243 address.**

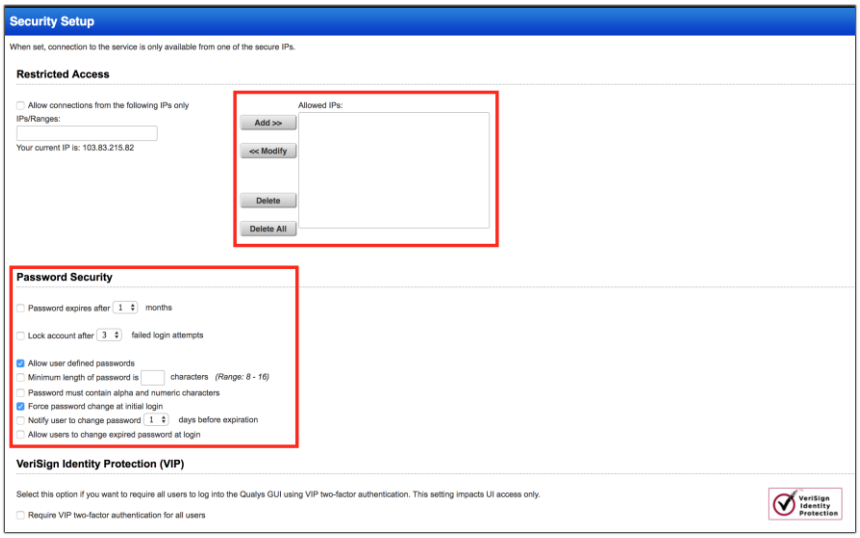
Keep in mind, once you exclude a host, it's a global setting for your subscription, the IPs will be excluded from ALL activity, even though it's still listed in your subscription.

Remember in Remediation how we talk about automatically closing tickets once the scan shows the vulnerability is no longer available? Well, under the "Setup" tab in the "Remediation" section, you will find:



You may also need to determine if the lower privileged groups will be able to Close and Ignore tickets or allow them to Delete tickets – both can be allowed here.

The Security function under the "Setup" tab in the "Users" section allows for the more critical security settings for users and the service:

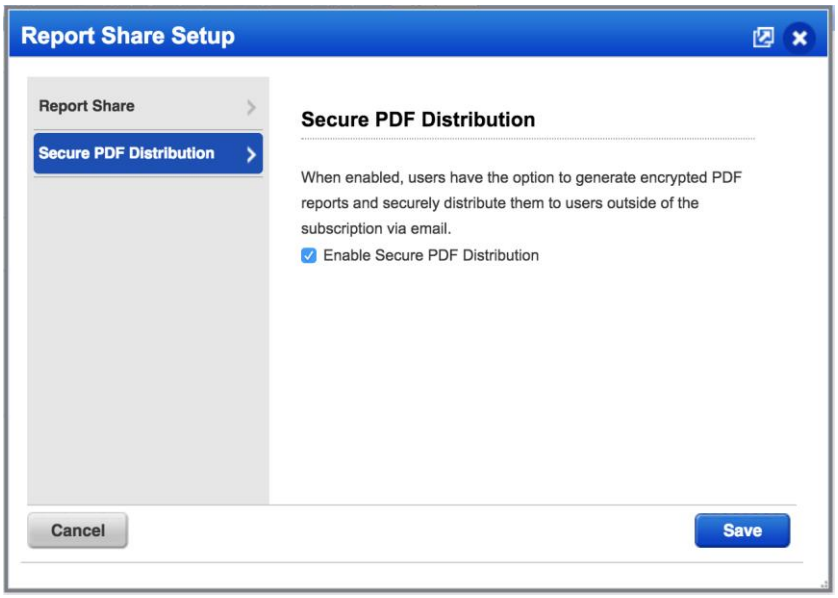


You may want to restrict which IPs have the ability to connect to your QG UI. For this reason, you can restrict access. You can also set password security, even allowing users to set their own passwords.

Finally, let's take a look at the "Report Share" section.

8. **Navigate to the "Setup" tab in the "Reports" section, and click on "Report Share".**

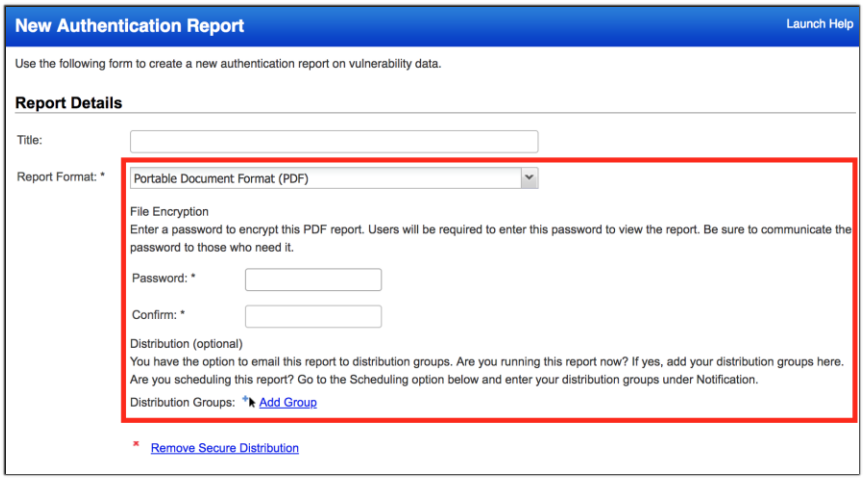
9. **Choose to "Enable Secure PDF Distribution".**



10. **Click "Save".**

11. **Now navigate to Reports and select New > Authentication Report.**

12. **Click "Add Secure Distribution" and choose an email to send your report to.**

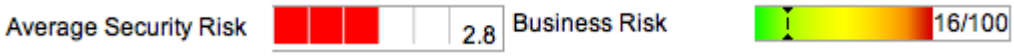


13. **Run the Report.**

Now when you generate a PDF report you'll have the chance to enter a list of email addresses that you'd like the report distributed to securely. As long as you have Adobe on your computer and you know the report password, you'll be able to pull up the report...OUTSIDE of Qualys.

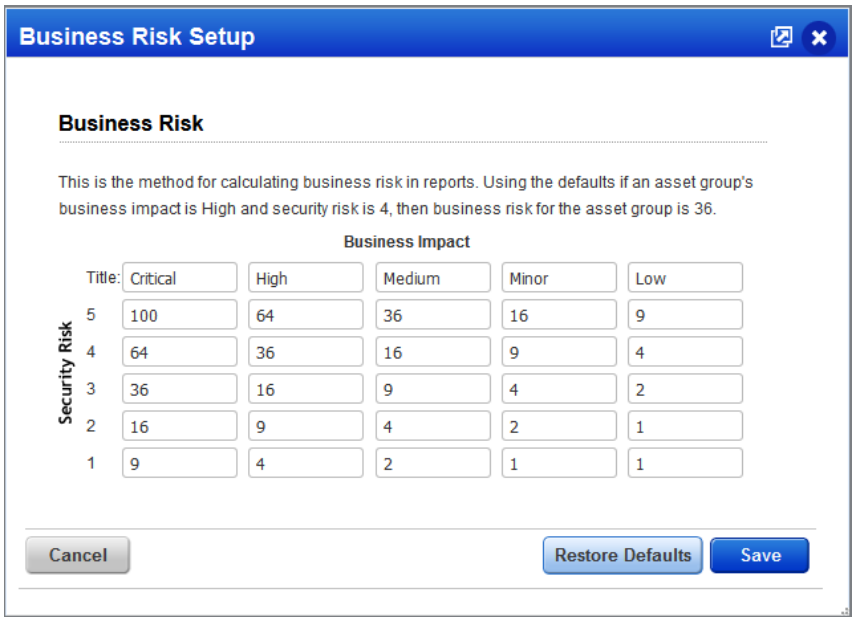
Configuring Business Risk

The Executive Report (and templates you might create) have a metric called "Business Risk."



Business Risk is the product of the "Average Security Risk" and the rating set by the Asset Group's "Business Impact." Let's take a look at how the weights are calculated.

Choose "Business Risk" from the "Setup" tab under the "Reports" section.

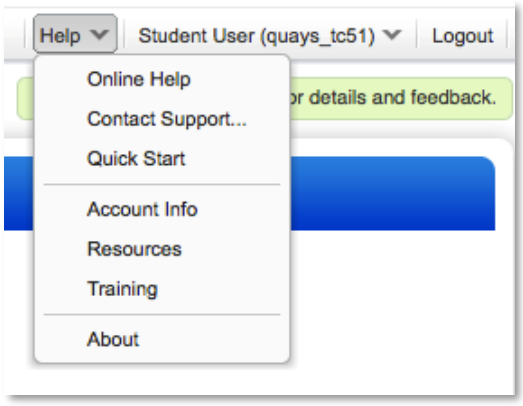


These are the default values for Business Risk. As you can see, a level 5 vulnerability on a host whose Asset Group is of "Critical" importance is weighted 100 times greater than that of a level 1 vulnerability on a host whose asset group is of "Low" importance.

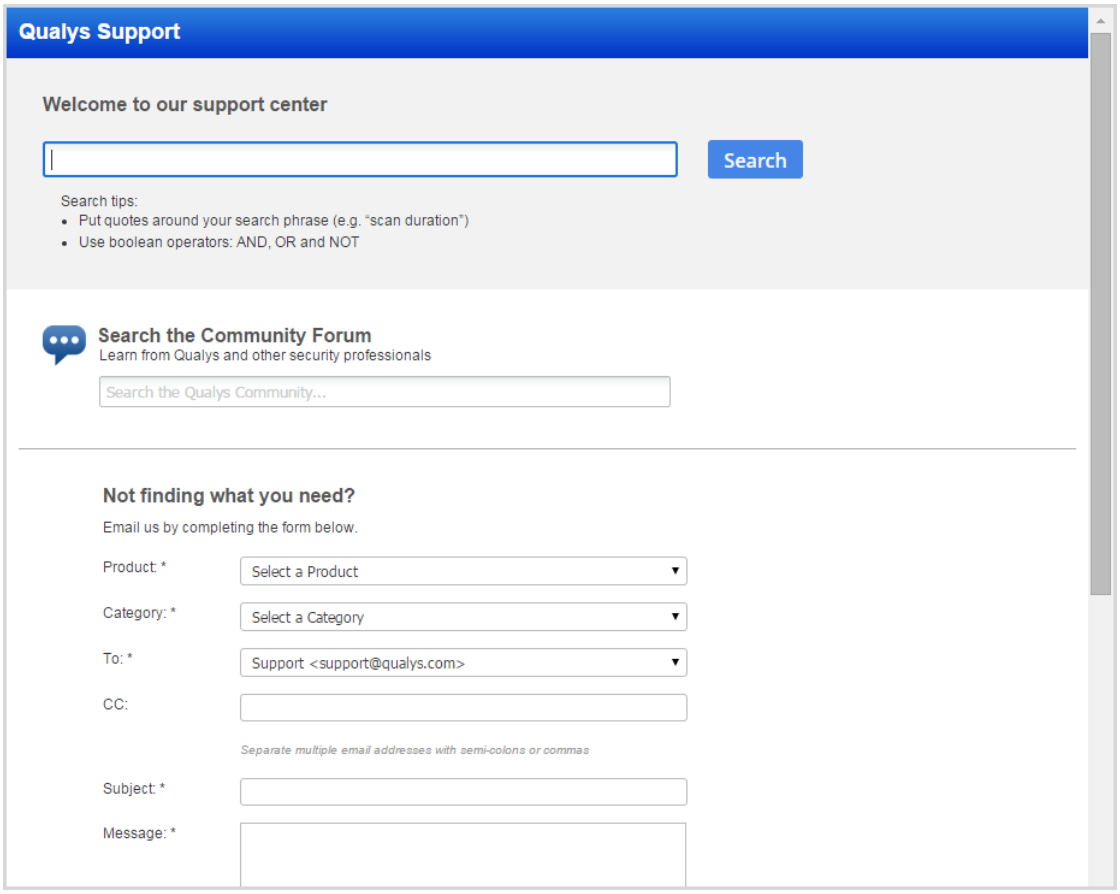
Appendix C: Contacting Support

Overview

With the Qualys interface, you will have all the necessary information at your fingertips. From the Qualys User Interface, click on "Help" and then "Contact Support".



You'll see our support center where you can find answers to your questions, learn from Qualys and other security professionals at our Community, submit support tickets. Scroll down to see our phone list with support contact numbers for your region.



So then, the question becomes – what information do you need to send to Qualys? Well, that can depend on the type of problems you are seeing.

False Positive

If you believe that you have identified a false positive, please provide us with additional information so that we can resolve the issue as quickly as possible.

Please provide the following in this message:

- Reasons you believe you have a false positive. Include steps you've taken to patch the system.
- Was the issue reported during an authenticated scan? If yes, was the authentication successful? There are several appendices in your scan results that provide information related to authentication.
- When was the vulnerability first detected? Have there been changes to the host since then?
- For publicly-facing IPs, we can greatly expedite the investigation if we can perform a light scan on the host. Do you grant permission for us to scan the host?

After receiving a ticket number from Support, send a follow-up email referencing the ticket number and attach the following items:

- A scan report with the vulnerability reported.
- A packet capture of traffic to/from the affected service/port for its typical communications. (only if requested by DEV)
- System configuration information. For Windows, this is provided by systeminfo.exe and MSinfo32.exe.
- Additional information, such as a registry dump or a screenshot of the system showing that it is patched and not vulnerable.

False Negative

On very rare occasions we may produce a False Negative. If you believe this to be the case, please provide the following in your message:

- IP address, DNS hostname or NetBIOS hostname for the host.
- QID, if available, for the potential false negative.
- Reasons you believe you have a false negative. Include steps taken to troubleshoot the issue.
- When was the vulnerability last detected? Have there been changes to the host since then?
- For publicly-facing IPs, we can greatly expedite the investigation if we can perform a light scan on the host. Do you grant permission for us to scan the host?

After receiving a ticket number from Support, send a follow-up email referencing the ticket number and attach the following items:

- A scan report of the scan that did not identify the vulnerability.
- Additional information, such as a registry dump or screenshot of your system.

Service Stopped Responding

This type of issue can have several causes, and rarely is caused by a test we have sent. Nevertheless, we need to determine what has happened and help expedite resolution. Quite often, resolution does require the vendor of the service to be involved in our troubleshooting effort.

Please provide the following in this message:

- A description of the symptoms. When did the issue first appear? If the issue is reproducible, please provide steps to reproduce the issue.
- Detailed information for each affected system, including: operating system version and patch level, IP address, the system's primary function and the location of the system on the network (i.e. behind a firewall, in DMZ or behind a load balancer.)
- Detailed information for each affected service, including: software name, exact version and build or patch level, the port number that the affected service is running on and whether the port is static or dynamic.
- For publicly-facing IPs, we can greatly expedite the investigation if we can perform a light scan on the host. Do you grant permission for us to scan the host?

After receiving a ticket number from Support, send a follow-up email referencing the ticket number and attach the following items:

- A scan report of the scan that caused the service to stop responding.
- A packet capture of traffic to/from the affected service/port for its typical communications.
- A list of open ports and services running on those ports.
    - # On a Windows system, you can run the free tcpview.exe and save the output. This program is available at:http://www.sysinternals.com/ntw2k/source/tcpview.shtml
    - # On a Linux system, you can run netstat -ntulp and save the output.
- An image of the box is useful to help us reproduce the issue. For Windows machines, images may be created using MS Virtual PC (free). For *nix, VMWare may be used. If the host has custom software on it, then please also provide us with a copy of the software.
- Additional information, such as screenshots and log files.

Scanner Appliance Issues

Before submitting a request to Support, please see the Qualys Scanner Appliance User Guide for troubleshooting information. The user guide describes troubleshooting techniques you can use to respond to errors and performance conditions when using the Scanner Appliance.

If you have followed the troubleshooting techniques and are still experiencing difficulty, please provide us with additional information so that we can resolve the issue as quickly as possible.

Please provide the following in this message:

- The error message on the LCD display of the Scanner Appliance.
- The IP configuration for the LAN interface (static or DHCP). For static configurations, include the IP address, netmask, gw, dns1, dns2, wins and domain.

- If WAN is enabled, provide the IP configuration for the WAN interface. For static configurations, include the IP address, netmask, gw, dns1, dns2, wins and domain.
- If proxy is enabled, identify the proxy software and list the proxy configuration. Indicate whether a username and password is used but do not send us the password.
- How long is the timeout from when you hit Enter on "Really enable.." to when the "Network Error" message appears?
- When you use a laptop with the same network configuration on the same network port, are you able to connect to the Qualys service at https://qualysguard.qualys.com?

Host Crash

Qualys scans are generally non-intrusive. If a scan has caused a host to crash then we will make resolving this issue a top priority. We are eager to work with you and any third-party vendors to quickly isolate and resolve the problem.

Please provide the following in this message:

- A description of the symptoms. When did the issue first appear? If the issue is reproducible, please provide steps to reproduce the issue.
- Detailed information for each affected system, including: operating system version and patch level, IP address, the system's primary function and the location of the system on the network (i.e. behind a firewall, in DMZ or behind a load balancer.)
- For publicly-facing IPs, we can greatly expedite the investigation if we can perform a light scan on the host. Do you grant permission for us to scan the host?

After receiving a ticket number from Support, send a follow-up email referencing the ticket number and attach the following items:

- A scan report of the scan that resulted in the host crash.
- A packet capture of traffic to/from the affected service/port for its typical communications.
- A list of open ports and services running on those ports.
    - On a Windows system, you can run the free tcpview.exe and save the output.
    - *On a Linux system, you can run netstat -ntulp and save the output.*
- An image of the box is useful to help us reproduce the issue. For Windows machines, images may be created using MS Virtual PC (free). For *nix, VMWare may be used. If the host has custom software on it, then please also provide us with a copy of the software.
- Additional information, such as screenshots and log files.