Vulnerability Management Detection & Response (VMDR)

Lab Tutorial Supplement

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of 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 Scannable Host Assets* tutorial:

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

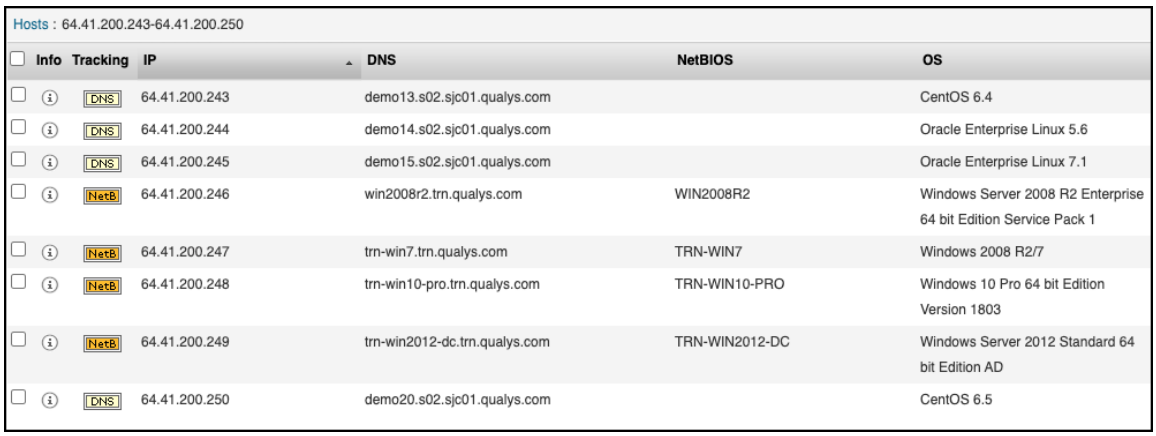
The Linux-based hosts in the Qualys Training Lab are configured to track vulnerabilities by host DNS name.

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.

Sensors To Produce Vulnerability Findings

Qualys Sensors provide the most comprehensive approach to collecting all your asset and software inventory data. This lab provides an overview of the various Qualys Sensors, with particular attention given to the Qualys Cloud Agent

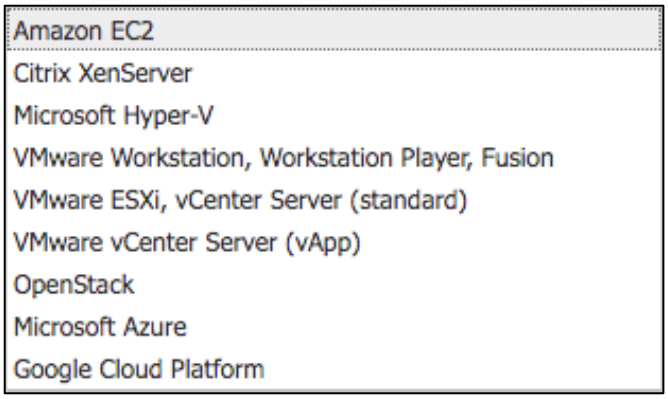
Scanner Appliance

Qualys Scanner Appliances are available in three different varieties: 1) Internet-based appliances located within the Qualys Cloud Platform, 2) Physical appliances, and 3) Virtual Appliances.

Any Qualys user with scanning privileges can access Qualys' pool of Internet-based Scanner Appliances. These appliances are ideal for targeting and scanning other Internet-facing assets.

Qualys physical and virtual scanner appliances can be deployed throughout your business or enterprise architecture.

Virtual scanner appliances are available for multiple virtualization platforms:

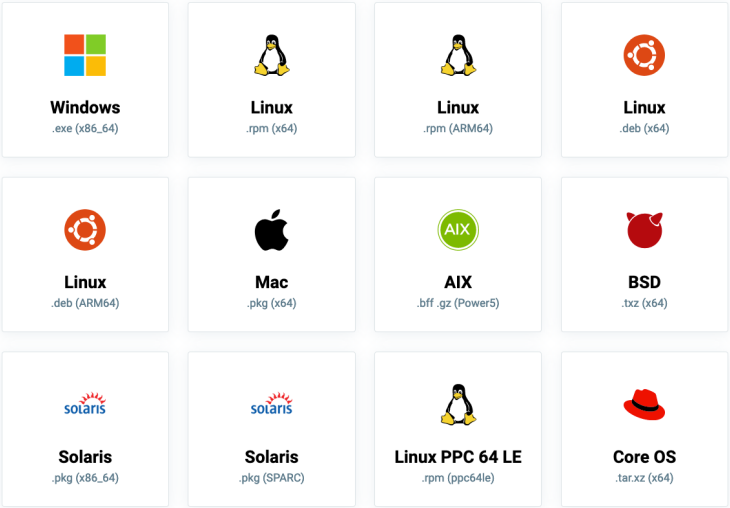


For a detailed discussion of Scanner Appliance deployment and usage, please see the "Scanning Strategies and Best Practices" training course (qualys.com/learning).

Cloud Agent

Qualys Cloud Agents install locally on the host assets they protect, sending all collected data to the Qualys Cloud Platform for analysis.

Qualys agents presently support Windows, Mac, Linux, and Unix-based operating systems.



For a complete list of supported operating systems, see the "Platform Availability Matrix" within the Cloud Agent Getting Started Guide:

https://www.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf

Configure Agents for VMDR

Qualys Cloud Agent supports multiple VMDR applications:

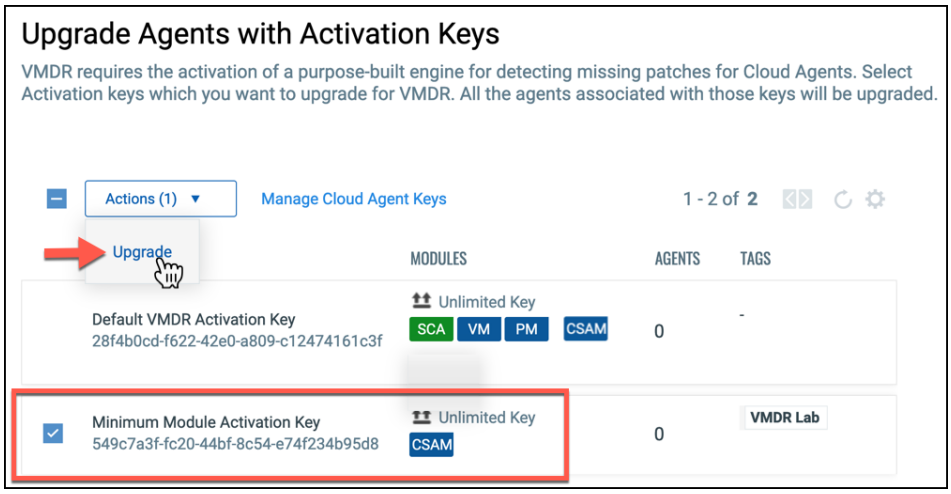
- CyberSecurity Asset Management (CSAM)
- Vulnerability Management (VM)
- Security Configuration Assessment (SCA) / Policy Compliance (PC)
- Patch Management (PM)

These supported application modules must be activated for your VMDR host assets. Activation Keys allow you to manage and control the distribution of agents throughout your organization.

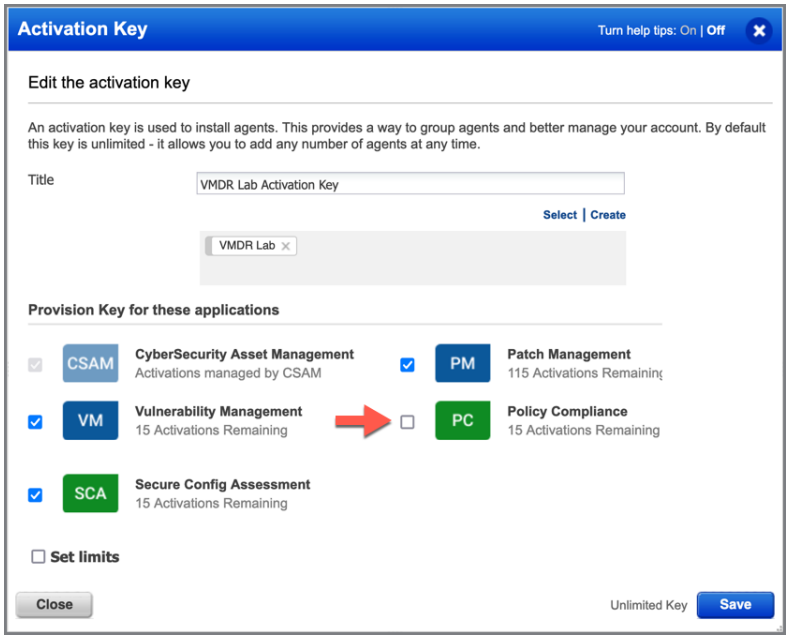
Click the following URL to view the *Build an Activation Key* tutorial:

PLAY https://ior.ad/8Wyj

Activation Keys can be configured from the Cloud Agent application or the VMDR "Welcome" page.



Upgrade Activation Keys to include the CSAM, VM, SCA, and PM application modules.



While VMDR includes the "Security Configuration Assessment" module (by default), agent Activation Keys can be updated to include Policy Compliance (PC) instead of SCA.

For a detailed discussion of agent installation and configuration steps, see the "Cloud Agent" training course (https://qualys.com/learning).

Agent Installation Components

While this lab tutorial highlights the components of a Windows Agent installation, the basic principles and concepts apply equally to other agent-supported OS installations. You'll find specific instructions for Mac OS installations, RPM-based OS installations, and Debian/Ubuntu OS installations in Appendix A, B, and C, respectively.

The installation steps that follow support Windows XP SP3 or greater. Older versions of Windows that do not support TLS 1.2 will need to connect to the Qualys Cloud Platform through a proxy or the Qualys Gateway Service (QGS).

To successfully perform a Cloud Agent installation, you must have administrative access to the target Windows host.

Click the following URL to view the *Obtain Agent Requirements* tutorial:

PLAY https://ior.ad/8Wye

Installing an Agent

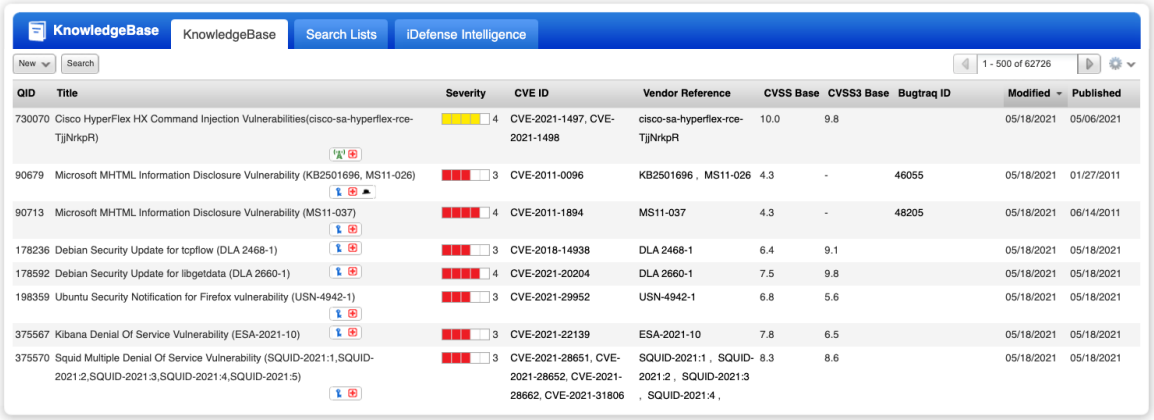
- Open a "Command Prompt" window on a target Windows host.
- Navigate to the directory that contains the Cloud Agent installation program (QualysCloudAgent.exe).
- Use the "dir" command to verify the existence of the installation program file. If you do not see the file "QualysCloudAgent.exe" navigate to its correct location before executing the installation command.
- Copy and paste the Cloud Agent installation command into the "Command Prompt" window and press the "Enter" key. The Agent installation program will execute with your Activation Key and Customer ID.

Click the following URL to view the *Install Agent* tutorial:

https://ior.ad/8Wyd

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 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:

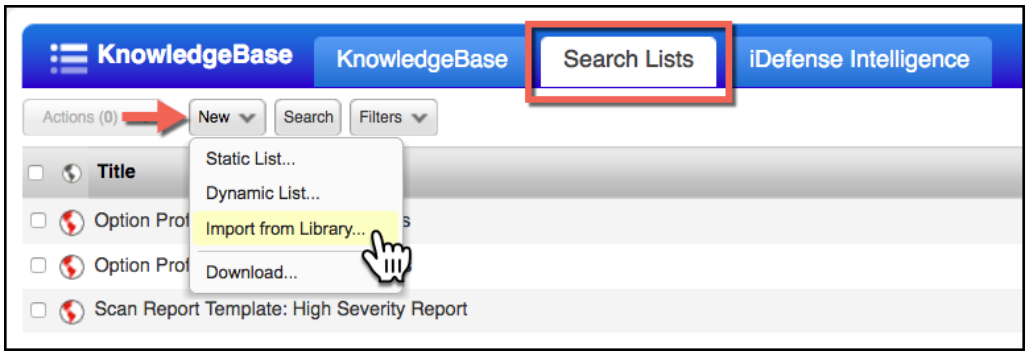
- Build a report to focus on specific vulnerabilities.
- Launch a scan that targets a specific type or group of vulnerabilities.
- Build a Remediation Policy to automatically assign or ignore vulnerabilities.

Navigate to the following URL to view the *Creating a Search List* tutorial:

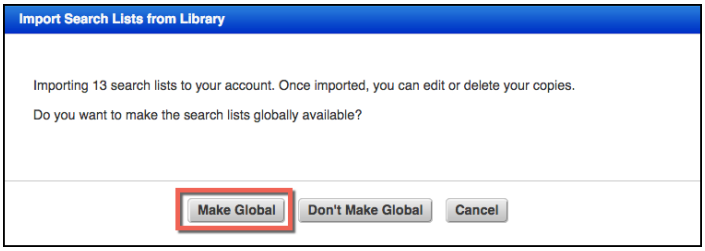
https://ior.ad/7ecF

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.

Qualys TruRisk

Qualys VMDR 2.0 offers an all-inclusive risk-based vulnerability management solution to prioritize vulnerabilities and assets based on risk and business criticality.

Use Cases

- Reduce Risk with Holistic Scoring – Quantify risk across the entire attack surface, including vulnerabilities, misconfigurations, and digital certificates, correlate with business criticality, and exploit intelligence from hundreds of sources, including Shodan's attack surface exposure data. Qualys VMDR with TruRisk automatically de-prioritizes vulnerabilities if compensating controls are in force, tracks risk reduction trends over time, and helps organizations measure and report on the effectiveness of their cybersecurity program across hybrid environments.
- Quickly Remediate at Scale – Leverage rule-based integrations between VMDR and ITSM tools such as ServiceNow and JIRA, along with dynamic vulnerability tagging, to automatically assign remediation tickets to prioritize vulnerabilities and bridge the gap between security and IT teams. Orchestrate remediation directly from the ITSM tool to help close vulnerabilities faster and reduce the mean time to remediation.
- Receive Preemptive Attack Alerts – External threat intelligence, from more than 180,000 vulnerabilities and 25 plus threat and exploit intelligence sources, is natively correlated with vulnerabilities and misconfigurations to proactively alert teams on vulnerabilities exploited by malware or those used in an active malicious campaign known to target your industry.
- Automate Operational Workflows – Teams save valuable time and resources with Qualys QFLOW technology. They can develop visual workflows to automate time-consuming and complex vulnerability management tasks, such as vulnerability assessments for ephemeral cloud assets, alerting for high-profile threats, or quarantining high-risk assets.

Asset Criticality Score (ACS)

Criticality is assigned to each Asset Tag. The Asset Criticality value will be the highest value of the assigned tags, or Business Criticality, to the asset. A value of 5 represents the most critical.

Example ACS Queries

Show assets with criticality scores of 4 and 5:

```
criticalityScore:[4,5]
```

A default value of 2 is assigned to assets without an assigned criticality score.

Show assets that do not have an assigned criticality score:
criticalityScore is null

Qualys Detection Score (QDS)

The QDS is an integer value 0-100. It provides a valuable metric for measuring the impact of a single vulnerability.

It is derived from the following:

- Vulnerability technical details (the CVSS base score)
- Vulnerability temporal details (Is this vulnerability associated with ransomware? Is the exploit code mature? Is it associated with malware? Is this trending on the dark web?)
- Vulnerability remediation details (Has the vendor released a patch?)
- If multiple CVEs contribute to a QID, the CVE with the highest score is considered for the QDS calculation.

The levels are as follows:

- Critical: 90-100
- High: 70-89
- Medium: 40-69
- Low: 1-39

Examples of QDS Queries

Show vulnerabilities with a detection score equal to 80:
vulnerabilities.detectionScore:80

Show vulnerabilities with a detection score greater than 80:
vulnerabilities.detectionScore > 80

Show vulnerabilities with Medium or High scores:
vulnerabilities.detectionScore:[40 .. 89]

TruRisk Score

The TruRisk Score is an integer value 0-1000. The score combines the Criticality Score of a single host with a weighted average of its combined vulnerability detections. The TruRisk score places the vulnerability in the context of other vulnerabilities discovered on the same host.

The following formula is used to calculate the TruRisk score:

Risk Score = ACS * {wc(Avg(QDSc)) + wh(Avg(QDSh)) + wm(Avg(QDSm)) + wl(Avg(QDSl))}

Examples TruRisk Queries

Show assets with risk scores greater than 850 and less than 1000:

riskScore:(850 .. 1000)

Show assets with risk scores greater than or equal to 850 and less than 1000:

riskScore:[850 .. 1000)

Show assets with risk scores greater than 850 and less than or equal to 1000:

riskScore:(850 .. 1000]

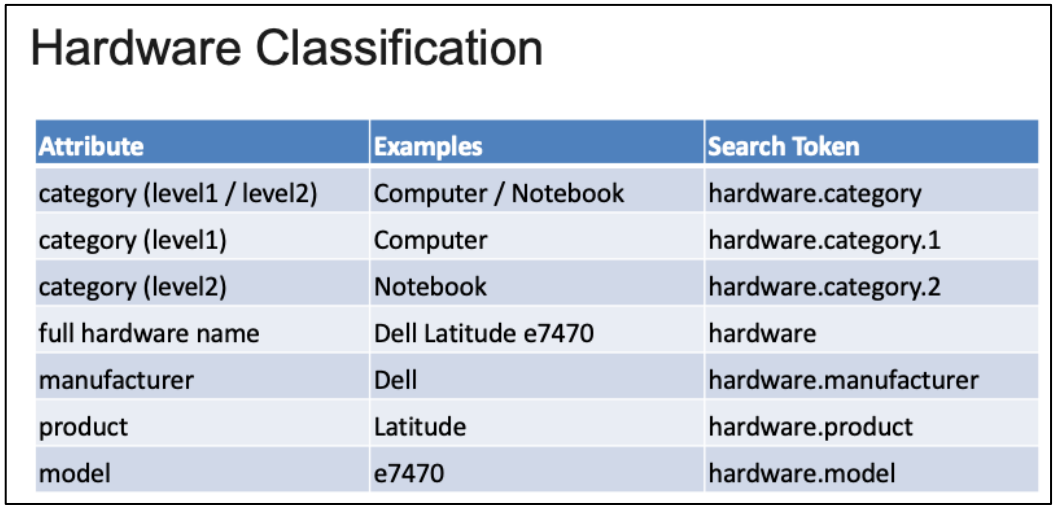
Click the following URL to view the *Qualys TruRisk Scoring* tutorial:

https://ior.ad/8AGe

Normalization & Categorization of Sensor Data

Qualys sensors populate the Cloud Platform with inventory, vulnerability, threat, compliance, cloud, and web app data. This gives you your data in one place. Global AssetView (GAV) and CyberSecurity Asset Management (CSAM) aggregate and correlate the data gathered by all Qualys sensors giving you a comprehensive, detailed inventory of all your hardware and software, as well as a multi-dimensional view of your global, hybrid IT environment.

Qualys provides Level 1 and 2 categories for Hardware, Operating Systems, and Software Application assets.



Hardware Classification

Attribute	Examples	Search Token
category (level1 / level2)	Computer / Notebook	hardware.category
category (level1)	Computer	hardware.category.1
category (level2)	Notebook	hardware.category.2
full hardware name	Dell Latitude e7470	hardware
manufacturer	Dell	hardware.manufacturer
product	Latitude	hardware.product
model	e7470	hardware.model

The table (above) provides some useful examples of “hardware” tokens.

To view all of the hardware categories in your account, group assets by hardware category (i.e., INVENTORY > Assets > Group Assets by… > Hardware > Category).

Operating System Classification

Attribute	Examples	Search Token
category (level1 / level2)	Windows, Unix, Linux, Mac, ...	operatingSystem.category
category (level1)	Windows	operatingSystem.category.1
category (level2)	Client	operatingSystem.category.2
full operating system name	Windows 7 Enterprise (6.1 SP2) 64-Bit	operatingSystem
publisher	Microsoft	operatingSystem.publisher
name	Windows 7	operatingSystem.name
architecture	64Bit	operatingSystem.architecture
market version	7	operatingSystem.marketVersion
version	6.1	operatingSystem.version
update	SP2	operatingSystem.update
edition	Enterprise	operatingSystem.edition

The table (above) provides some useful examples of "OS" tokens.

To view all of the OS categories in your account, group assets by operating system category (i.e., INVENTORY > Assets > Group Assets by… > Operating System > Category).

Software Classification

Attribute	Examples	Search Token
type	Application, Driver, OS Update, Unknown	software.type
category (level1 / level2)	Productivity > Productivity Suites	software.category
category (level1)	Productivity	software.category.1
category (level2)	Productivity Suites	software.category.2
full software name	Microsoft Office 2016 (16.0.1.2) Professional 64-Bit	software.name
publisher	Microsoft	software.publisher
product	Office	software.product
architecture	64-Bit	software.architecture
market version	2016	software.marketVersion
version	16.1	software.version
update	16.1.1.2	software.update
edition	Professional	software.edition

The table above provides some useful examples of "software" tokens.

To view all of the software categories in your account, group software by software category (i.e., INVENTORY > Software > Group Software by… > Category).

Example Queries

To build a dynamic tag for Windows-based systems, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category1:'Windows'
```

To build a dynamic tag for “Server” host assets, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category2:'Server'
```

To build a dynamic tag for Windows Servers, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category:Windows / Server
```

The first value (Windows) is separated from the second value (Server) by the slash (“/”) symbol.

Click the following URL to view the *Search Using Categories* tutorial:

https://ior.ad/7Uue

Asset Tags and Asset Groups

There are many ways to organize the host assets within your Qualys subscription, including geographic location, service or function, device type, operating system, asset owner, IP address range (netblock), and more.

Although the methods listed above are common, you may choose other grouping or labelling methods that are unique to your company or organization.

The proper use of Asset Groups and Asset Tags will allow you to effectively organize and manage host assets. Asset Groups and Asset Tags can be combined to accomplish numerous objectives, such as:

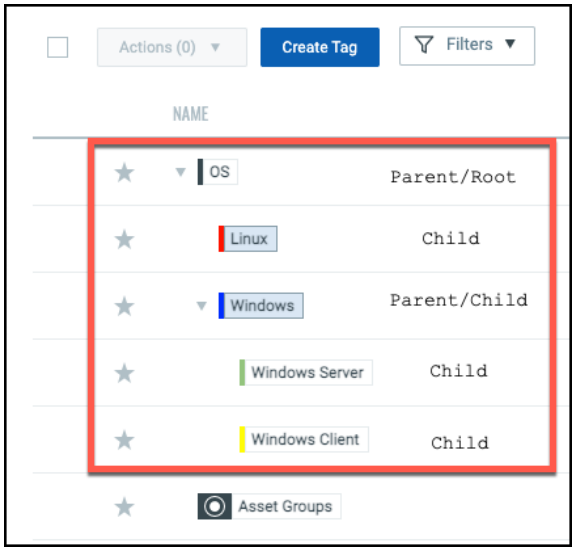
- Creating targets for scanning, reporting, and remediation.
- Assigning access privileges to user accounts.
- Host identification and inventory management.

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.

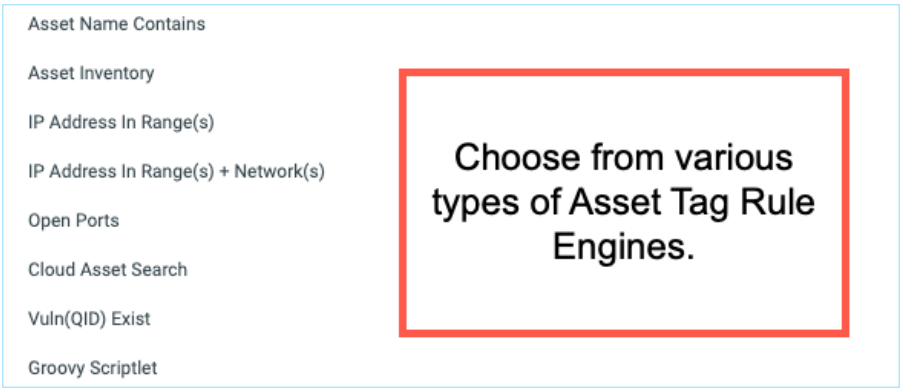


Many tag hierarchies begin with a static “parent” that serves as a “placeholder” for its dynamic “child” tags. Tags located at higher levels of the hierarchy reflect a broader scope of host assets, while tags at lower

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:

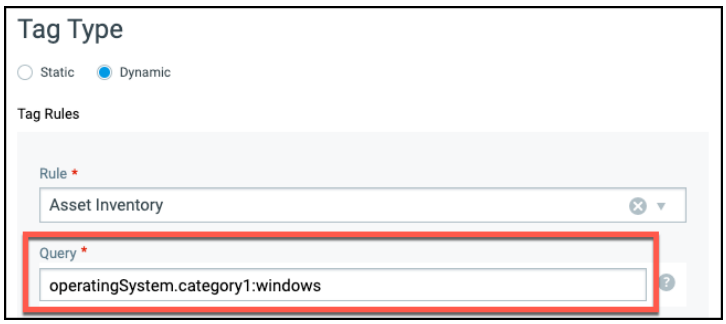
PLAY https://ior.ad/7emE



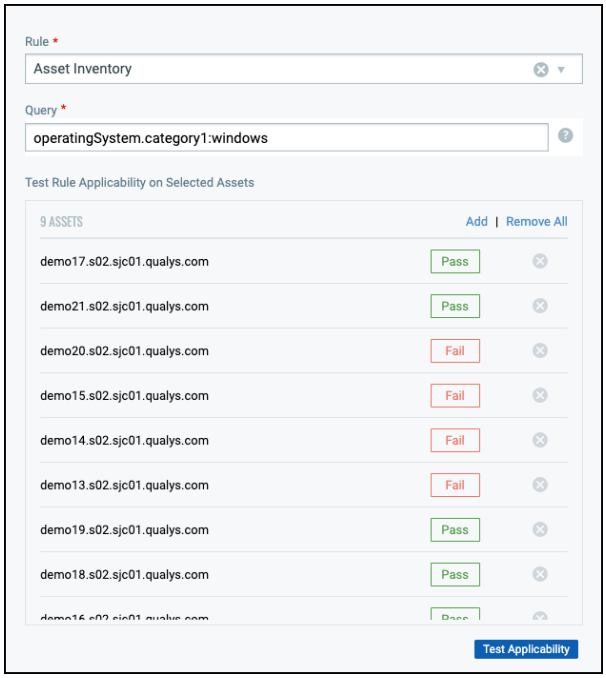
Dynamic Asset Tags are created using various types of Asset Tag Rule Engines. These tags are automatically updated as new information is received from Qualys Sensors.

Windows Tag

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

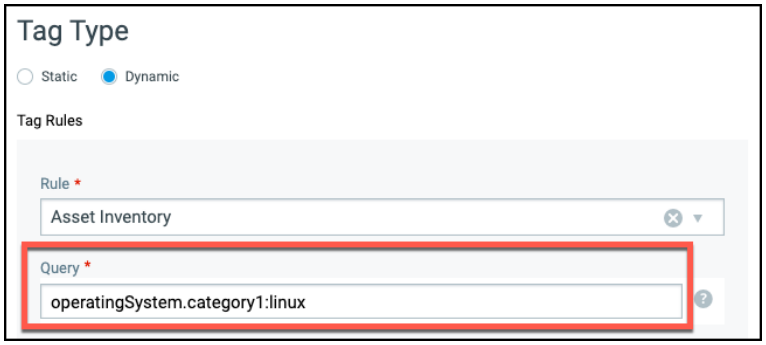


When testing your queries, hosts that meet the query conditions(s) will Pass, while all other hosts will Fail.

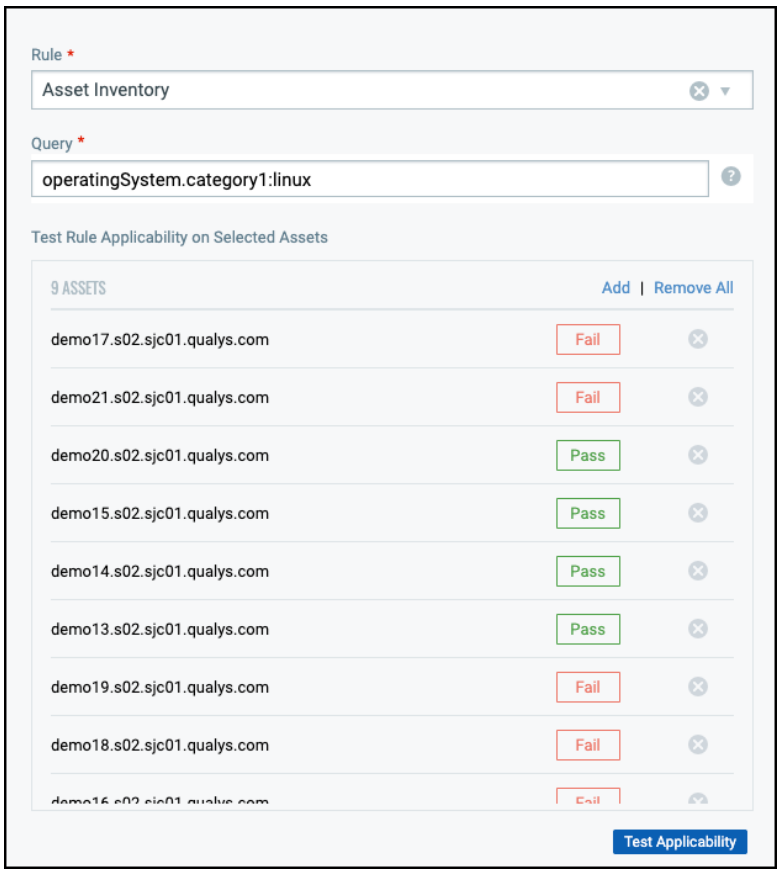


Linux Tag

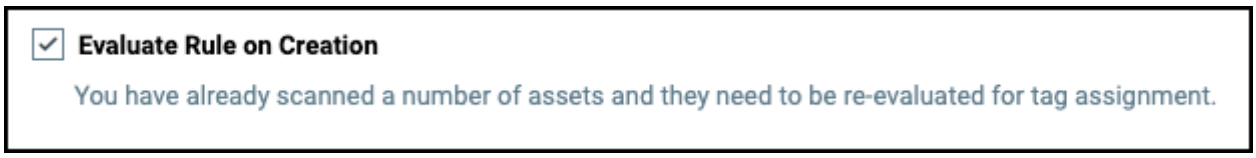
Linux hosts are easily tagged using the "Asset Inventory" rule engine and `operatingSystem` query token.



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



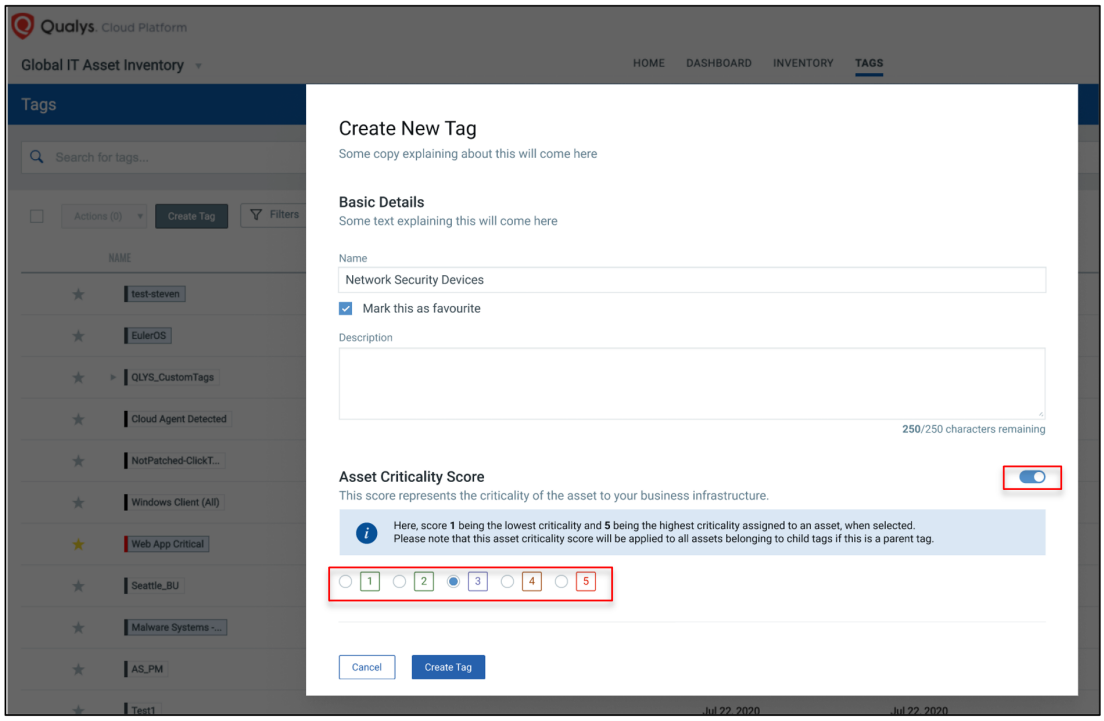
Using the “Evaluate Rule on Creation option (while building or editing a tag) will add the tag to host that have already been scanned.



Asset Tag Criticality

With GAV/CSAM, you can apply tags manually or configure rules for automatically classifying your assets in logical, hierarchical, business-contextual groups. And you can assign Asset Criticality through tags to establish asset priorities.

You can set the asset criticality score between 1 to 5. Score 1 is the lowest criticality, and 5 is the highest criticality assigned to an asset when selected.



Types of Tags where user can enable and assign Criticality Score or disable Criticality Score :

- Dynamic tag
- Static Tag
- IFA (Internet-facing asset tag)
- Asset groups

Asset Criticality Score

CSAM automatically calculates the Asset Criticality Score of an asset based on the highest aggregated criticality.

Example: Asset A1 has three tags attached with Criticality Scores as listed in the table.

Tag	Criticality Score
T1	2
T2	4
T3	*Null

So the Criticality Score for this asset is 4.

*Note that the tag criticality score for system tags will always be Null. We cannot assign any criticality to them. Example: Cloud Agent, Business Unit, etc.

Criticality for Asset Group Tags

Assets that are part of the current Business Criticality of Asset Groups in Qualys Vulnerability Management are mapped to their respective criticality levels.

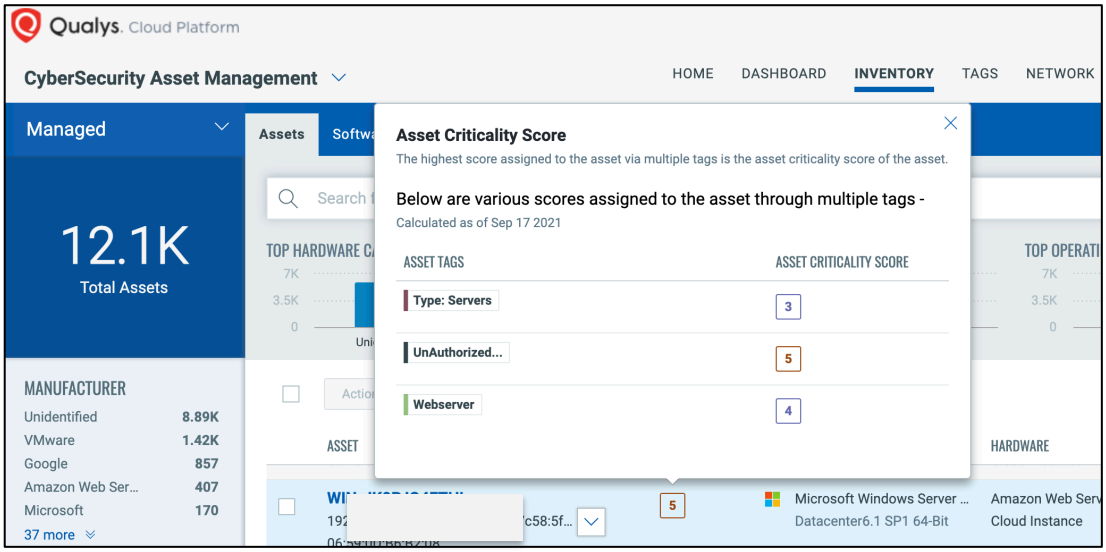
The following mapping is used:

1. Critical Business Group - Level 5 ACS
2. High Business Group - Level 4 ACS
3. Medium Business Group - Level 3 ACS
4. Minor Business Group - Level 2 ACS
5. Low Business Group - Level 1 ACS

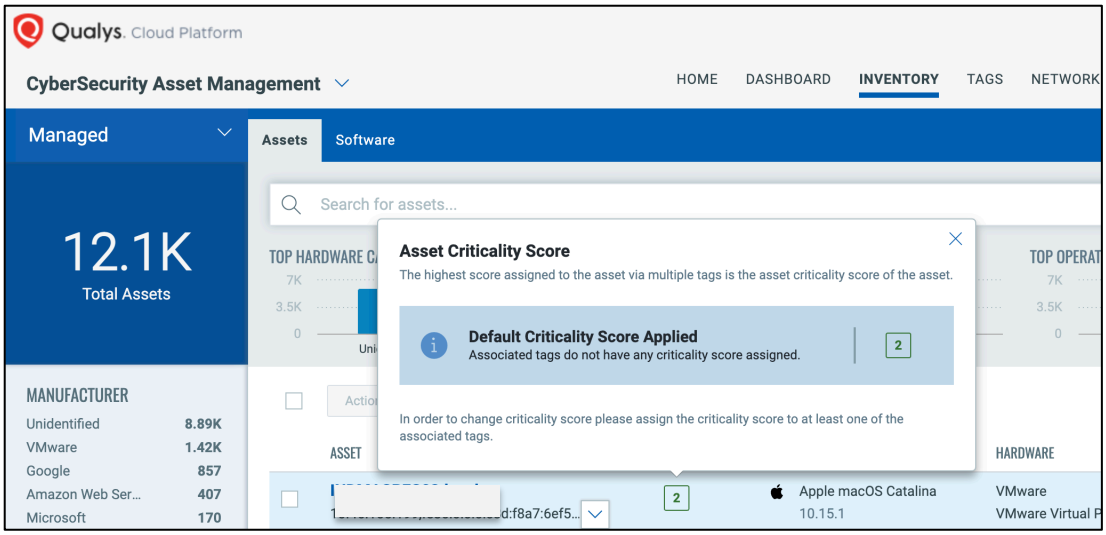
ACS = Asset Criticality Score

Inventory Asset List Page

The Asset Criticality Score for assets can be seen on the click of the score in the Inventory section.



The default criticality score for an asset is 2 (If there is no tag having a Criticality Score attached to it.)



In case the criticality score assigned to the tag is updated, like from 4 to 5, the Criticality Score for associated assets will be updated following the subsequent scan, in the event of a modification to the existing tag rule, when a new tag is assigned to an asset, or when a current tag is removed from the asset and on tag re-evaluation.

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:

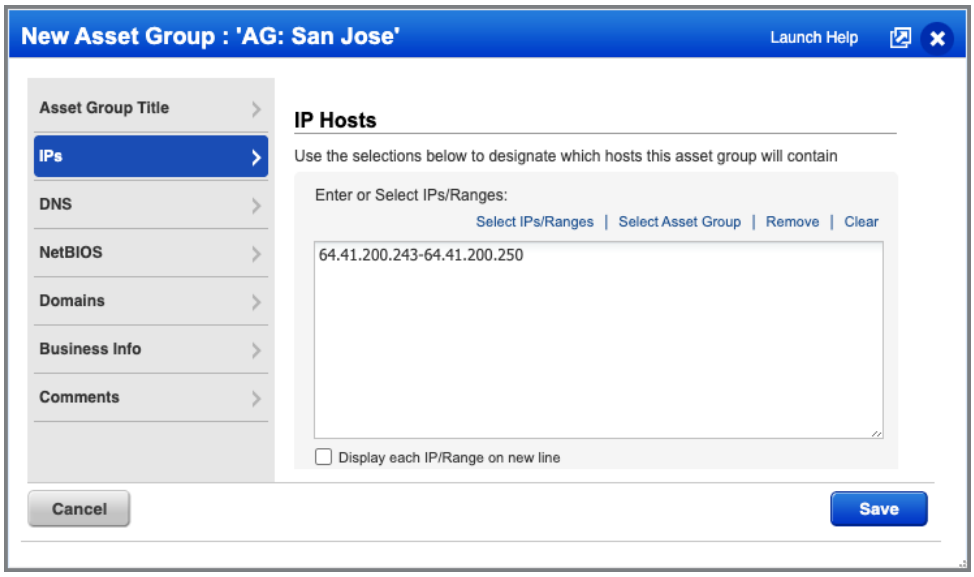
- Used to assign access privileges to user accounts.
- Contains a "Business Impact" setting that is used to calculate Business Risk.
- Can be used as a target for mapping, scanning, reporting, and remediation.
- A single host can be a member of multiple Asset Groups.
- Nesting one Asset Group inside 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:

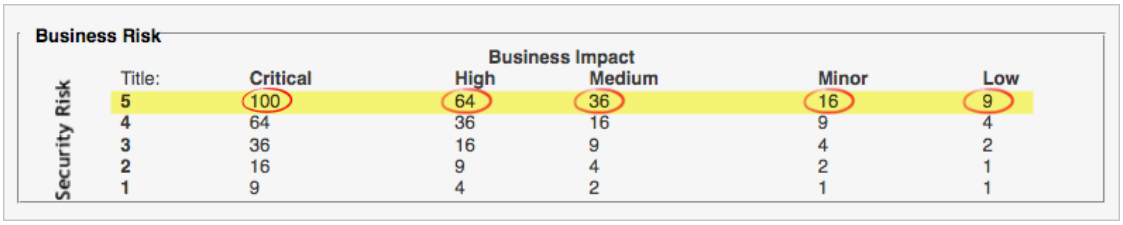
PLAY https://ior.ad/7eiB

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.



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.

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.

Authentication Records

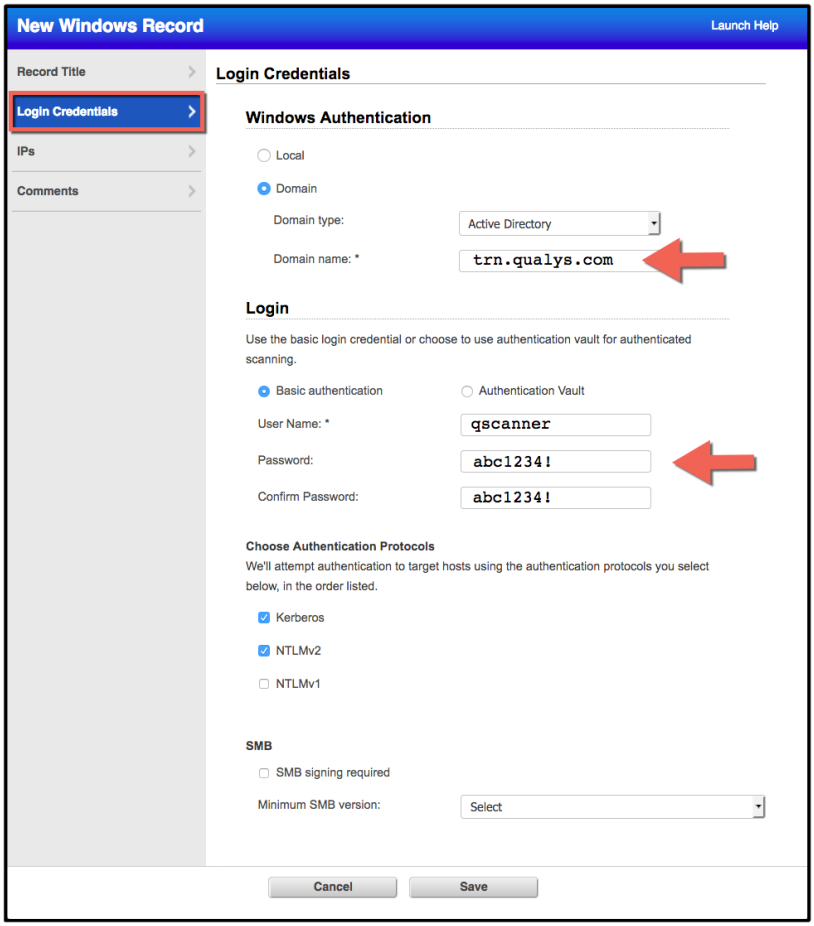
Performing a “trusted” scan requires one or more authentication records. Alternatively, a Qualys Scanner Appliance can use authentication credentials collect from multiple types of authentication vaults
In this exercise, you’ll create authentication records for the Window and Linux hosts in our training lab environment.

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

https://ior.ad/7ecH

Windows Authentication Record

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

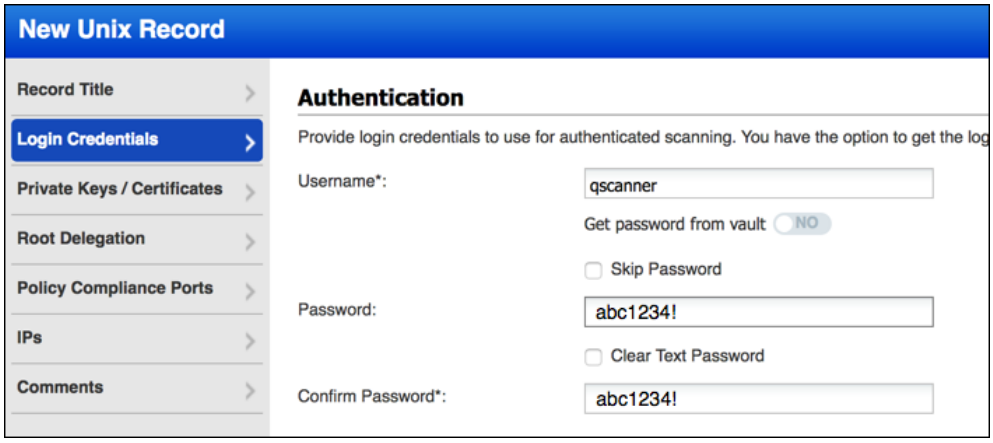


The “qscanner” user account is a member of the Domain Admins user group within the “trn.qualys.com” domain. At least on authentication protocol is required.

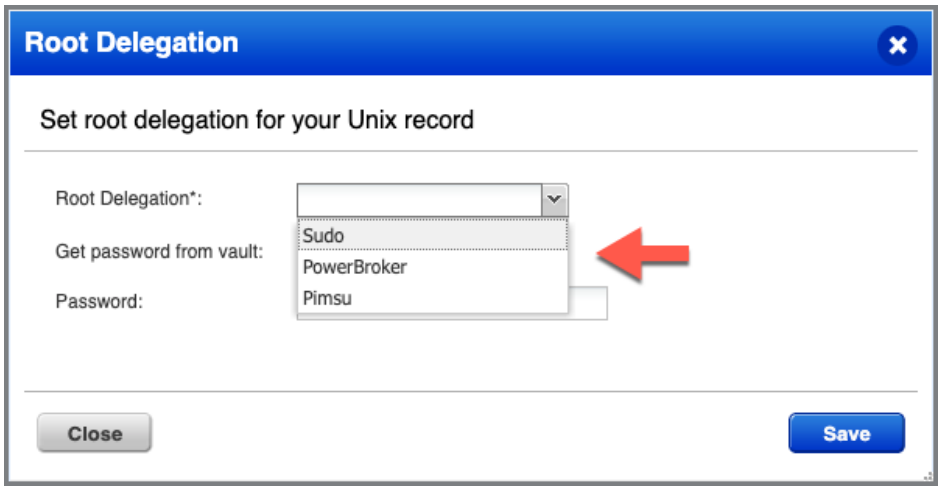
IP addresses are not required for Active Directory authentication records. This information will be collected at scan-time, from the Windows Domain service.

Unix Authentication Record

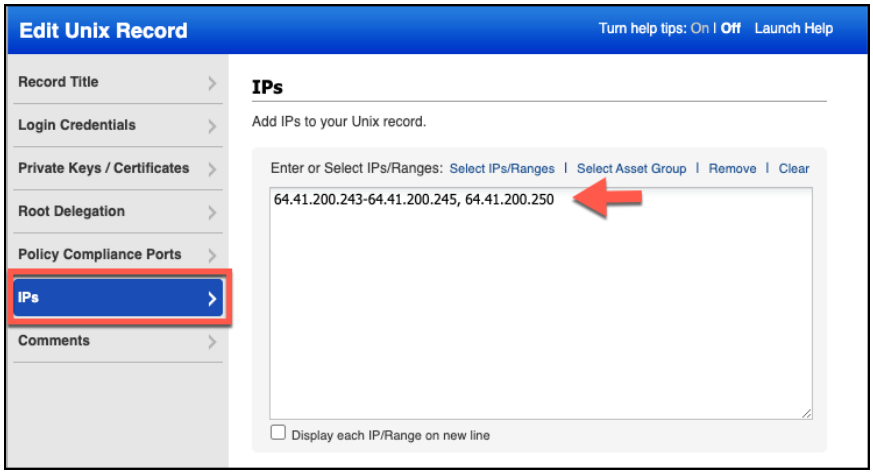
Unix authentications records can be created with a standard user account (avoid using the 'root' account).



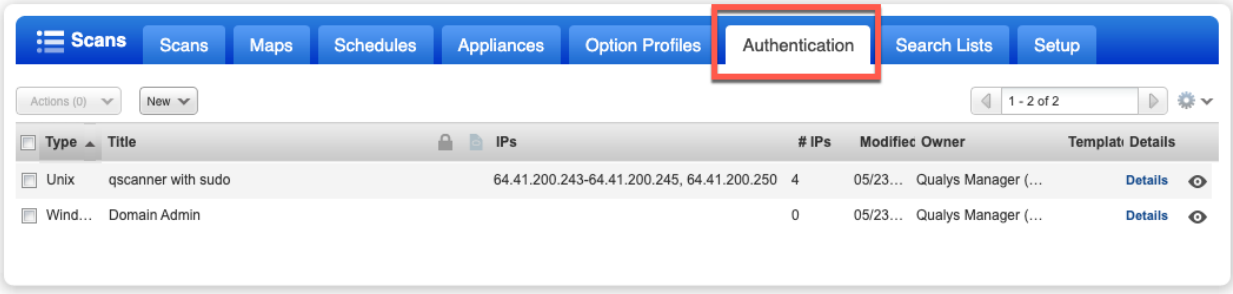
Root Delegation can then be used to provide elevated privileges to the scanning user account, via Sudo, PowerBroker or Pimsu.



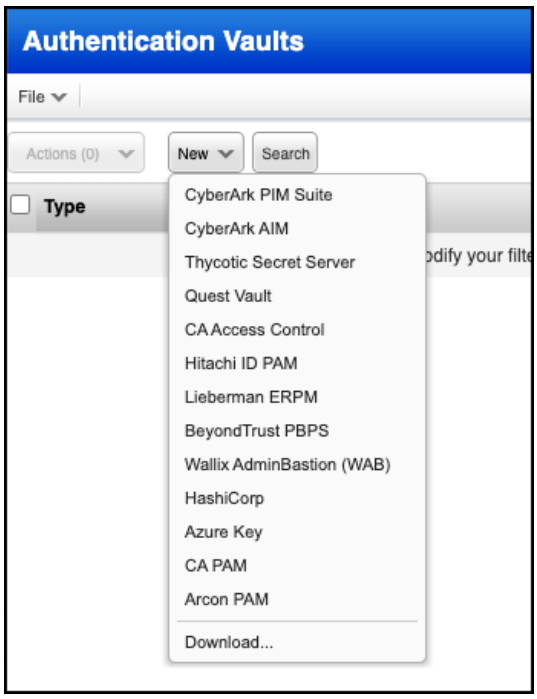
IP addresses are required for all Unix-based authentication records.



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.

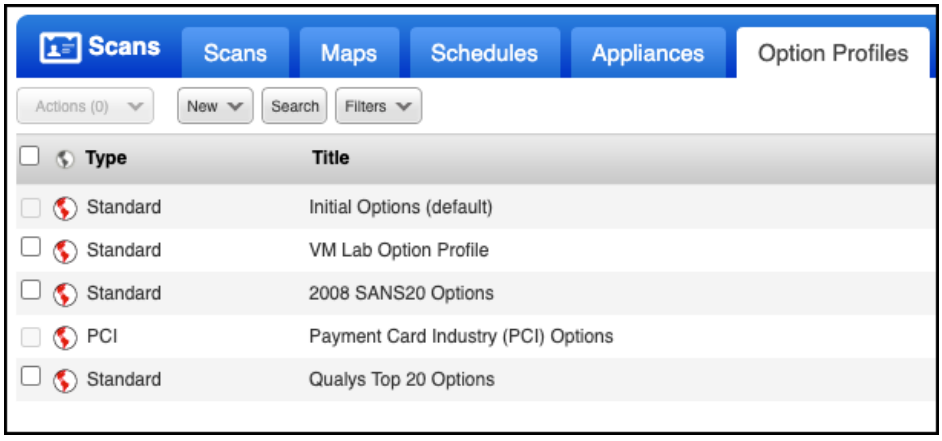
Option Profile

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

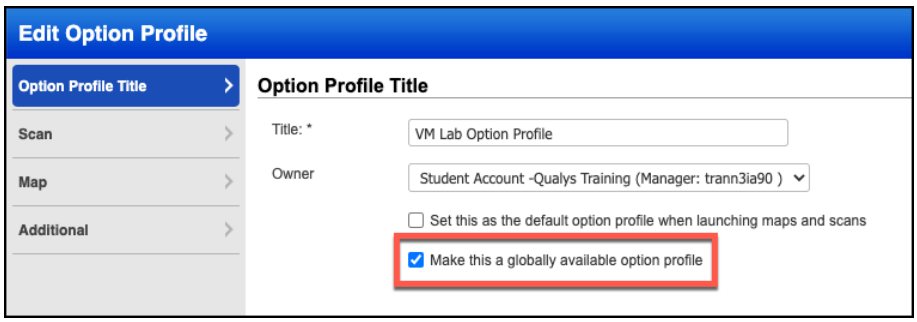
Navigate to the following URL to view the *Scanning Options* tutorial:

PLAY 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.

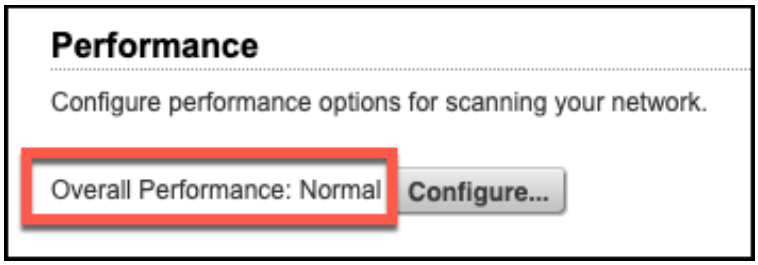
Make an Option Profile “global” to allow other Qualys users to see and use it.



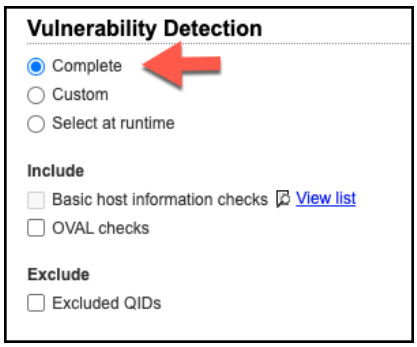
The “Standard Scan” port setting contains the most commonly used port numbers (about 1,900) found in a typical network environment.

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

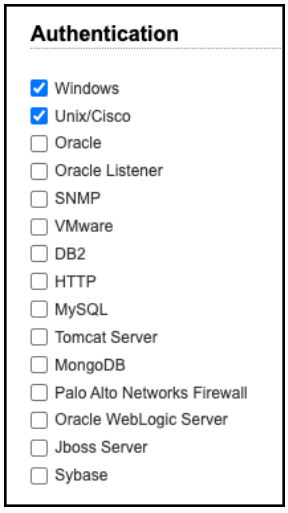
The preset configuration options for scan performance include High, Normal, and Low. A “Custom” setting is also available and will allow you to adjust individual performance settings and options.



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.

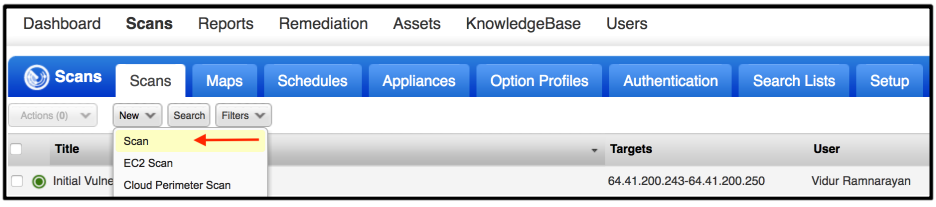


The lab targets in our training lab use both Windows and Unix authentication.

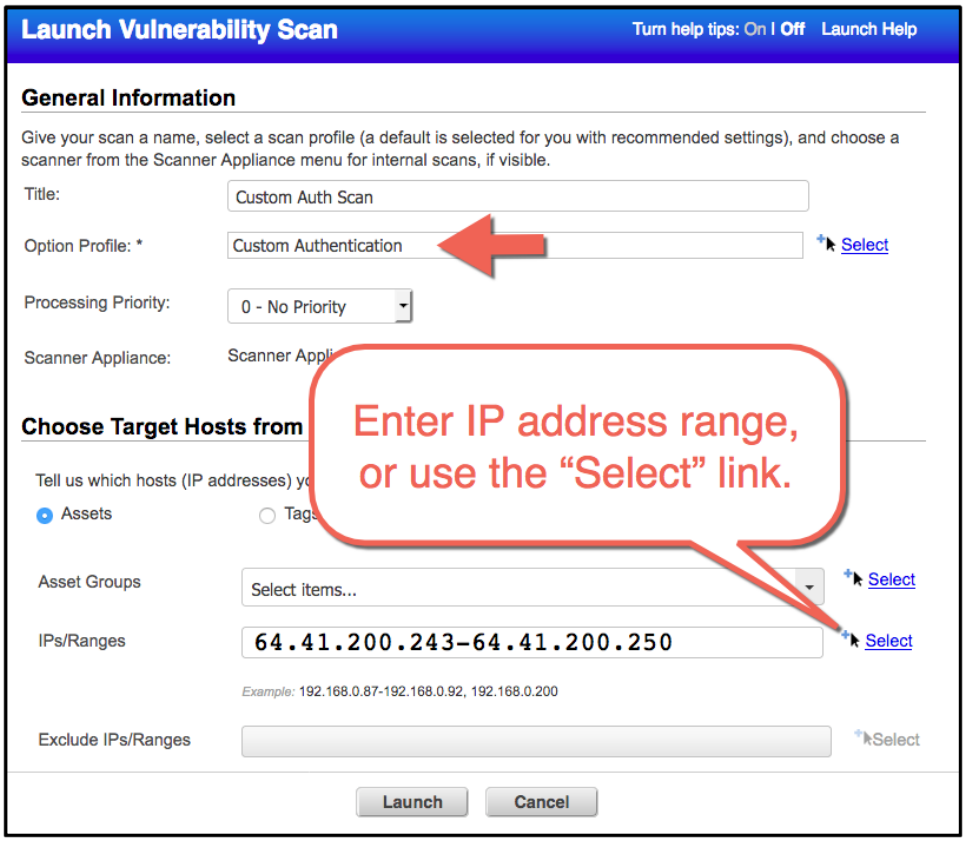
Launch Scan

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

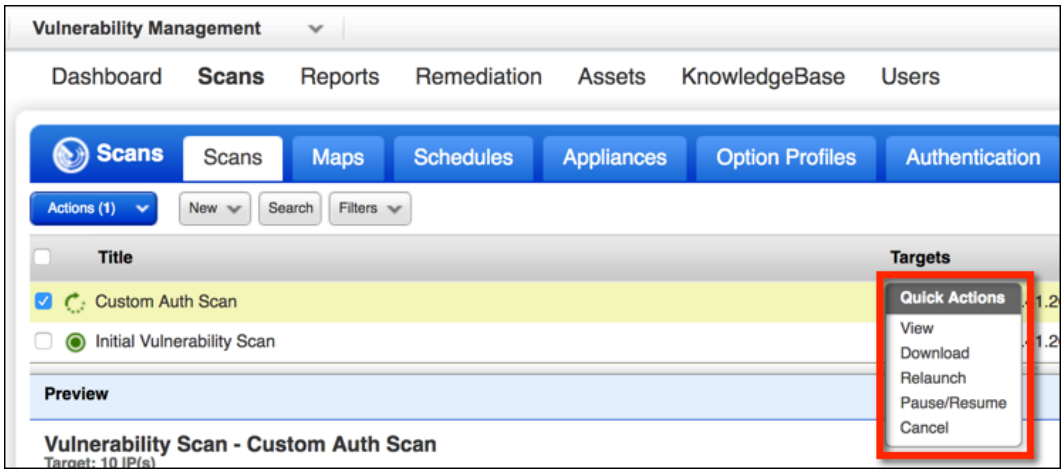
PLAY https://ior.ad/7edJ



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



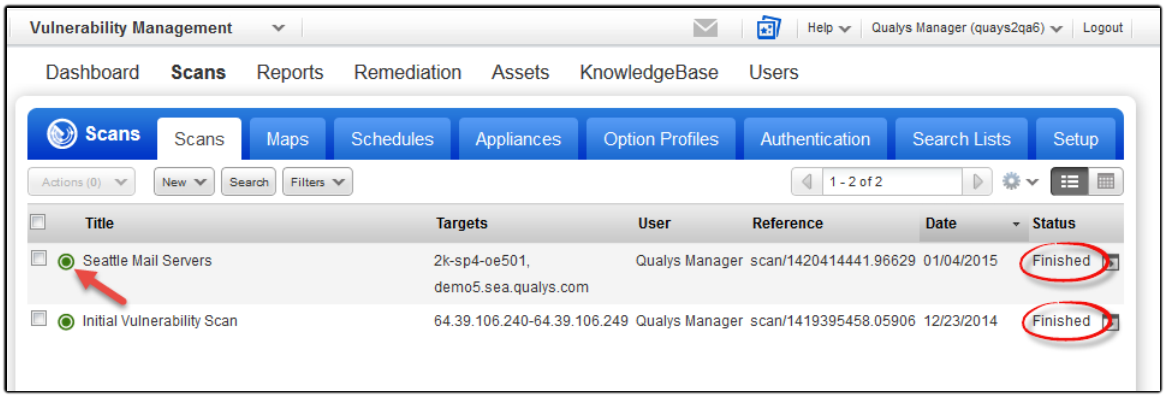
2. Enter the Title: Custom Auth Scan.
3. Select the "Option Profile" you just created (Custom Authentication).
4. In the "Choose Target Hosts from" section, enter the IP address range for all host IPs (64.41.200.243-64.41.200.250), or click the "Select" link to select all IPs from a list.
5. Click the "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

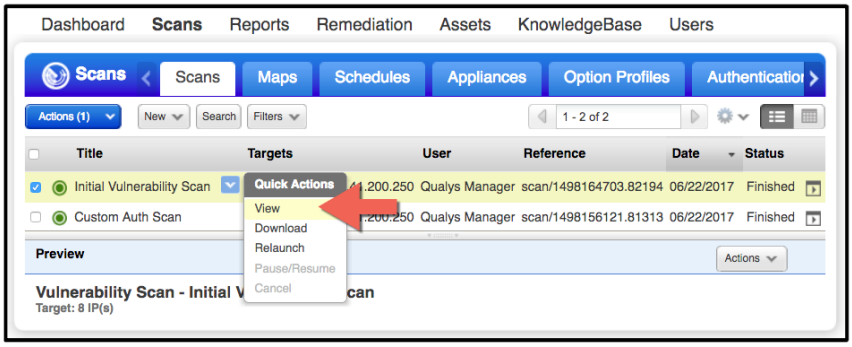
When a Scanner Appliance has finished performing a vulnerability scan, the scan results are sent to the Qualys Secure Operations Center (SOC). The raw scan data is then processed and integrated with the “Host Based Findings” within your subscription.



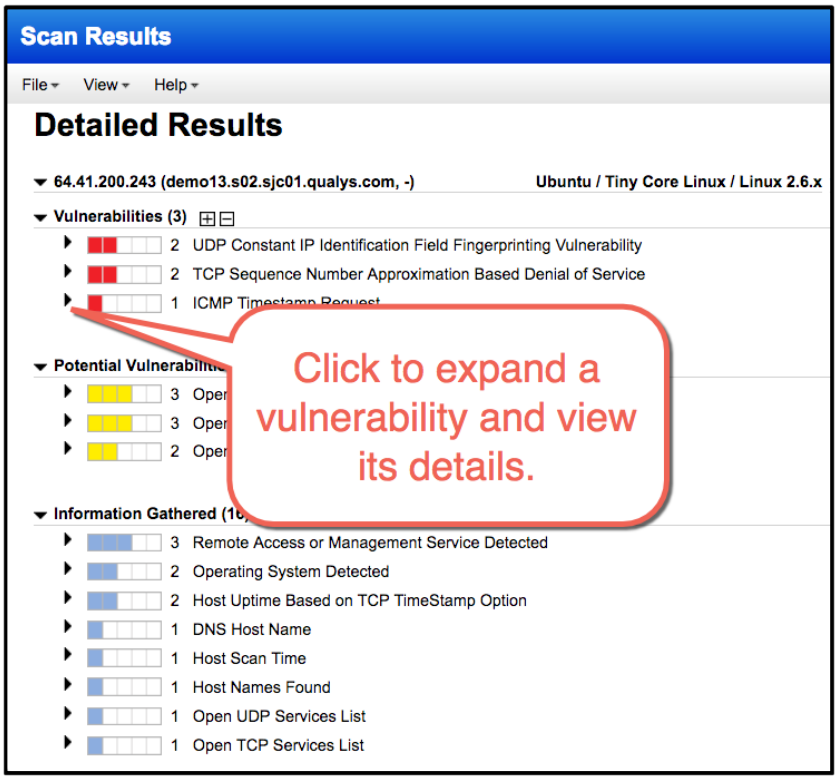
Although the “Status” column may display the “Finished” status, your scan results will not be available for use until the ○ icon changes to the ◉ icon (as illustrated above).

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

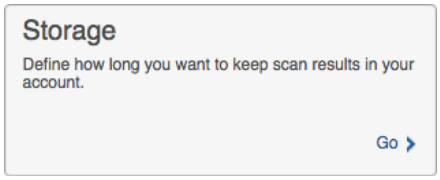
Severity Levels

Level 5 Remote root/administratorRemote 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

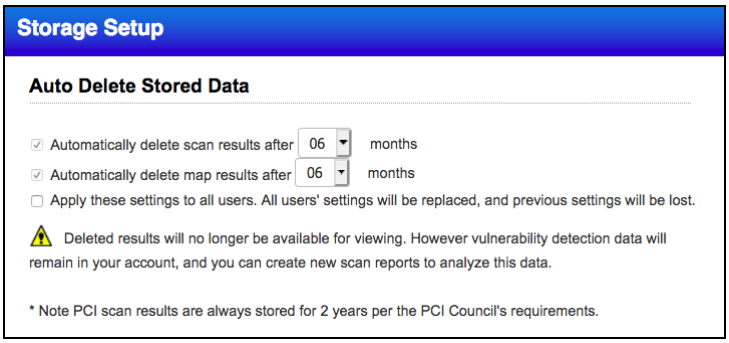
Storage

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.

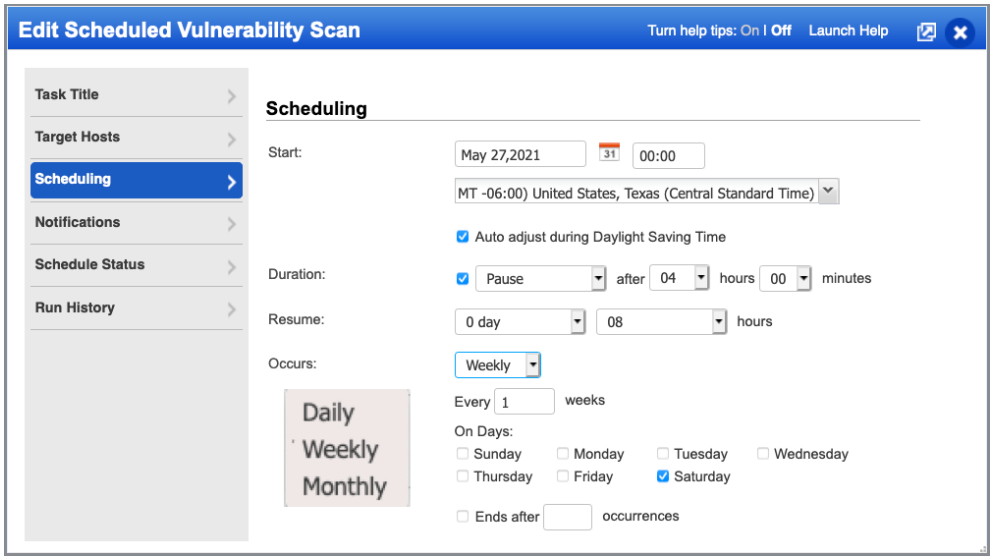


3. Use either drop-down menu to view the available range of storage time frames.

   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:

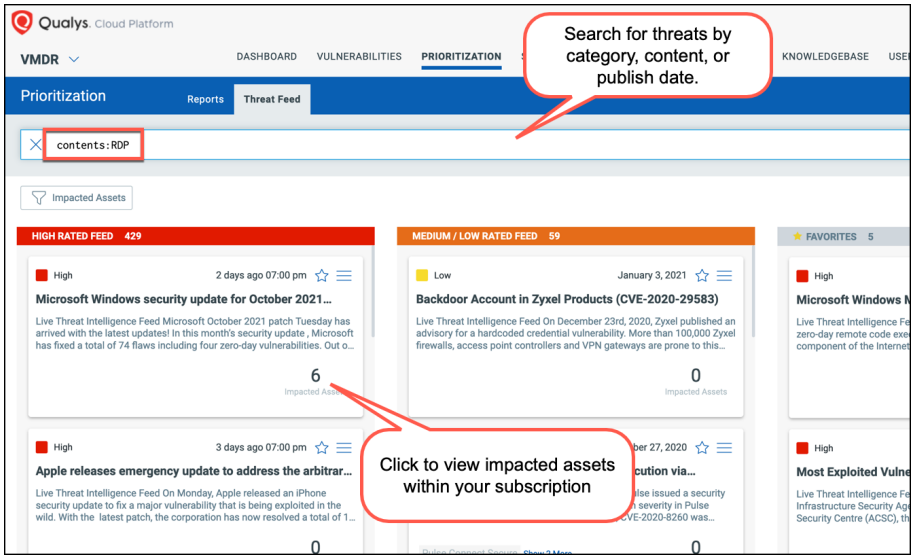
PLAY https://ior.ad/7edW

Reporting - Prioritization

Use the VMDR Prioritization report to automatically prioritize the riskiest vulnerabilities for your most critical assets – reducing potentially thousands of discovered vulnerabilities to the ones that matter.

VMDR Threat Feed

The Threat Intelligence Feed provides a key element to the Prioritization Report. Focus remediation efforts on high-severity vulnerabilities with known or existing threats.



Qualys Threat & Malware Labs provides this threat intelligence feed and several other exploit and malware sources.

Other Threat Feed Sources

Exploit Sources

Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosporus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

Malware Sources

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

- Qualys Threat Protection leverages exploit and malware data from multiple sources.

VMDR Prioritization Report – Option 1

By correlating vulnerability information with threat intelligence and asset context, the Prioritization Report will help you to "zero in" on your highest-risk vulnerabilities and quickly patch them.

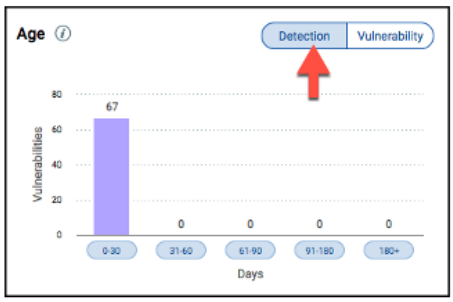
The VMDR Prioritization report :

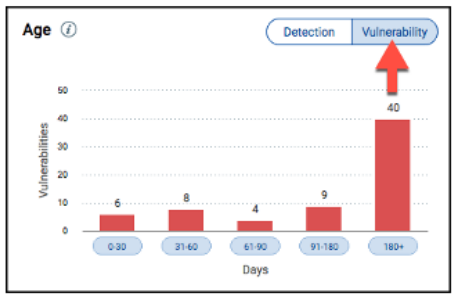
- It guides you to target and quickly patch your highest-risk vulnerabilities.
- It helps you find the specific patch to fix a particular vulnerability.
- It allows you to quickly identify and remediate the vulnerabilities that are most likely to get exploited.
- Empowers security analysts to pick and choose the relevant threat indicators for your specific and unique organization.
- Provides an integrated workflow that reduces vulnerability detection and patch deployment time.

After selecting one or more Asset Tags to specify the report context, prioritization options are provided in three categories:

Age

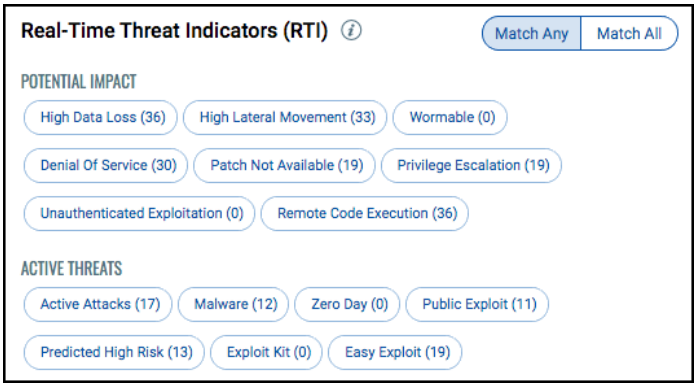
Prioritize vulnerabilities by their age. Detection age is the number of days since the vulnerability was first discovered (e.g., by a Scanner Appliance or Cloud Agent). The "Vulnerability" option will distribute vulnerabilities by actual or KnowledgeBase age.





Real-Time Threat Indicators (RTI)

Prioritize vulnerabilities by their known and existing threats.



Combine multiple threat indicators using the “Match Any” or “Match All” operators. Current Real-time Threat Indicators are:

High Data Loss - Successful exploitation will result in massive data loss on the host.

High Lateral Movement - After a successful compromise, attacker has high potential to compromise other machines in the network.

Denial of Service - Successful exploitation will result in denial of service.

Patch Not Available - Vendor has not provided an official fix.

Privilege Escalation - Successful exploitation allows an attacker to gain elevated privileges.

Unauthenticated Exploitation - Exploitation of this vulnerability does not require authentication.

Remote Code Execution - Successful exploitation allows an attacker to execute arbitrary commands or code on a targeted system or in a target process.

Actively Attacked - Active attacks have been observed in the wild. This information is derived from Malware, Exploit Kits, acknowledgment from vendors, US-CERT and similar trusted sources.

Malware - Malware has been associated with this vulnerability.

Zero Day - Active attacks have been observed in the wild and there is no patch from the vendor. If a vulnerability is not actively attacked this RTI will not be set (even if there is no patch from the vendor). If a patch becomes available Qualys will remove the Zero Day RTI attribute.

Public Exploit - Exploit knowledge is well known and working exploitation code is publicly available. This attribute is set for example when PoC exploit code is available from Exploit-DB, Metasploit, Core, Immunity or other exploit vendors. While potentially increasing the probability of attack, this RTI does not necessarily indicate that active attacks have been observed in the wild.

Predicted High Risk - Leverages machine learning to determine if a presently non-exploited vulnerability should be prioritized.

Easy Exploit - The attack can be carried out easily and requires little skills or does not require additional information.

Exploit Kit - Exploit Kit has been associated with this vulnerability. Exploit Kits are usually cloud based toolkits that help bad actors to identify vulnerable browsers/plugins and install malware. Search for Exploit Kits by name like Angler, Nuclear, Rig and others.

Wormable - The vulnerability can be used by “worms” – to spread without user interaction.

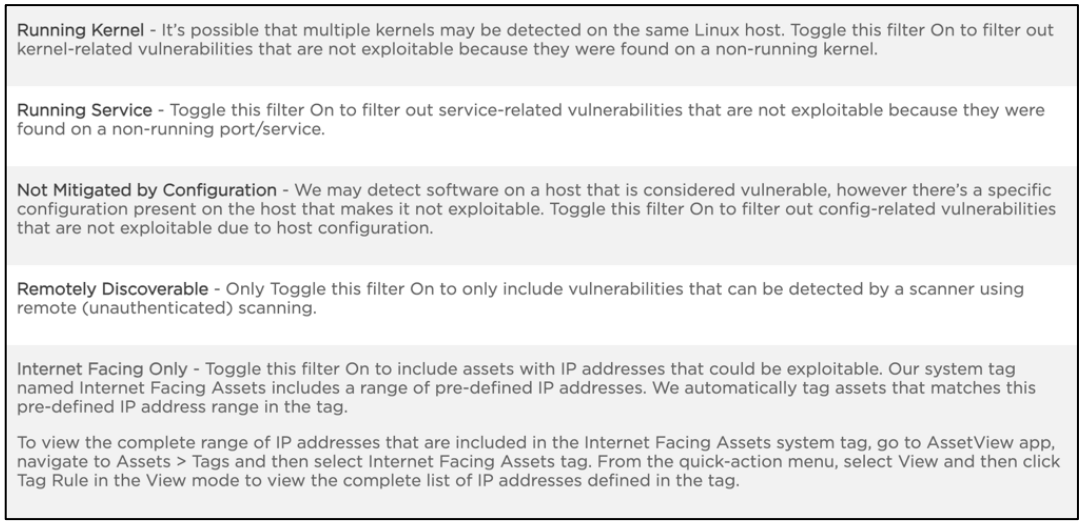
Solorigate Sunburst - Solorigate Sunburst has been associated with all the CVEs used by FireEye's Red Team tools to test the security of their client environments and compromised versions of SolarWinds Orion.

Ransomware - This vulnerability has been exploited in attack vectors where ransomware has been deployed. In other words, this vulnerability is associated with known ransomware.

Attack Surface

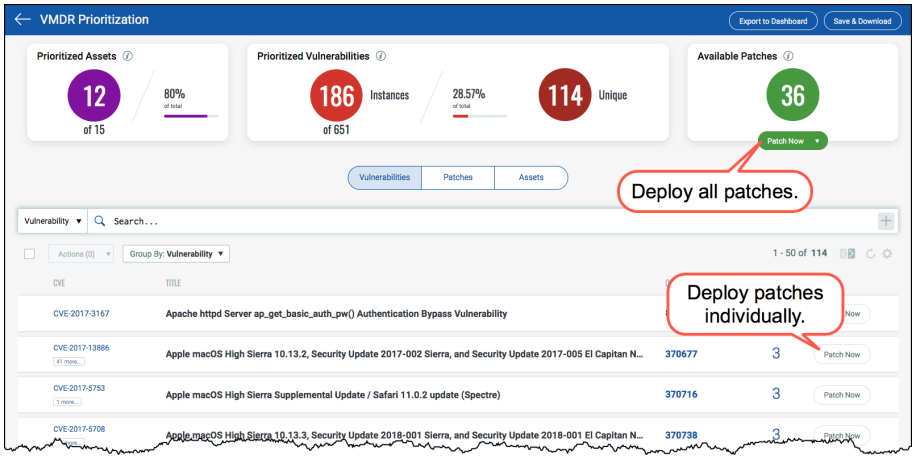
Attack Surface options provide additional context for the assets in the Prioritization Report.

Use Attack Surface options to refine further the context already provided by the included Asset Tags.



Once your priority options have been selected, click the “Prioritize Now” button.

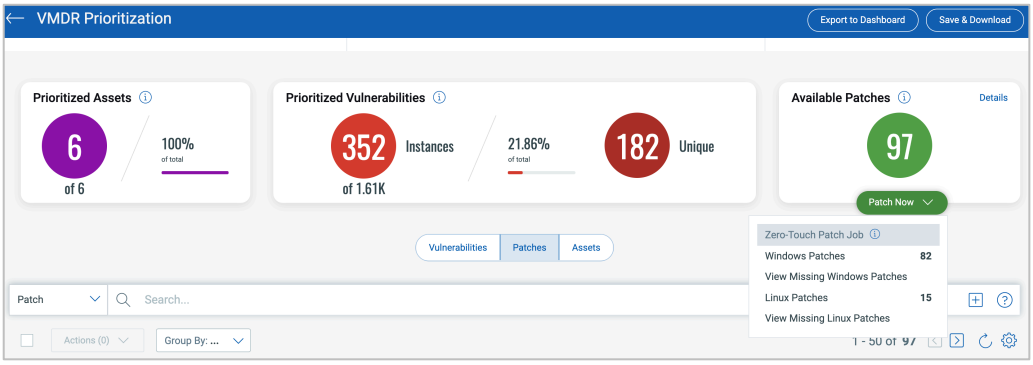
The displayed assets, vulnerabilities, and patches will reflect your priority options.



As you continue to make adjustments to the priority options, the displayed vulnerabilities and patches are automatically adjusted. Patches can be deployed individually or all at once.

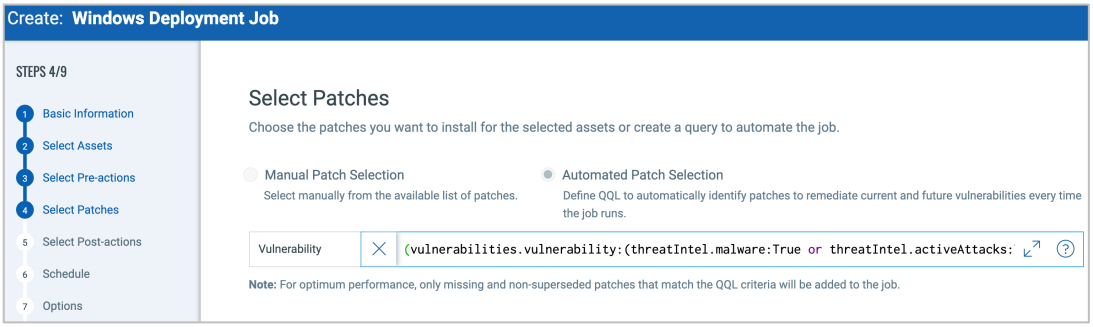
Zero-Touch Patch Jobs

Select the “Zero-Touch Patch Job” option from the VMDR Prioritization Report.



- Automates the selection of patches for recurring deployment jobs
- Patches are selected using QQL
- Patches meeting the query condition are included in scheduled deployment jobs (daily, weekly, monthly)

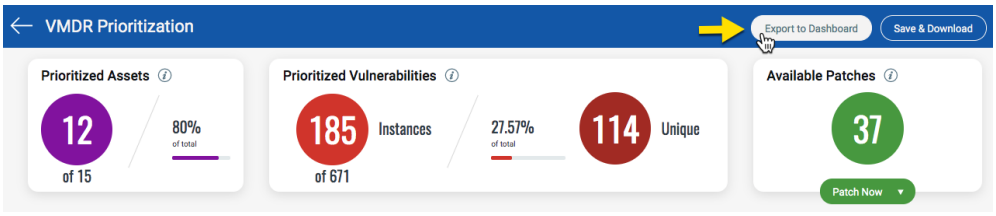
Patches will be expressed as query conditions.



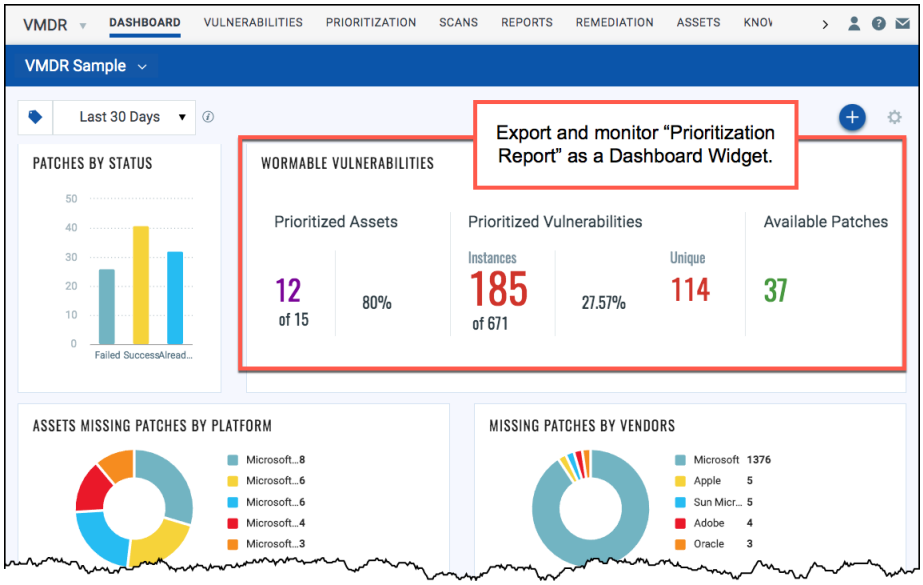
The query is generated from the options (Age, RTIs, and Attack Surface) selected in the Prioritization Report.

Export to Dashboard

Export the results of any VMDR Prioritization Report as a Dashboard Widget.



Results will be continuously updated within the Widget.



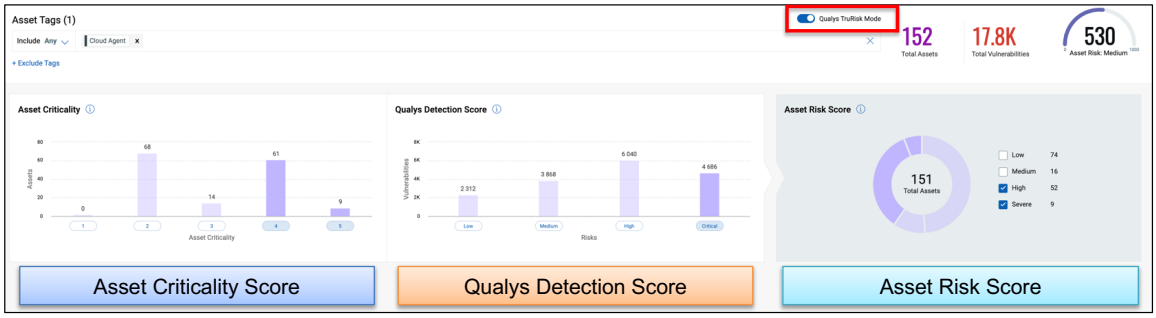
Click the following URL to begin the *VMDR Prioritization Report* tutorial:

PLAY https://ior.ad/7UuA

VMDR Prioritization Report – Option 2 (TruRisk Mode)

Qualys has introduced the TruRisk feature. Using this feature, you can detect vulnerabilities within the context of your critical and non-critical host assets to help you remediate and fix the vulnerabilities that count. This mode provides data for Asset Criticality, Qualys Detection Score (QDS), and TruRisk score. This mode helps prioritize Assets or Vulnerabilities based on risks generated in the result.

You can also generate a report using the Qualys TruRisk Mode. To enable it, toggle the Qualys TruRisk Mode button. The priority options change when this mode is enabled.



Qualys TruRisk is comprised of three components:

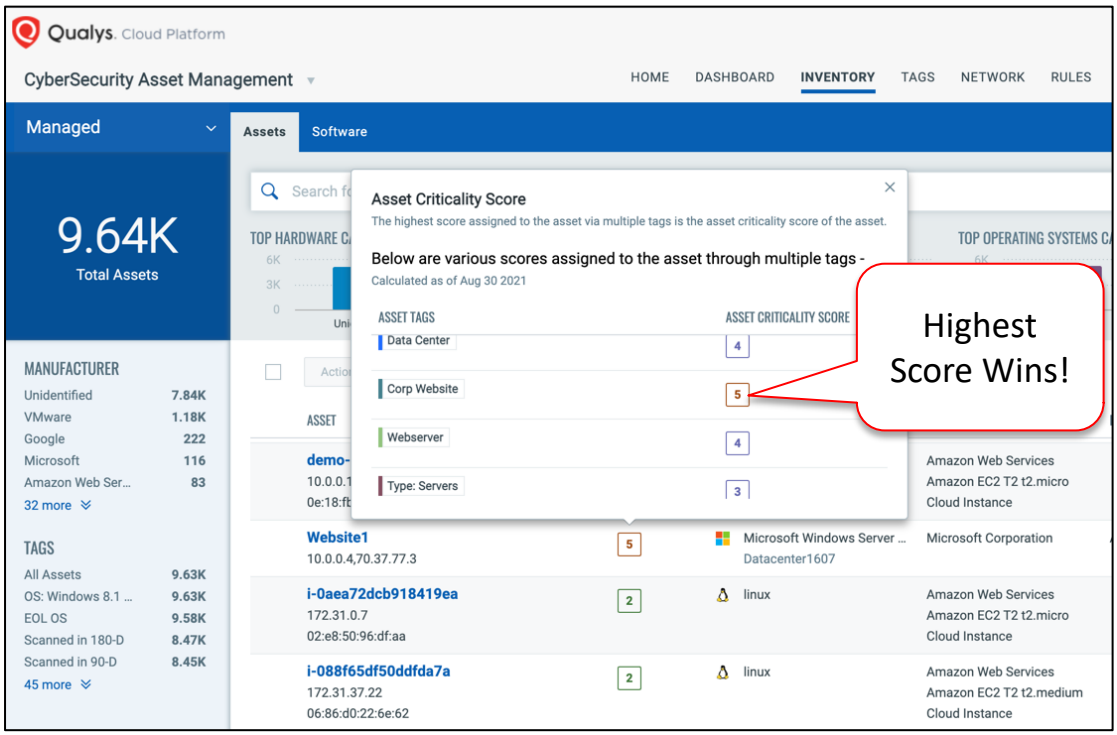
- Qualys Detection Score (QDS) token = vulnerability.detectionScore
- Asset Criticality Score (ACS) token = criticalityScore
- TruRisk Score token = riskScore

QDS and TruRisk have calculated values, while ACS is assigned to assets via Asset Tags.

Asset Criticality Score

Asset Criticality Score represents the criticality of the asset to your business infrastructure. By defining key business and technical contexts, asset criticality helps to focus your security prioritization efforts on high-importance and high-risk assets. Typically, asset criticality is derived from the function, environment, and service the asset provides to the business.

Asset Criticality Score is a value between 1 to 5.



In the above image, the INVENTORY tab displays all assets where Qualys has collected data. Clicking on the Criticality score of an asset displays all the Asset Tags assigned to the asset along with their configured Criticality Scores. The Asset Criticality Score (ACS) is automatically calculated based on the highest aggregated criticality across all tags assigned to the asset. The asset has multiple tags in this illustration with Criticality Scores of 5, 4, and 3. So the Asset Criticality Score of the asset is 5, the highest Criticality Score among the assigned tags. If the tags associated with your assets do

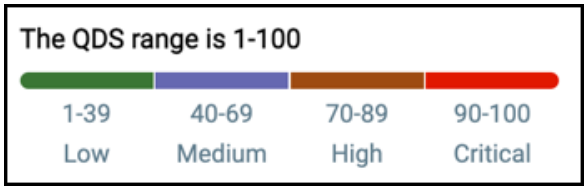
not have a criticality score set, the asset criticality score “2” will be applied to that asset by default.

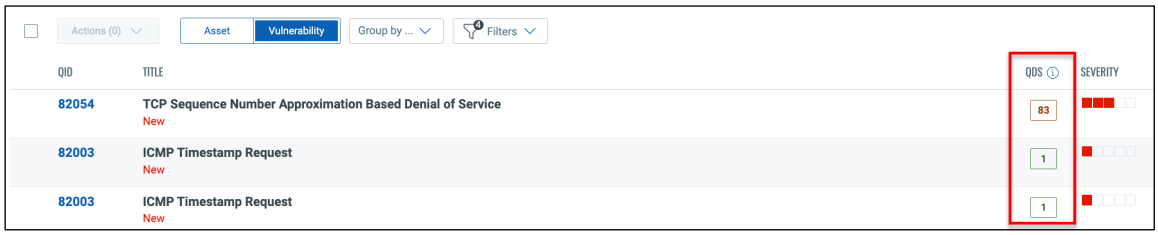
The Asset Criticality Score setting is turned off by default when creating a new Asset Tag.

Qualys Detection Score (QDS)

This is the score assigned to the respective Qualys detection. It ranges from 1 to 100. The severity levels are:

1. Critical: 90-100
2. High: 70-89
3. Medium: 40-69
4. Low: 1-39





QDS is derived from three factors.

1. The highest CVSS score for the CVEs associated with the QID.
2. It then includes Vulnerability temporal details and external threat intelligence details for a vulnerability. It collects data like Exploit Code Maturity (ECM), malware, active threat actors, and if a threat is trending.
3. Lastly, it includes Vulnerability remediation details (CIDs) which are the data on applied mitigation controls to mitigate the risk from the vulnerability.

Vulnerabilities that have applied mitigation controls via Qualys compliance modules will have reduced risk scores. Here, it is essential to note that if multiple CVEs contribute to a QID, the CVE with the highest score is considered for the QDS calculation.

TruRisk Score

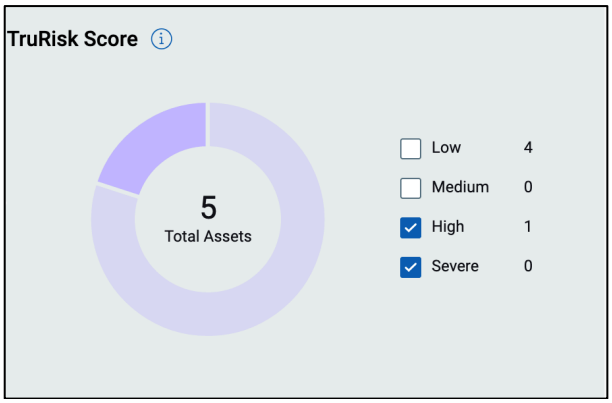
TruRisk score is the overall risk score assigned to an asset. It combines the Criticality Score of a single host with a weighted average of its combined vulnerability detections. While the Qualys Detection Score provides a valuable metric for measuring the impact of a single vulnerability, the Asset Risk Score places the vulnerability in the context of other vulnerabilities discovered on the same host.

It is dependent on the following:

a. Asset Criticality Score (ACS)

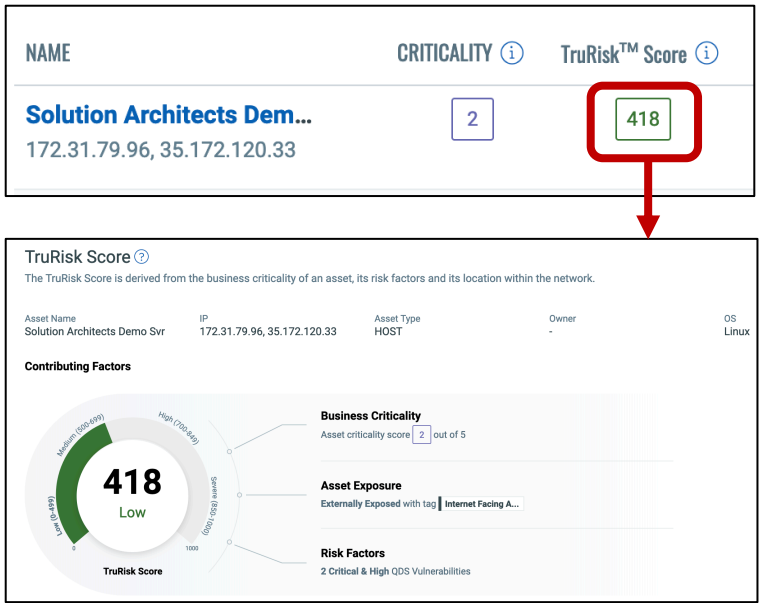
b. Qualys Detection Score (QID) for each severity level (Critical [C], High [H], Medium [M], Low [L])

c. Auto-assigned weighting factor (w) for each criticality level of QID



Calculating the TruRisk Score

The calculation of TruRisk score involves Qualys Detection Score (QDS) and Asset Criticality Score (ACS.)



The following formula is used to calculate the TruRisk score:

$$TruRisk = ACS * \{w_c(Avg(QDS_c)) + w_h(Avg(QDS_h)) + w_m(Avg(QDS_m)) + w_l(Avg(QDS_l))\}$$

In the above formula:

1. ACS - Asset Criticality Score.
2. w - weighing factor for each severity level of QIDs [critical(c), high(h), medium(m), low(l)]
3. Avg(QDS) - Average of Qualys risk score for each severity level of QIDs on that asset
4. You can click any TruRisk value to understand how it is calculated.
5. The weights assigned to QDS based on their range is:
   a. Critical (90-100) – weights = 1.0
   b. High (70-89) – weights = 0.7
   c. Medium (40-69) – weights = 0.4
   d. Low (1-39) – weights = 0.25

Click the following URL to begin the *VMDR Prioritization Report with TruRisk™* tutorial:

PLAY https://ior.ad/8AFq

Reporting – Report Templates

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.

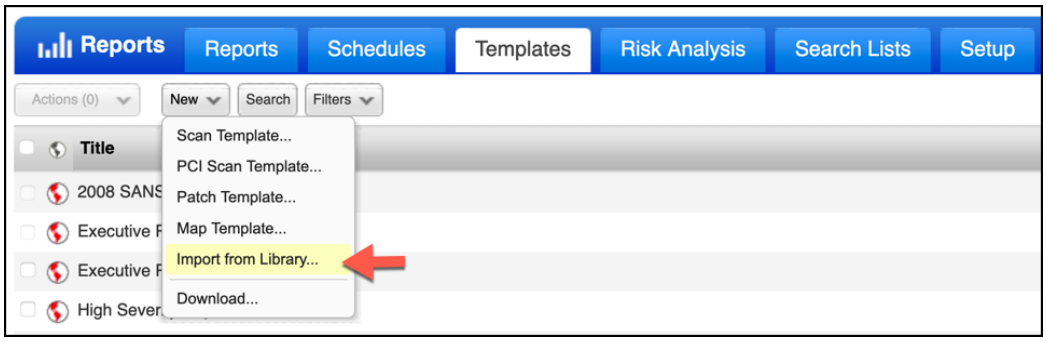
Report Template Library

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

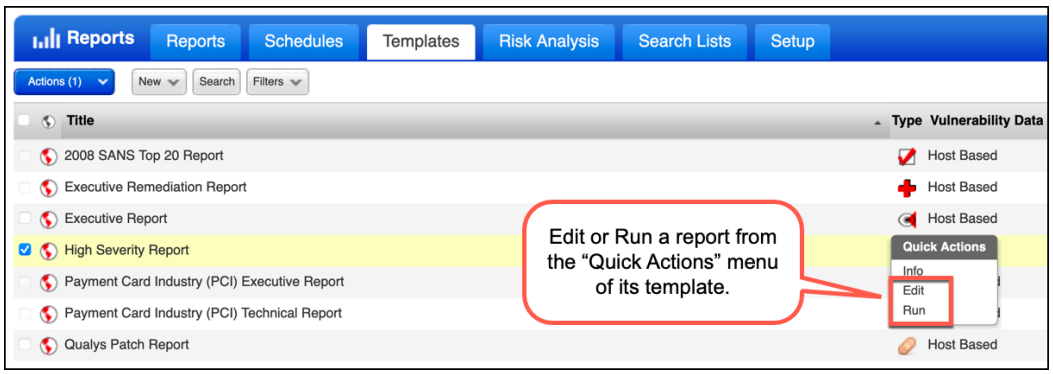
Navigate to the following URL to view the *Running a Scan Report* tutorial:

PLAY https://ior.ad/7emY

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

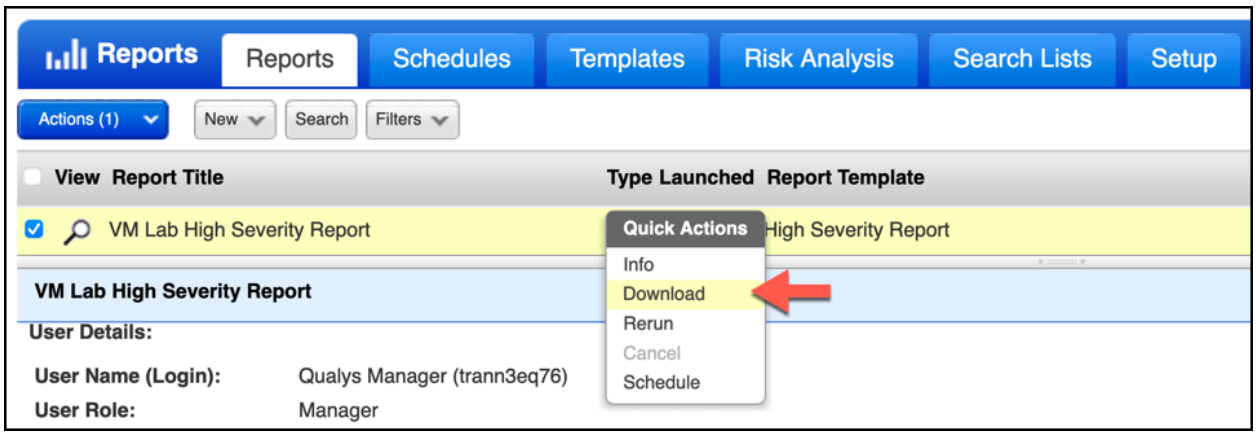


You can edit the "out-of-box" templates to meet your unique reporting needs and objectives.



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

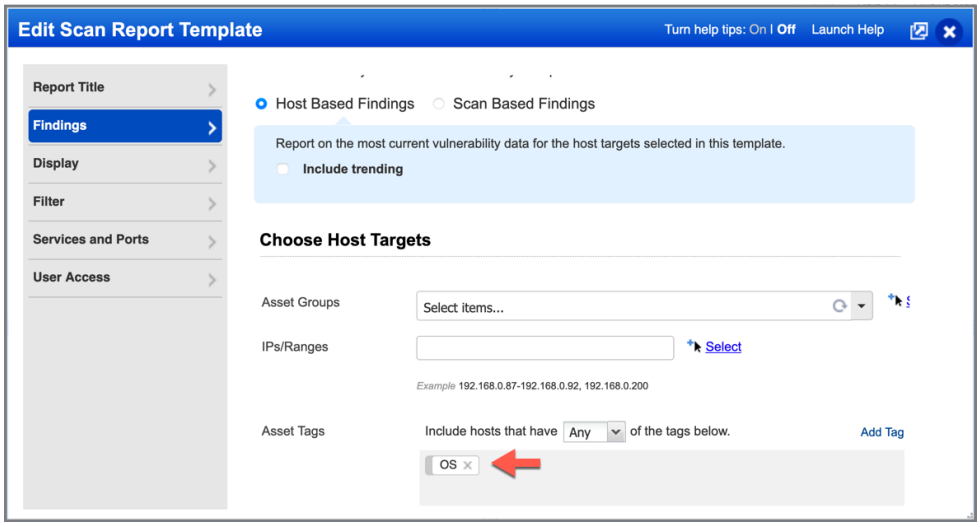
While the “out-of-box” templates are convenient and easy to use, you’ll typically want to design and build your own Report Templates to meet your organization’s custom reporting objectives. Each template is organized by Findings, Display, Filters, Services and Ports, and User Access.

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

PLAY https://ior.ad/7eDm

Findings

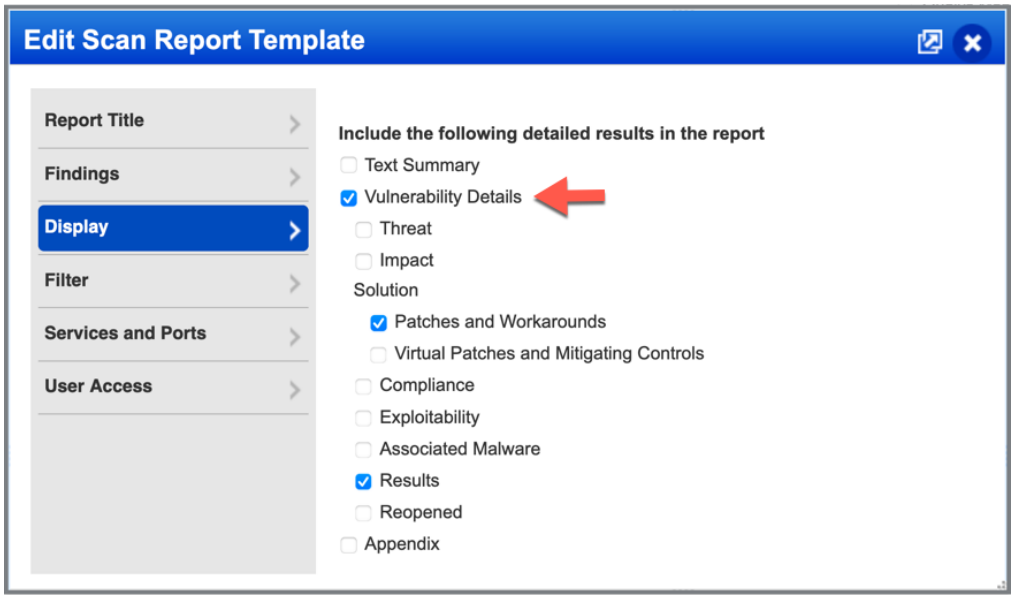
Select Findings in the navigation pane to choose between host-based or scan-based findings.



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

Display

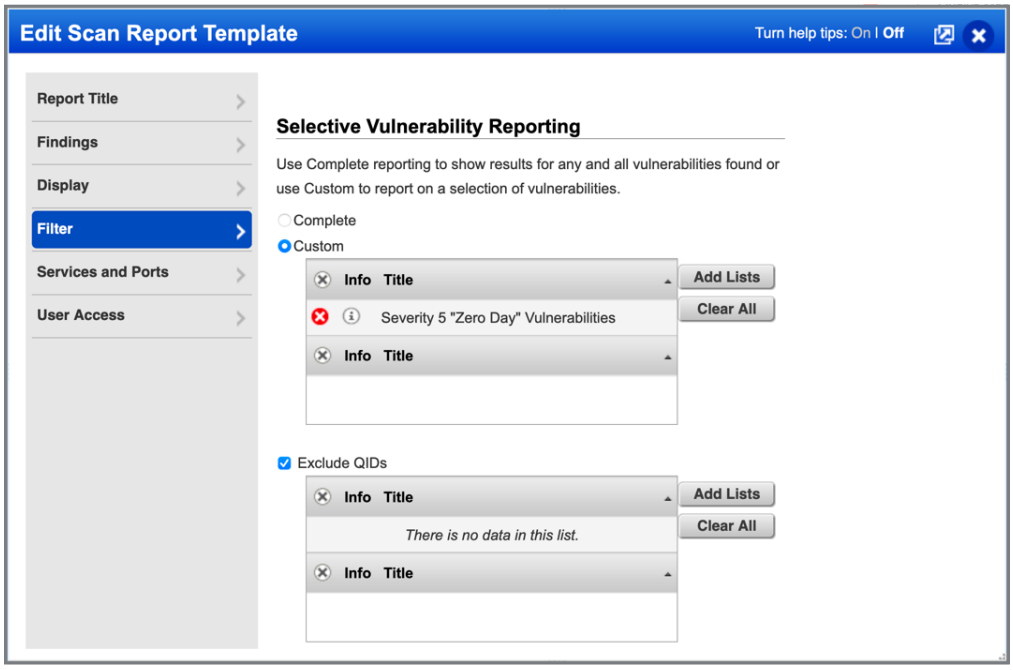
Select Display in the navigation pane to choose amongst various graphics and details settings and options.



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

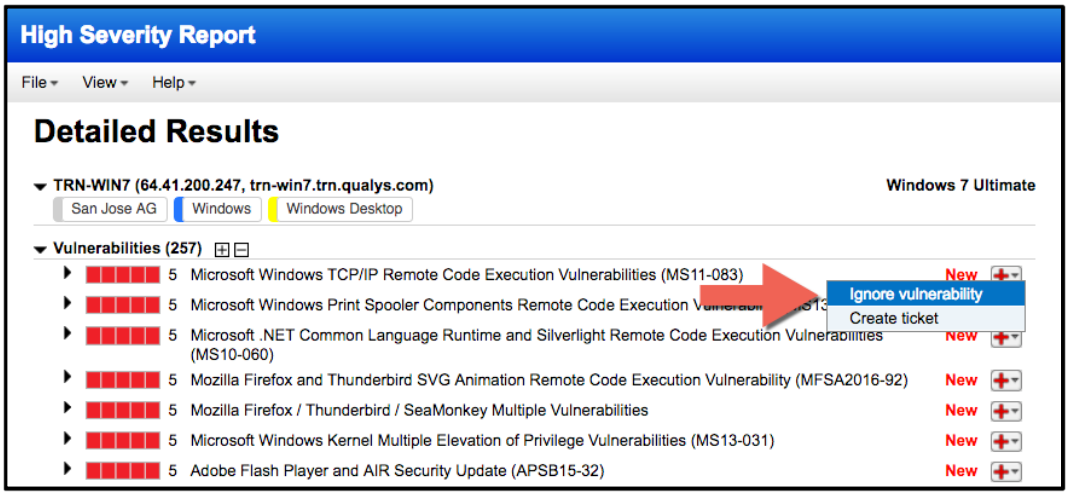
To focus report on a specific list of vulnerabilities, select Filter in the navigation pane and then click the “Custom” radio button to add one or more Search Lists.



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.

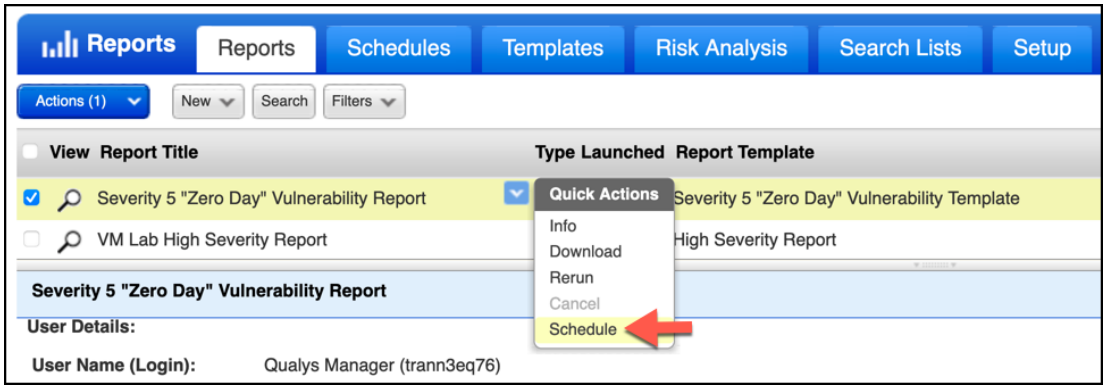
Scheduled Reports

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.

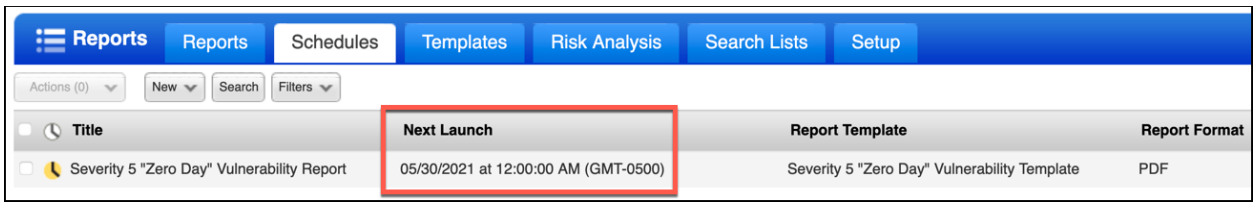
Navigate to the following URL to view the *Scheduled Report* tutorial:

PLAY 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.



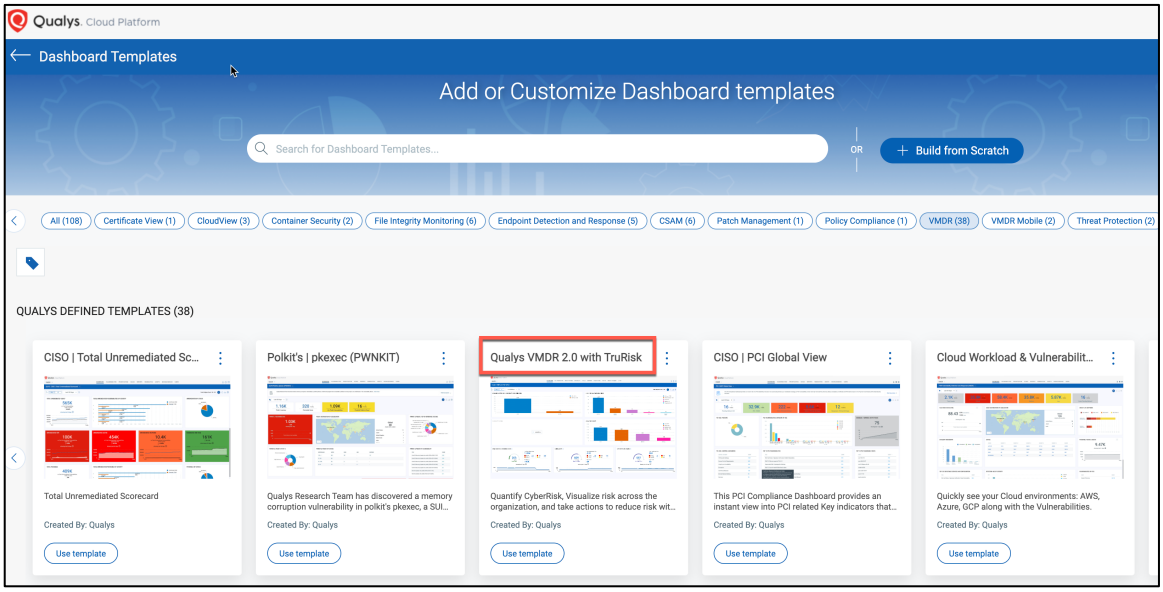
Reporting - Dashboards

Continuously monitor assets and vulnerabilities with any number of “out-of-box” Dashboards or build your own custom Dashboards and Widgets.

Dashboard Library

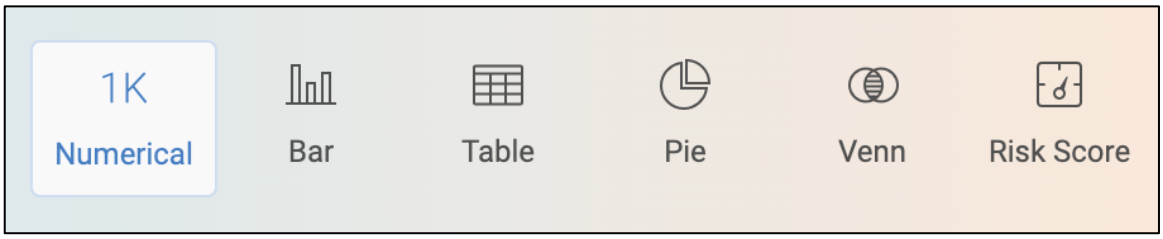
Dashboards bring information from all Qualys applications into a single place for visualization. You can customize and share the information with specific users. The dashboards allow you to view your organization's data in a single place. This will enable you to understand your data better and make an informed decision.

The Dashboard library allows you to create your dashboard using existing widget templates, customize existing widgets, or create widgets to suit your needs. The templates are segregated based on the subscription to other Qualys products.



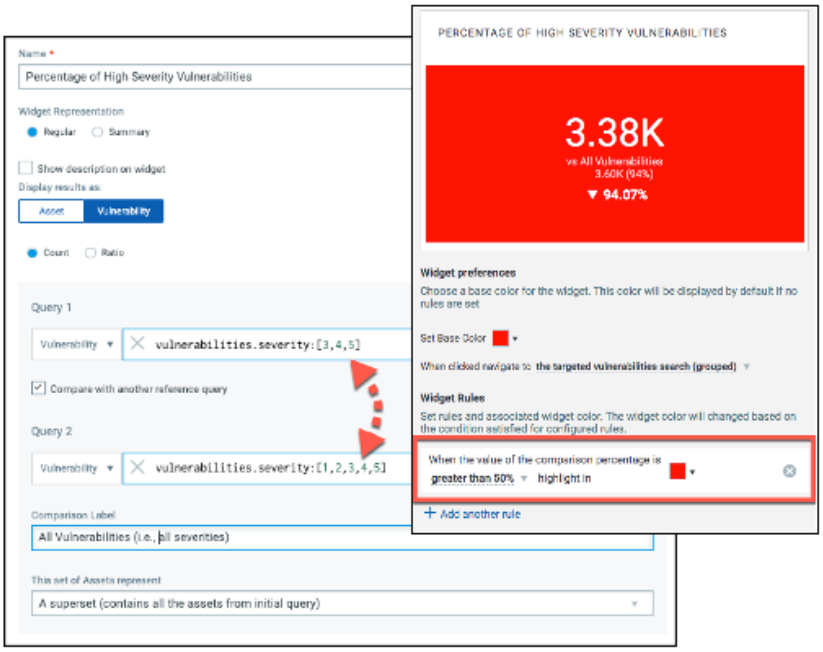
Widget Types

Widgets are designed to display query results graphically. There are different graphic options:



Widgets are automatically updated to reflect changes in your asset data and findings.

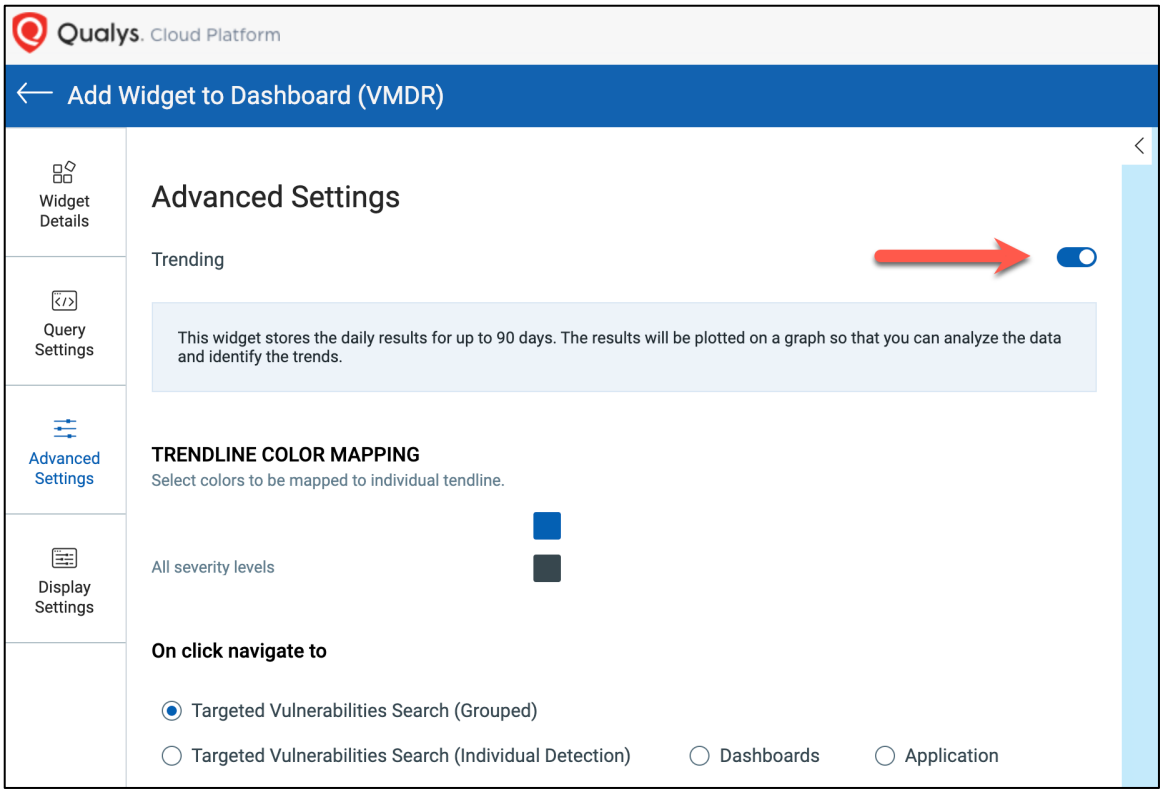
The “Numerical Count” widget can be configured to change its color as changes to assets and vulnerability findings reach specific thresholds or special conditions.



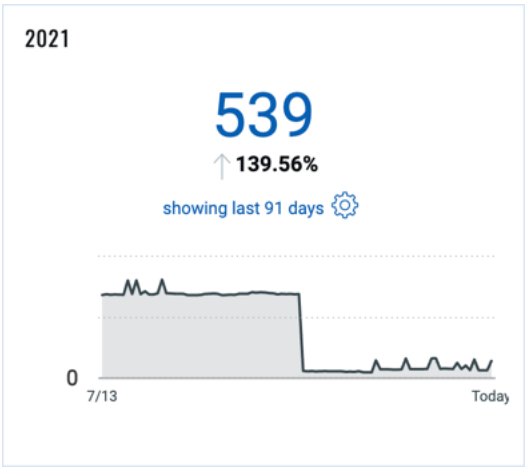
A “reference” query in the count widget helps compare the “initial” query’s result to some control or benchmark. The difference between the result sets of both queries is represented as a percentage.

In the example above, MEDIUM-HIGH severity vulnerabilities (Sev. 3, 4, 5) are presently about 94% of ALL vulnerabilities (Sev. 1, 2, 3, 4, 5). The “count” widget is configured to change from its base color to red when this percentage exceeds 50 percent.

Count widget types have the option to Enable Trending. When enabled, widgets can store trend data for up to 90 days.

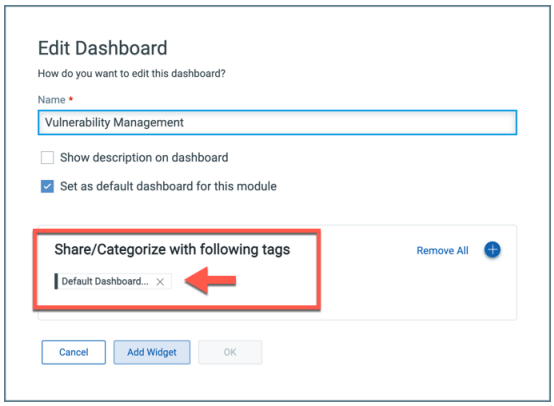


A trend line plotted on a graph will be added to the other information typically displayed in the widget.

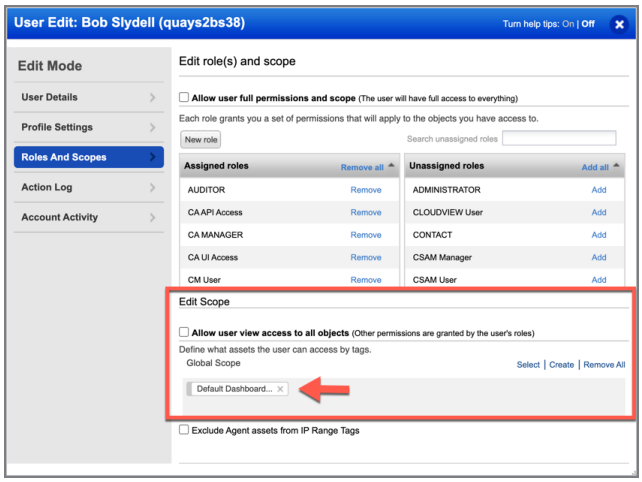


The graphic perspective provided by the trend line will make it easier to visualize swings in momentum and anticipate critical thresholds and milestones.

You can add one or more Asset Tags to a Dashboard through the Dashboard Editor.



The “Default Dashboard Access Tag” is created by Qualys.



Share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.

For more information and details on Dashboard and Widget capabilities, check out the Qualys Reporting Strategies & Best Practices training course (https://qualys.com/learning).

Click the following URL to begin the *Adding Risk Score Widgets* tutorial:

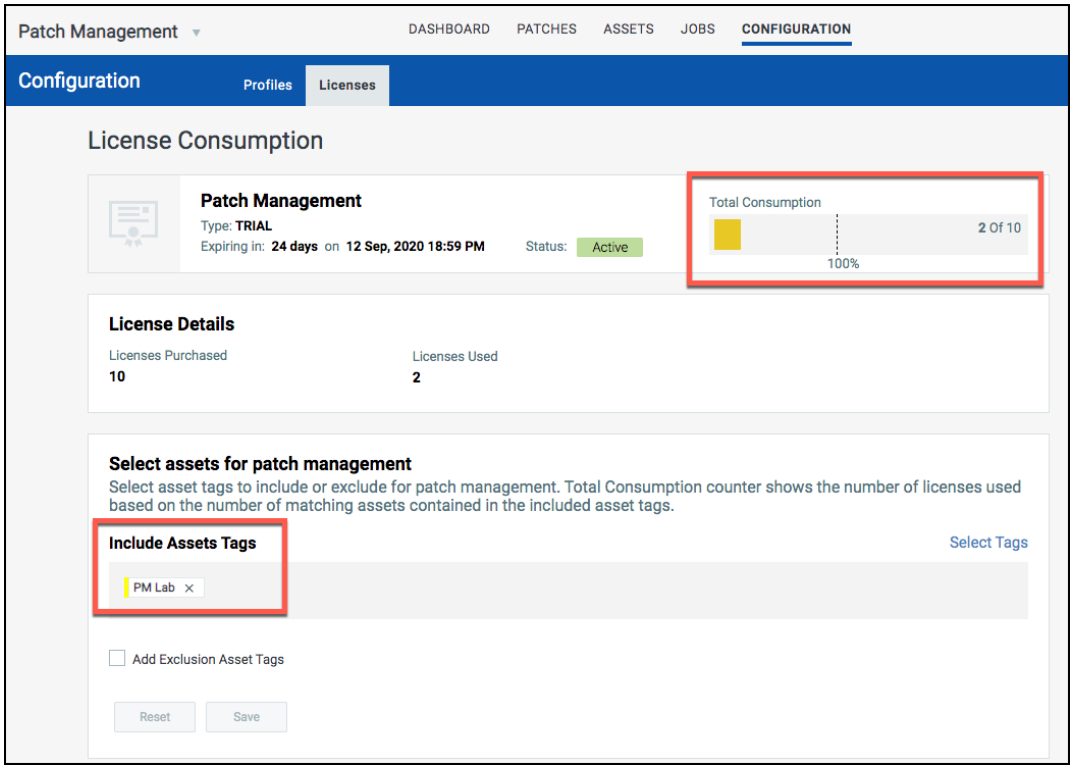
PLAY https://ior.ad/8xke

Patching Vulnerabilities

Along with the help of Qualys Cloud Agent, the Patch Management application provides patch response functionality in VMDR.

Allocating Patch Licenses

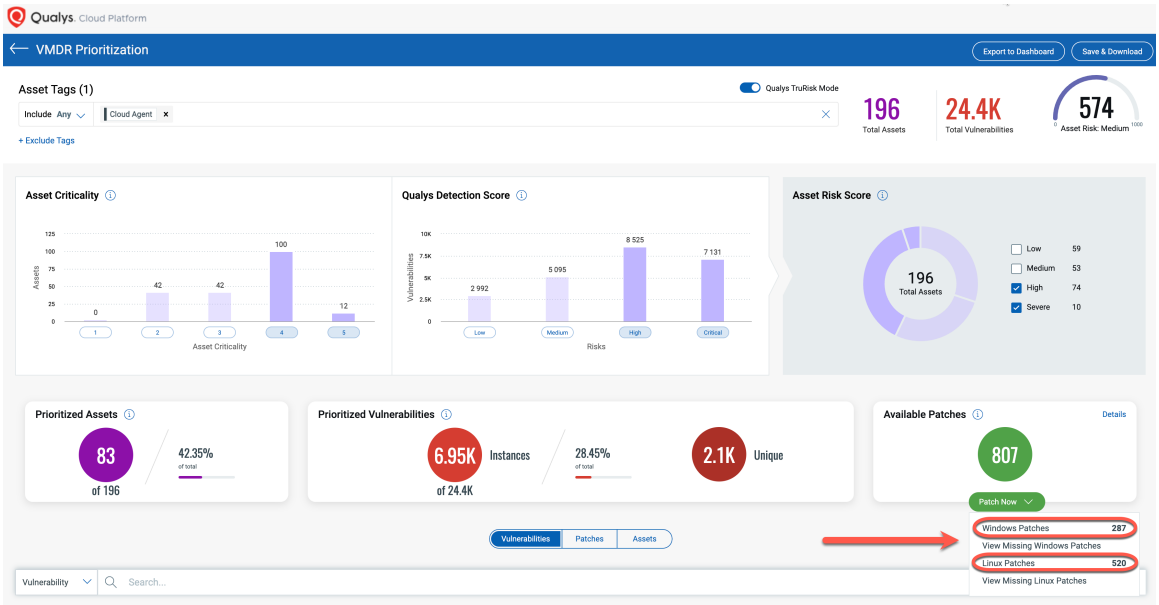
Before creating a job, add one or more Asset Tags to the Patch Management License Consumption Configuration to identify the “patchable” host assets within your account.



You can explicitly exclude sensitive assets from being included in any patch jobs. The “Total Consumption” indicator is updated with the number of agent hosts labeled with the tag(s) included.

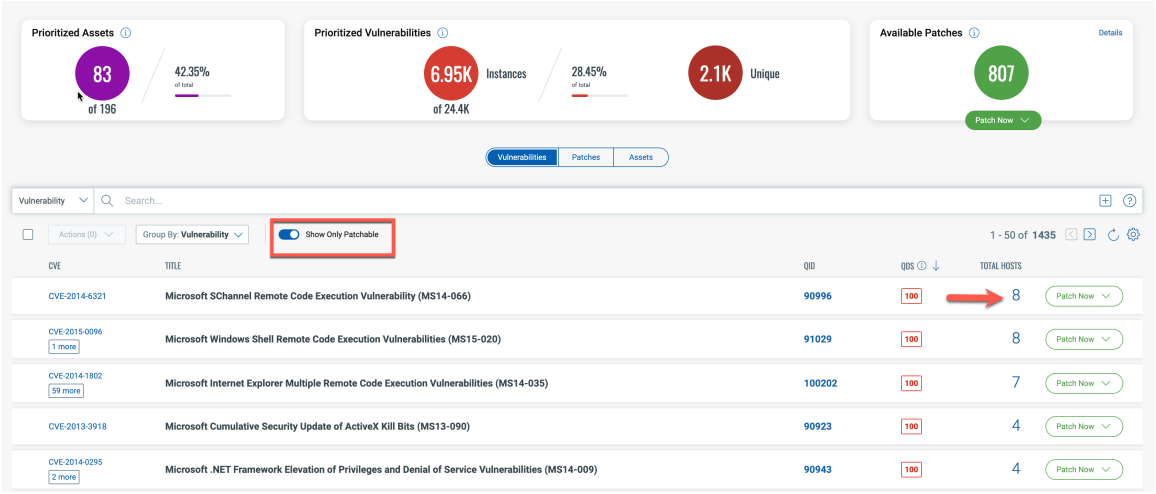
Patching From VMDR

This short section will have a lab activity showing that you can go from the Prioritization Report in VMDR to patching assets.



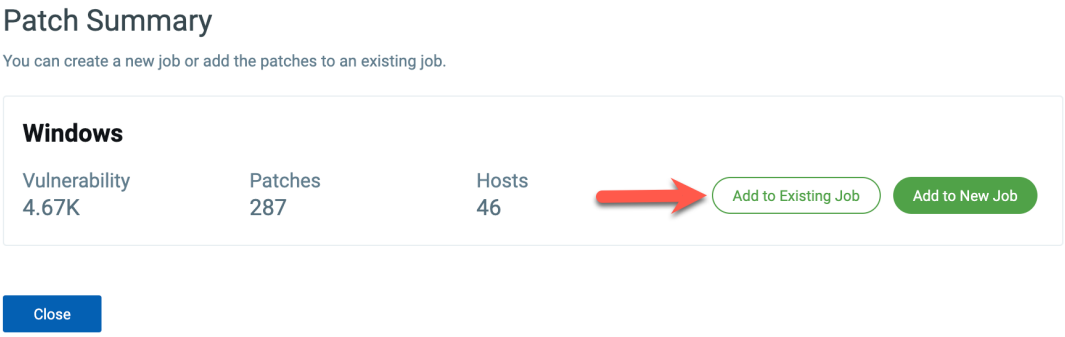
The Patch Management application separates deployment jobs into Windows and Linux jobs.

Patches can be selected individually and added to different jobs, or you can use the large green button to add many at once.



Once patches are selected, they can be added to their own “New” deployment job or add them to an existing job.

You can add patches to a job that uses the manual patch selector but not a job that is QQL-based. You can add assets to a patch job that is QQL-based.



Click the following URL to view the *TruRisk Mode Linux Patch Job* tutorial:

PLAY https://ior.ad/8xc3

Appendix A
VMDR Prioritization Report Use Cases

The VMDR Prioritization Report provides countless ways to combine Asset Context, Vulnerability Age, Real-Time Threat Indicators, and Attack Surface options. The following labs are use cases to demonstrate approaches to building a Prioritization Report using VMDR features.

Databases

Hosts with large data stores are especially impacted by “High Data Loss” vulnerabilities.

Click the following URL to view the *Prioritization Report Use-Case: Databases* tutorial:

https://ior.ad/7UuB

Internet Facing Assets

Hosts with public interfaces are at greater risk because of their exposure to the Internet, especially with vulnerabilities that can be exploited without authentication. The risk becomes even more significant if the same host has vulnerabilities that can lead to privilege escalation.

Click the following URL to view the *Prioritization Report Use-Case: Internet Facing Assets* tutorial:

https://ior.ad/7UuK

Appendix B
Steps for Success

There is a lot to know about the Qualys user interface. The high-level steps below provide a blueprint for being successful with Qualys. This will not cover everything you'll ever need to know. This will provide an important checklist you'll want to review for success.

1. **Start with Scoping**: Outline which assets and vulnerabilities are the most important to your organization and understand your remediation SLAs.
2. **Deploy Sensors**: As part of this onboarding process, you will deploy Qualys Scanner Appliances and Cloud Agents.
3. **Manage Assets**: Set up Asset Groups and Tags so you can easily refer to and report against your assets.
4. **Report:** Get visibility into your vulnerability data for your high-priority assets using dashboards, Qualys Query Language, and reports.

Scope

Scoping is important because it helps you understand where the biggest risk factors lie. With a scope, you will know what to prioritize and where to take action first.

1. SCOPE: Make a list of all the parts of your organizational assets that you would like to manage in the short term and long term from within Qualys.
    a. Examples: Cloud assets, workstations, internal servers, laptops, External Assets, air-gapped networks, etc.
    b. Where are they? (This will determine sensor deployment). If you have a network diagram, here is a good place to bring it out.
    c. Prioritize that list – where do we start? What are the most important assets in your organization? Do you have a ranking of assets from least important to most important? If not, Qualys can help you define this.
2. GOALS: Define goals and SLAs for your VM program.
    a. This step may already be done. Does your organization have a security policy?
    b. What assets will be prioritized? Crown Jewels? External Assets? Internal Servers? Workstations?
    c. What types of vulnerabilities will be prioritized?
    d. What is your company's SLA for remediation for a given type of asset and vulnerability?
    e. More tips on establishing a RISK-based approach to Vulnerability Management. You don't need to get into the details of these articles just yet, they will be shared again later. That said, these

articles set the stage for your ultimate goal: Reduce Risk to your organization using Qualys.

- https://blog.qualys.com/product-tech/2022/12/12/operationalizing-qualys-vmdr-with-qualys-trurisk-part-1
- https://blog.qualys.com/vulnerabilities-threat-research/2022/12/16/implement-risk-based-vulnerability-management-with-qualys-trurisk-part-2
- https://blog.qualys.com/product-tech/2023/01/03/implement-risk-based-vulnerability-management-with-qualys-trurisk-part-3

f. Don't only focus on critical vulnerabilities.

- According to the 2023 Qualys TruRisk Threat Research Report, Initial Access Brokers attack what organizations ignore.
- Automate what you can automate.

Sensors

Determine what sensors you'll use to collect your vulnerability data. This step is vital and a big piece of your deployment. What are the best mechanisms to ship your data to the platform so you can SEE it? Remember, for exploitable vulnerabilities in a risk-based approach, the clock is ticking.

1. Cloud Agents – Give you near real-time vuln data and the potential to remediate. This is the latest and greatest way to detect MOST of the vulnerabilities on your hosts.
2. Qualys Scanner Appliances – Deployed in your environment. These are point-and-shoot. They ACTIVELY (meaning they interact from the outside) with your hosts and detect vulnerabilities during the scan.
3. Qualys Cloud Scanners – Available in the cloud, they can be pointed at your external IP addresses. These help you understand what those external assets look like. These scanners are automatically associated with your subscription. No installation is necessary.
4. Connectors - API calls into cloud environments to pull all your inventory data from Amazon, Azure, GCP, etc.
5. TIPs: Many customers deploy both agents and scanners. This offers full vulnerability assessment coverage and helps speed detection and remediation time.

Manage Assets

Your sensors will collect data about your assets, but you must organize them in Qualys. This is a vital piece of success and often frustrates organizations.

There are two ways to "group" assets in Qualys:

1. Asset Groups – This is the traditional way but still has useful functionality.
2. Asset Tags – This is the newer way and should be your focus.

When to use Asset Groups

1. Use these only when defining IP RANGES.
2. Don't use them with scattered individual IP addresses.
3. These are typically used when SCANNING (using a Scanner Appliance) full ranges of your network for vulnerabilities.
4. These are typically NOT useful when running reports (use tags instead).
5. If you set these up correctly, you'll make scanning much easier on yourself in the long run. Use this article to help you set up both groups and tags.

When to use Asset Tags

1. When you are grouping assets by categories like OS, Device Type, Software.
2. These allow you to set a Criticality on any asset with a given TAG. This will be VITAL later on when it comes to reporting and remediation.
3. This article will provide a framework for successfully setting up tags. The more you work to get these right, the easier finding assets and reporting on them will be. https://success.qualys.com/support/s/article/000005819
4. Don't forget about Asset Criticality – This is an important piece to helping automate where prioritization should occur in your environment.

Reporting

Dashboards
Dashboards are collections of widgets. A widget is a visual display of meaningful data points.

Refer to your security policy for which assets take the highest criticality.

Refer to your security policy for which vulnerability metrics you're using for prioritizing remediation.

When it comes time to invest in reporting, focus on the most important assets and vulnerabilities first. You will spend much time getting your dashboards and reports the way you want them, but remember the 80/20 rule and get going with the dashboards that will make the biggest impact first.

Get Moving with Reporting

1. First, consider your highest-priority assets and vulnerabilities. Spend a proportionate amount of time figuring out dashboards and reports on those highest-priority items.
2. Dashboard Home

- This contains a "Start Here" when it comes to reporting and dashboarding
- This also has many importable dashboards that are already built for you.

3. Use the out-of-the-box dashboards provided by VMDR to help you visualize your top risks. You can find this right in the UI by going to the Dashboards section, clicking on the gear icon in the upper right corner, and clicking "Create Dashboard."
4. Remember to use TruRisk to prioritize your vulnerabilities on your most critical assets. This step will get you thinking about how you want to view your vulnerabilities.
5. Use the prioritization report to help drive patching. This report is very effective in providing you with actionable items that are of critical priority.
6. Use report templates to report on your vulnerability data appropriately.
    - Report templates allow you to get detailed vulnerability data about your hosts.
    - Verify that the reports go to the correct users.
    - There will be high-level reports with minimal technical data
    - There will be detailed reports dedicated for specific audiences.

7. Distributing Reports – This video walks you through distributing reports to people not logging into Qualys. You can send your reports as a link, attachment, or simple notification requiring users to log into Qualys to get their reports. Go to Qualys Help for more information.

Appendix C
Useful Resources

Training Page
Shows all available training. After going through this course, enhance your knowledge on this site.

Learning System
Where you can enroll in all Qualys Training.

VMDR How-to videos
This video series will walk you through the steps for setting up Qualys Vulnerability Management, Detection, and Response (VMDR).

Cloud Platform
Whitepaper explaining the basics of the Qualys Platform

Support Portal
Useful landing page for docs, training, forums, and managing cases.

How to Collaborate with Support
This article tells you all the different ways you can interact with Support. Call, chat, open a case, etc.

Opening Cases
This document tells you what you need to provide support to drive faster resolution for your cases.

Documentation
Here is where you can find ALL Qualys documentation

Systems Status
Shows the operational status, maintenance, upgrades, and outages of each platform.

Find my platform
Shows the Qualys platform your organization is using.

Vulnerability Detection Pipeline
Browse, filter by detection status, or search by CVE to get visibility into upcoming and new detections (QIDs) for all severities.

New Vulnerability Feature Request
This article will walk you through how to log a feature request

Appendix D
Useful Resources for Cloud Agent

Cloud Agent Platform Availability Matrix
Verify that Cloud Agent supports your OS.

How-Tos for Cloud Agents
This full video series will walk you through how to deploy and configure Cloud Agents.

Getting Started with Cloud Agent
This is the official guide for deploying Cloud Agents.

All Installation guides for each OS
Here are the installation guides for all Operating Systems.

Deploying your agents in bulk
This article will help you understand how your agents can be deployed at scale.

Cloud Agent Help
will help you troubleshoot any connectivity issues or errors you see as part of your deployment.

Troubleshooting Agent Connectivity
This document will walk you through how to troubleshoot any agent connectivity issues.

Appendix E
Useful Resources for Purging

Purging: What, why, when, how, what happens to the data?
This article will walk you through how purging works.

Purging Stale Data
Watch this video on why you need a good purging practice for account maintenance. This will save you and your team time and energy in the long run.

Subscription Health Dashboard and Purging Explanation
Find the Subscription Health dashboard on this page. Download the file as a JSON file and import it into your account.

Qualys Help for setting up purge rules
This will show you the process for setting up purge rules.

Purging is covered in more detail in our *Reporting Strategies and Best Practices* course.