Vulnerability Management Training Labs

All Material contained herein is the Intellectual Property of Qualys and cannot be reproduced in any way, or stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the express written consent of Qualys, Inc.

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

Introduction 5
Prerequisites/System Requirements 5
LAB 1 – Account Setup (15 min.) 6
Login to Qualys 6
Update User Profile 10
Account Settings 13
Context Sensitive Help/Online Manual 15
Add IP Assets to Your Account 16
Launch Initial Scan 19
LAB 2: KnowledgeBase & Search Lists (10 min.) 21
Customize the KnowledgeBase 21
Search List 22
LAB 3: Vulnerability Assessment (20 min.) 26
Trusted Scanning 26
LAB 4: Assets (30 min.) 39
Vulnerability Management Assets 39
AssetView 44
Asset Tagging 45
AssetView Search 57
AssetView Dashboard 62
LAB 5: Reporting (25 min.) 65
High Severity Report 65
Selective Vulnerability Reporting 68
Scheduled Reporting 70
LAB 6: Threat Protection (20 min.) 73
Activate Threat Protection 73
Reporting with Threat Protection RTIs 1
LAB 7: User Management (10 min.) 5
User Roles 5
Create User Account 6

LAB 8: Remediation (15 min.) 8
Assign Vulnerability to User 8
Ignore Low Risk Vulnerabilities 10
Create Remediation Report 12
Appendix A: Mapping 14
Mapping Targets 14
View and Use Map Results 17
Appendix B: Asset Tag Examples 23
Asset Name Contains Rule Engine 23
Software Installed Rule Engine 24
Vuln (QID) Exists Rule Engine 25
Stale Host Tag 26
Appendix C: Account Configuration 27
Appendix D: Contacting Support 32
Appendix E: Qualys Cloud Agent Installation 36
Create Cloud Agent Activation Key 36
Windows Agent Installation 41
Mac OS Agent Installation 46
RPM-Based Agent Installation 49
Debian or Ubuntu Agent Installation 52
CA Install Programs and Scripts 55
Cloud Agent Inventory 56

Introduction

The Vulnerability Management application will provide you and your organization with the tools and features needed to successfully manage and mitigate vulnerabilities. When you complete all the exercises in this lab document you will be able to:

1. **Perform Host Assessments**
2. **Manage Host Assets**
3. **Create Host Assessment Reports**
4. **Manage User Accounts**
5. **Remediate Risk**

Please do not skip any of the required lab exercise steps, as they will be needed to complete other lab exercises later. Some labs contain a section called "Additional Exercises" that can be performed any time, at your own convenience.

Prerequisites/System Requirements

To perform the exercises in this lab, you will need:

1. **Qualys Account**
2. **Web Browser (Current or Stable Release)**
   - **Microsoft Edge or Internet Explorer**
   - **Mozilla Firefox**
   - **Google Chrome**
   - **Safari**
3. **Java Browser Plug-in**
4. **Adobe Acrobat Reader or comparable**

Tip: Your browser's Pop-up Blocking configuration can interfere with the proper functioning of the Qualys User Interface. Please modify the settings of your Web browser to allow pop-ups from qualys.com.

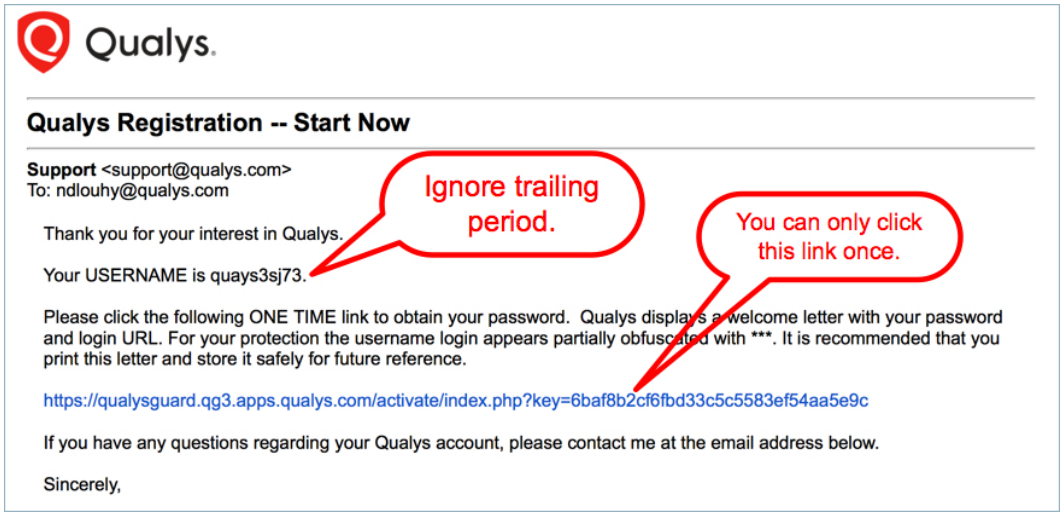
LAB 1 – Account Setup (15 min.)

This lab will address the steps needed to setup your Qualys student trial account and the Vulnerability Management application. These steps will make it possible to complete the remaining lab exercises in this document.

Login to Qualys

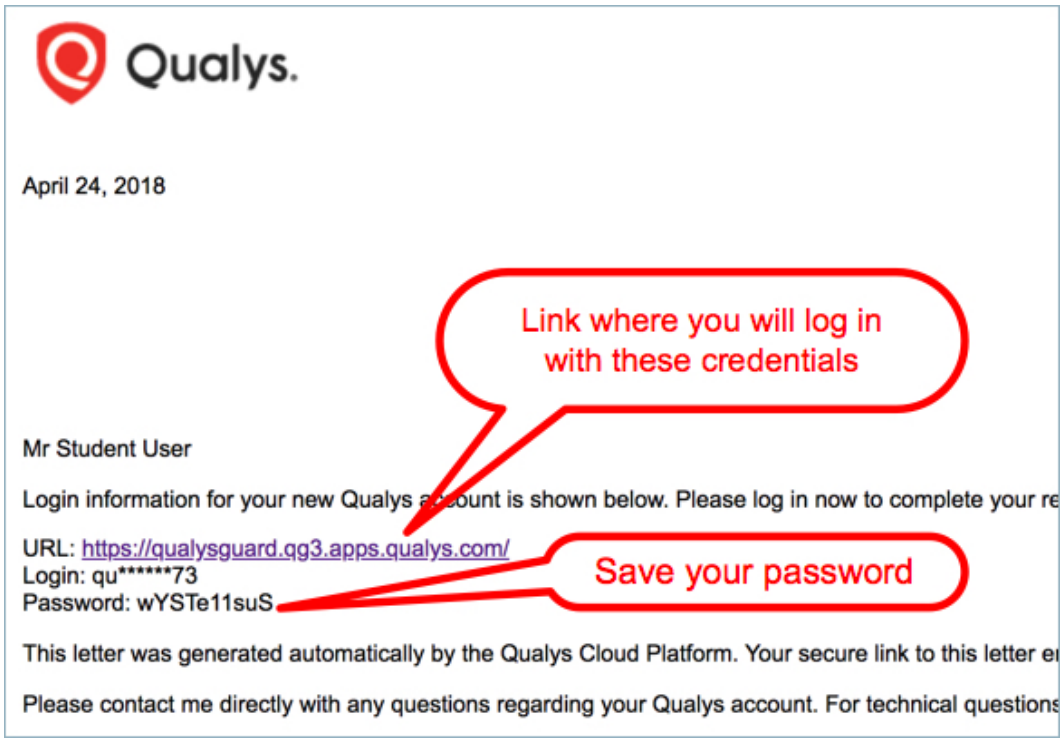
Qualys student trial account credentials are generated and sent to the email address specified in your "learner" account user profile. Our Learning Management System will not send student account credentials to public email domains (e.g., yahoo.com, gmail.com, outlook.com, etc…).

Your student trail account will remain active for 30 days (this is the maximum time limit for all training accounts). Please contact training@qualys.com with account credential issues or questions.



1. **Open your Qualys student trial account message/document.**
2. **Record and save your USERNAME (e.g., text document, password manager, etc…).**

   *****The period at the end of the sentence is NOT a part of the USERNAME.***
3. **Click the ONE-TIME link to view the PASSWORD page. The "one time" link is designed to prevent others from viewing your password information; it will not work a second time.**

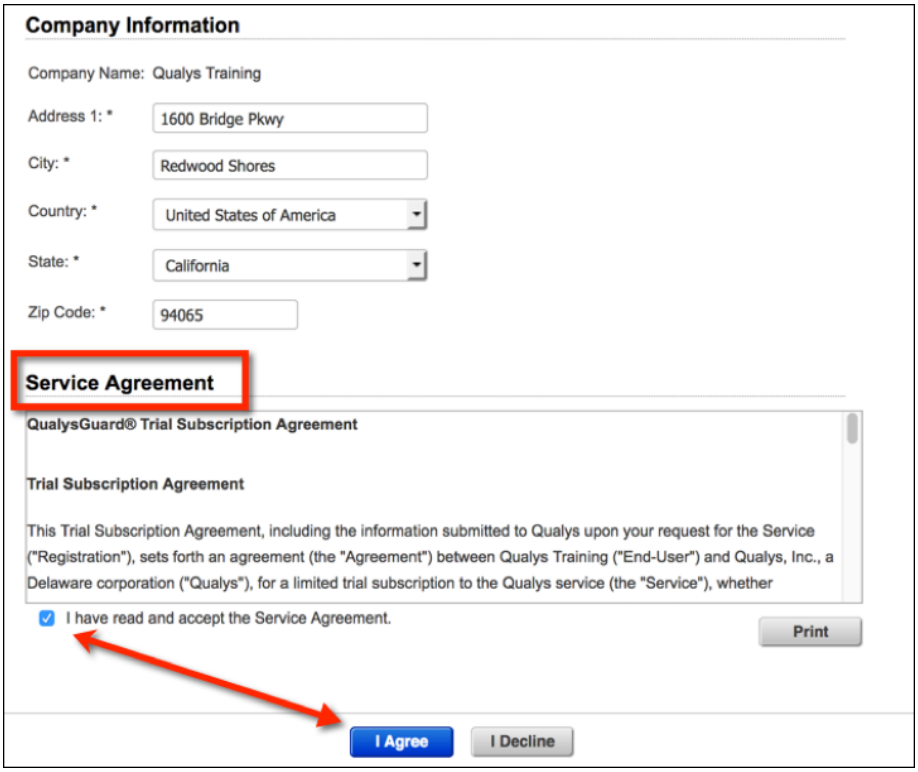


*For security, the Login username on this page appears partially obfuscated with ******.*

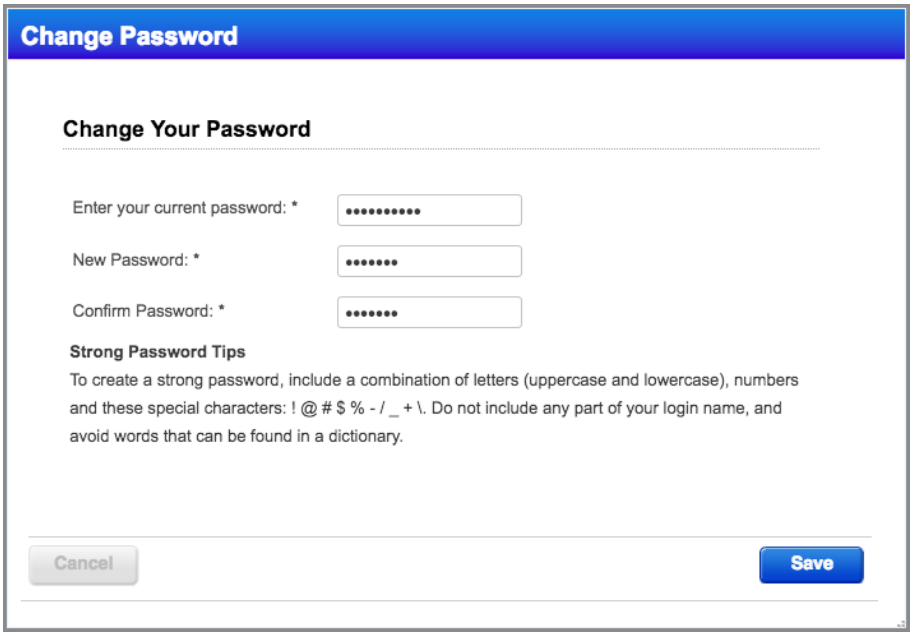
4. **Please, record your student trail account PASSWORD.**

5. **Use the link provided in the "password" document to login and activate your Qualys student trial account.**

   Presently, all student trial accounts run on US POD3: https://qualysguard.qg3.apps.qualys.com/. Please use this URL to login to your trial account, unless instructed otherwise, by a Qualys Trainer.



6. **Scroll down and select the check box to accept the "Service User Agreement" and click the "I Agree" button.**



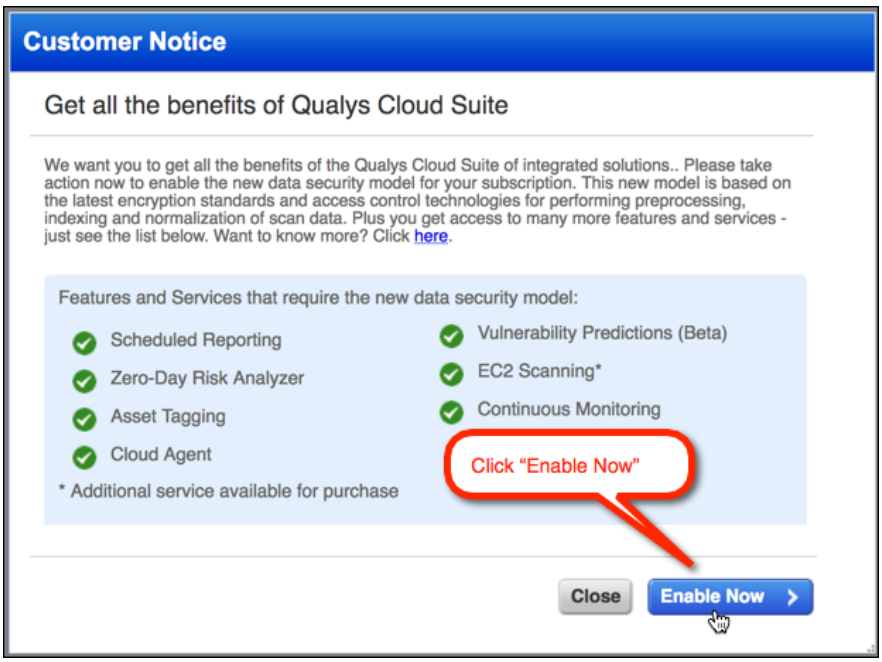
7. **Enter your current password, and then chose a new password (***please record your new password along with your trial account username***).**

8. **Click the "Save" button, followed by the "Close" button.**

9. **Log back in to your student account using your new credentials.**

   The New Data Security Model (NDSM) combines high performance disk encryption with Virtual Private Database (VPD) technology to ensure that your data is only visible and accessible to authorized users (i.e., users within your account subscription) that have valid authentication credentials.

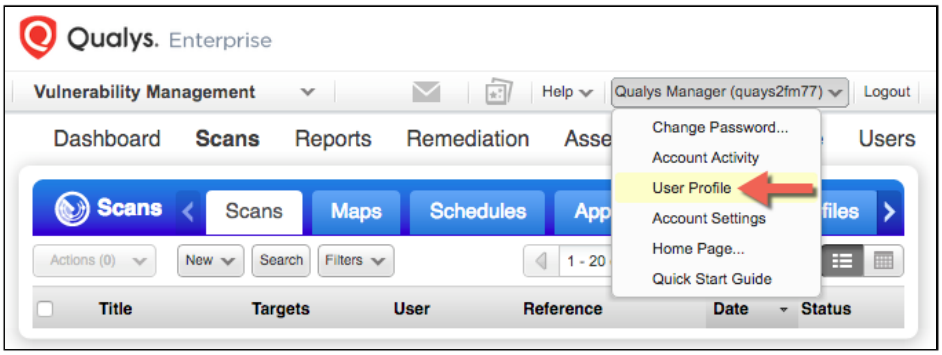
   Enabling the NDSM also provides advanced productivity and detection features:



10. **When you receive the "Customer Notice" pop-up window, click the "Enable Now" button.**

Update User Profile

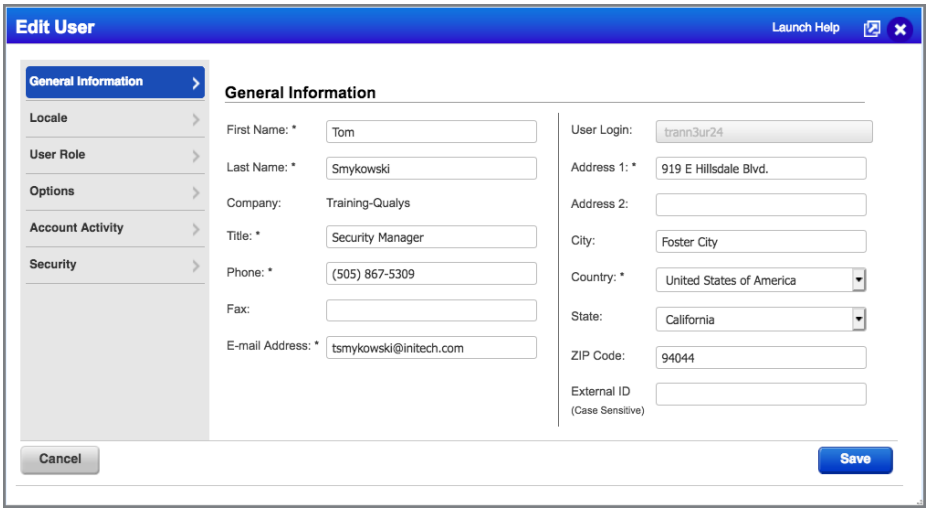
The steps that follow will help to personalize your student user account and make other adjustments that will provide a more effective training environment.



1. **Click on your User ID (located between "Help" and "Logout") and select the "User Profile" option.**

General Information

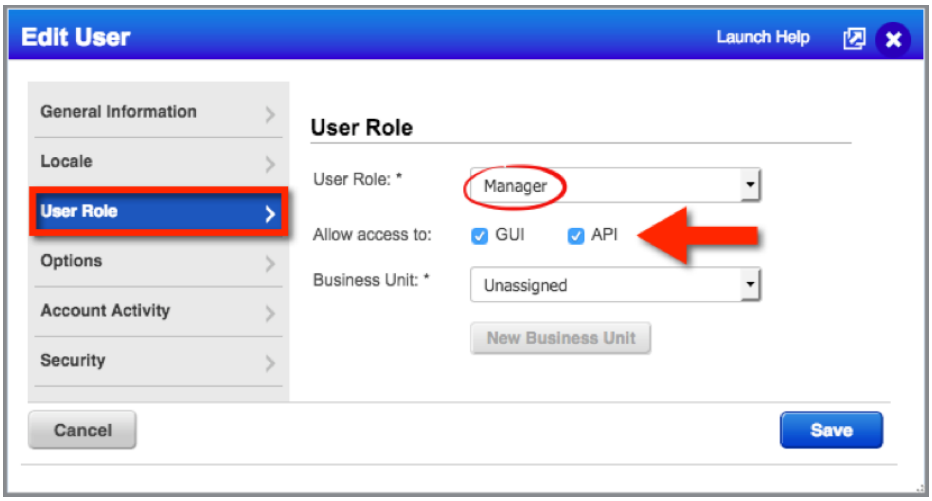
You may keep the default "General Information" settings (to save time) or make adjustments according to your personal preferences. All system and platform notifications will be sent to the email address specified on this page.



2. **Make any necessary adjustments to the "General Information" section of your user profile.**

User Role

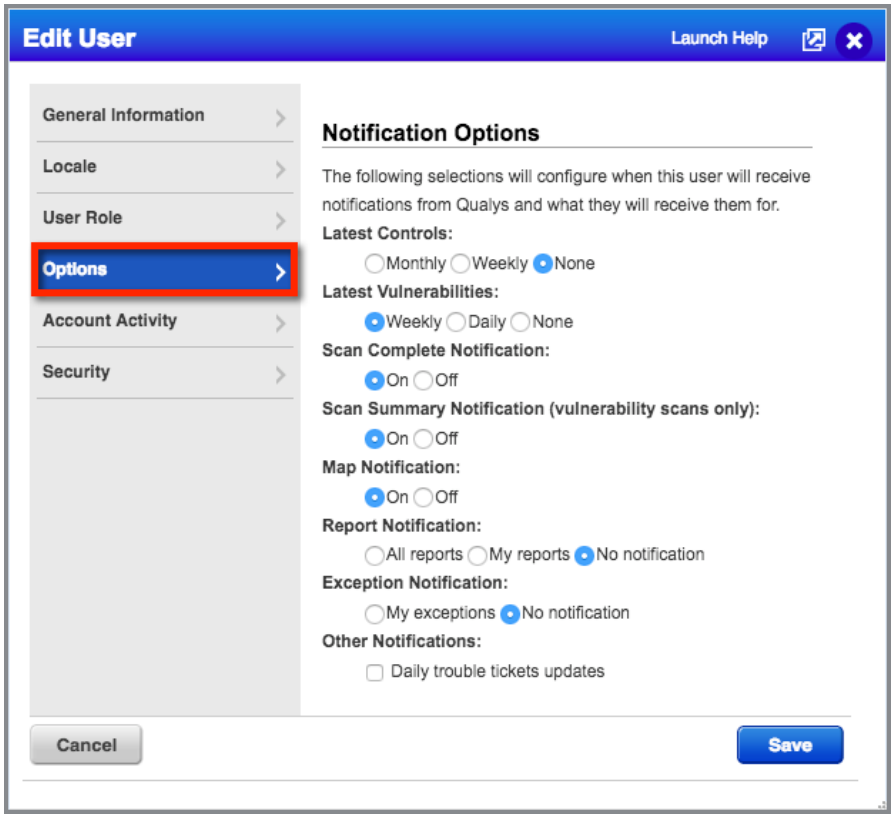
Different Qualys user accounts, take on different user roles.



3. **Click "User Role" in the navigation pane (left) and make note that your student account user role is: Manager, and you can access your account using the Graphical User Interface (GUI) or the Application Program Interface (API).**

Notification Options

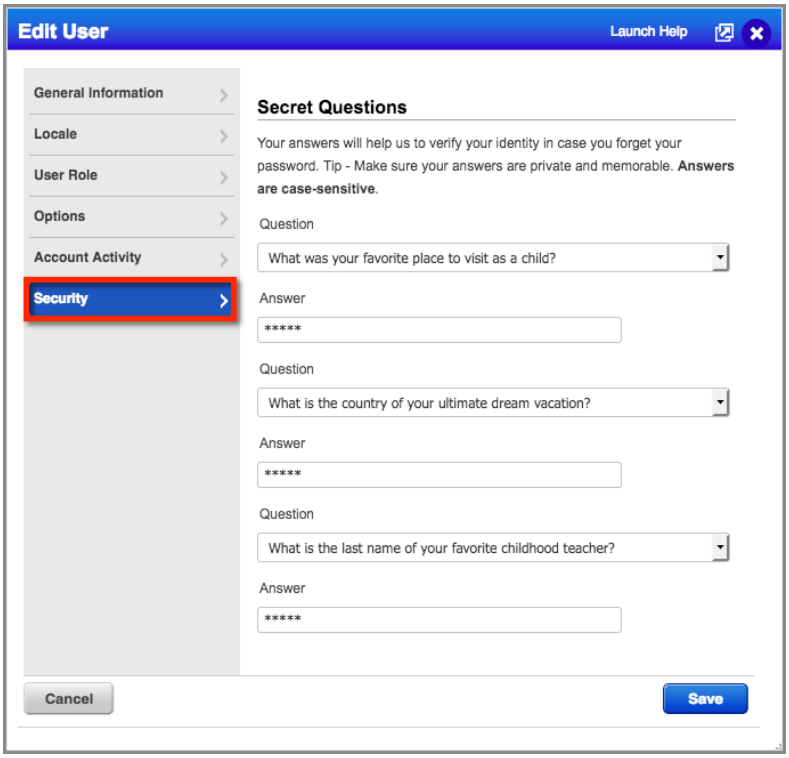
All notifications will be sent to the e-mail address specified in the "General Information" section.



4. **Click "Options" in the navigation pane (left) and make the appropriate selections for the type of notifications you would like to receive.**

Security

Security Questions are provided here to facilitate your password reset attempts.

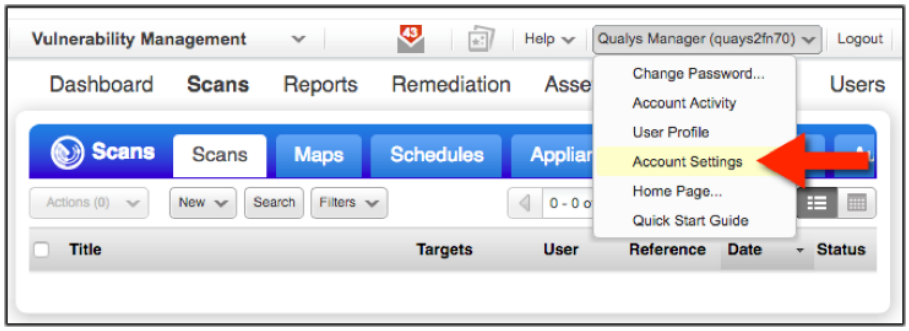


5. **Click "Security" in the navigation pane (left) and take a moment to complete the Security Questions.**
6. **Click the "Save" button.**

You'll need to provide the answers to your security questions, when using the "Forgot Password" link found on the Qualys Login page.

Account Settings

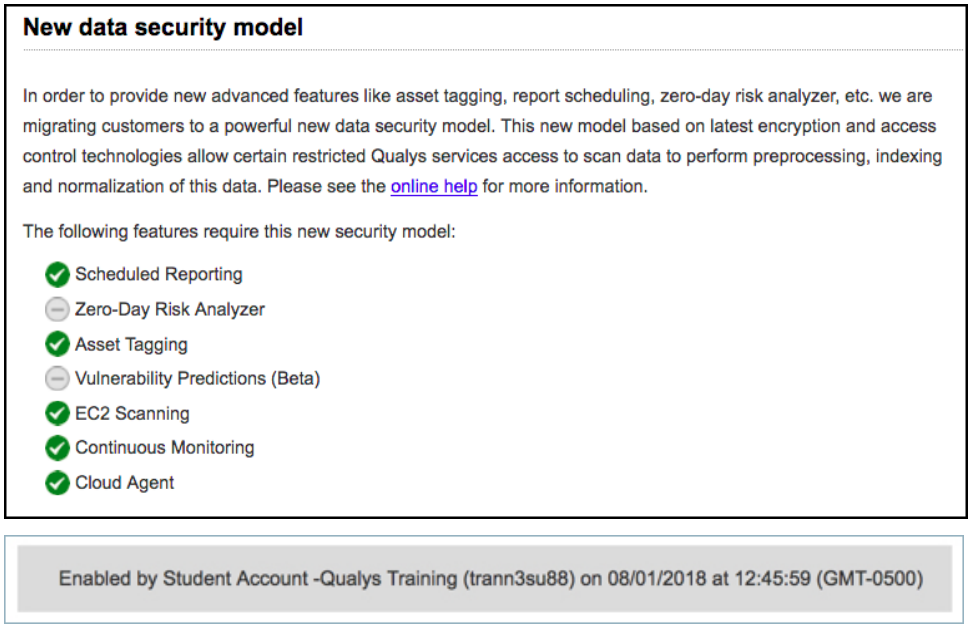
Changes made to account settings will affect all user accounts in your Qualys subscription.



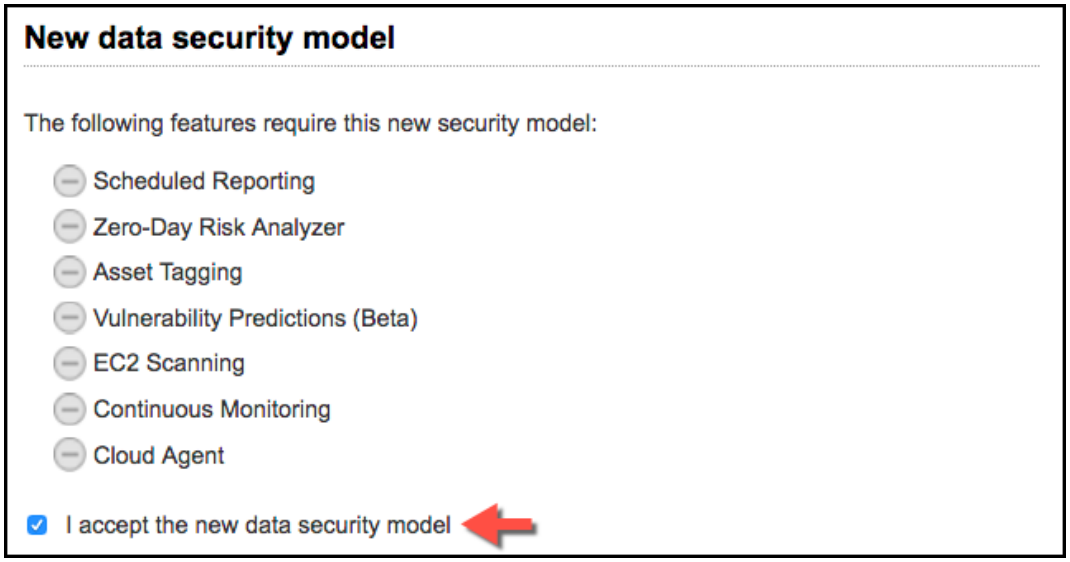
1. **Click on your User ID (located between "Help" and "Logout") and select the "Account Settings" option.**

2. **Click the "Security" setup option.**

3. **Scroll down to the "New Data Security Model" section.**



4. **Just below the NDSM settings ensure this feature has been enabled (as depicted above).**
5. **If the NDSM has not yet been enabled, select the check box to "accept the new data security model" (as depicted below).**



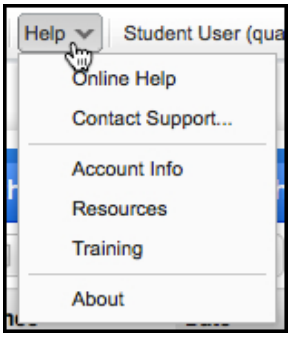
6. **Increase your Session Timeout value to the maximum (240 min.)**

   This adjustment will help you to maintain an ACTIVE session throughout the entire training class.

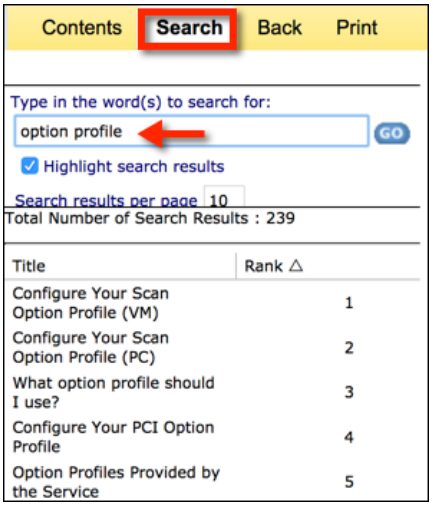
7. **Click the "Save" button, followed by the "Close" button.**

Context Sensitive Help/Online Manual

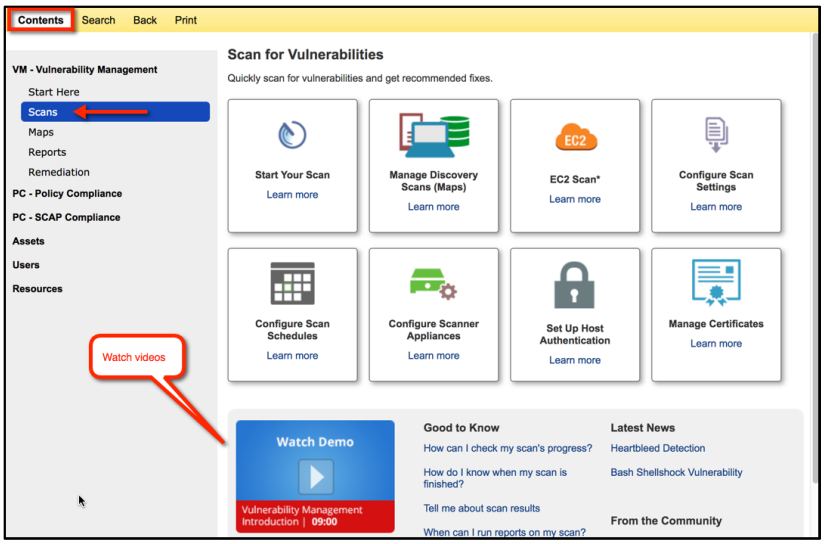
Online help is available for all Qualys applications and for everything in the User Interface.



1. **Click on the "Help" button in the upper right hand corner and select the "Online Help" option.**



The "Search" option will help you to find specific topics and provide links to helpful Qualys videos where applicable.



The "Contents" option will provide you with a start-to-finish explanation of Vulnerability Application tasks and features.

Add IP Assets to Your Account

Host Tracking

When adding host assets to your account, three basic methods are available for tracking discovered vulnerabilities:

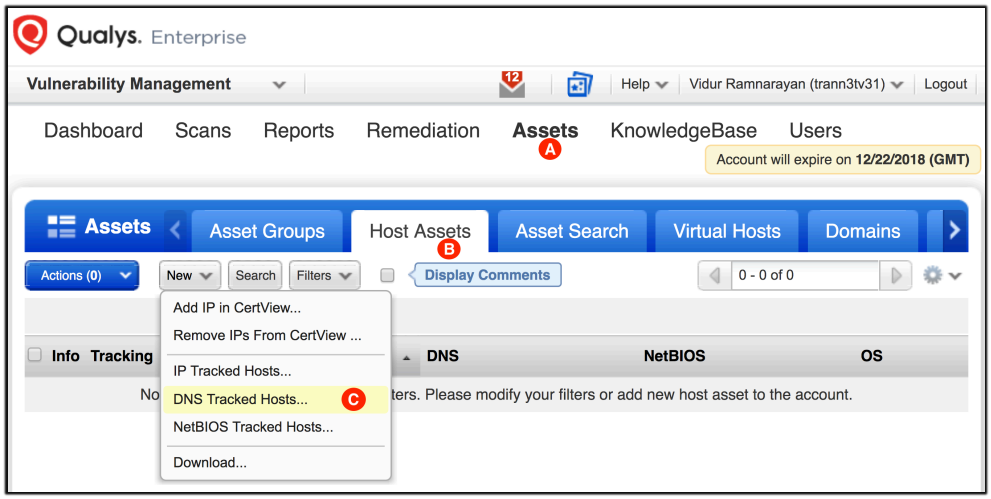
- Host IP Address
- Host DNS Name
- Host NetBIOS Name

A fourth host tracking method, the Qualys Host ID, is used by default, for all "Cloud Agent" host assets. The Qualys Host ID is unique for each host asset, and is available for "scannable" host assets, when the "Agentless Tracking" feature is enabled.

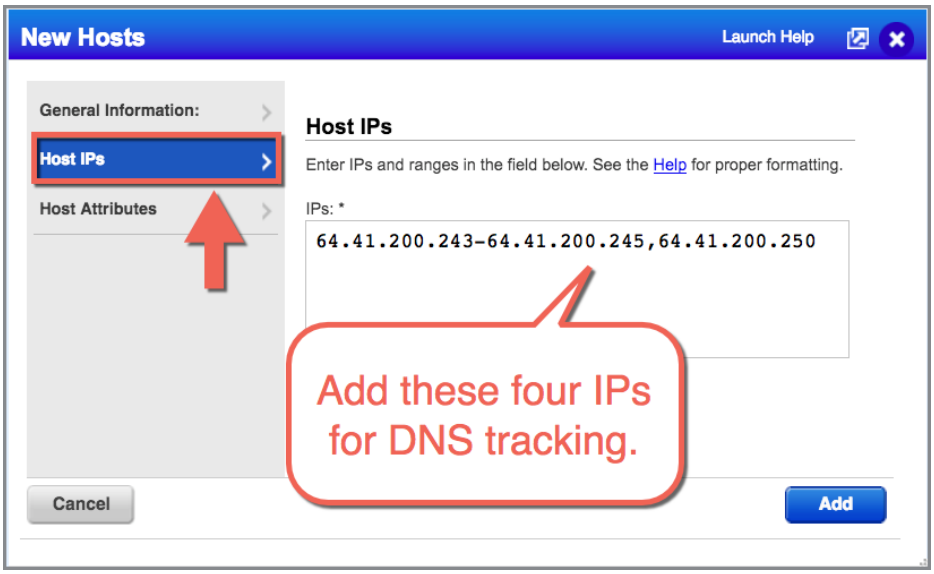
The main goal or objective is to choose a tracking method that is both unique and persistent, for each host.

DNS Tracked Hosts

Use DNS tracking for the Linux-based lab hosts.

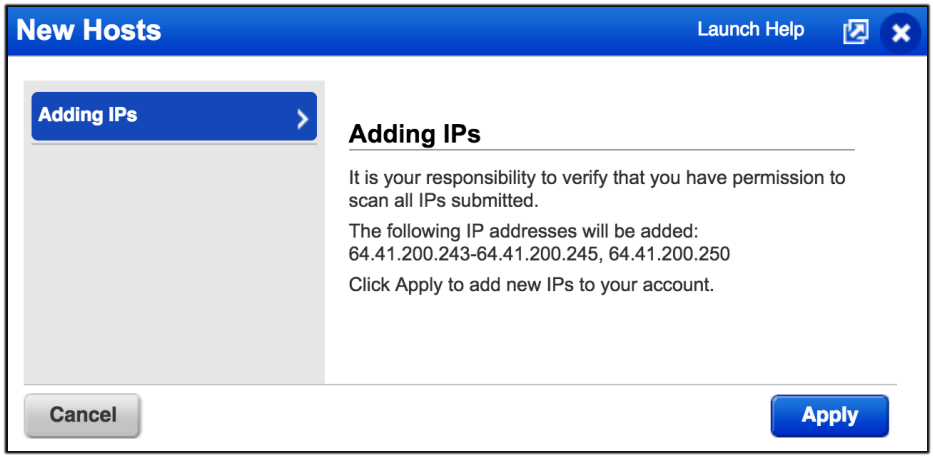


1. **Navigate to A) the "Assets" section, and then click B) the "Host Assets" tab.**
2. **Click the "New" button and select C) the option to track each host by its DNS name.** Tracking host vulnerabilities by DNS name maintains a consistent and accurate vulnerability history, even if the IP address changes.



3. **Click the "Host IPs" section (left navigation pane) and type the following IP address range into the "IPs:" field: `64.41.200.243-64.41.200.245,64.41.200.250`.**
4. **Click the "Add" button, to add all four IP addresses to your account.**

   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.



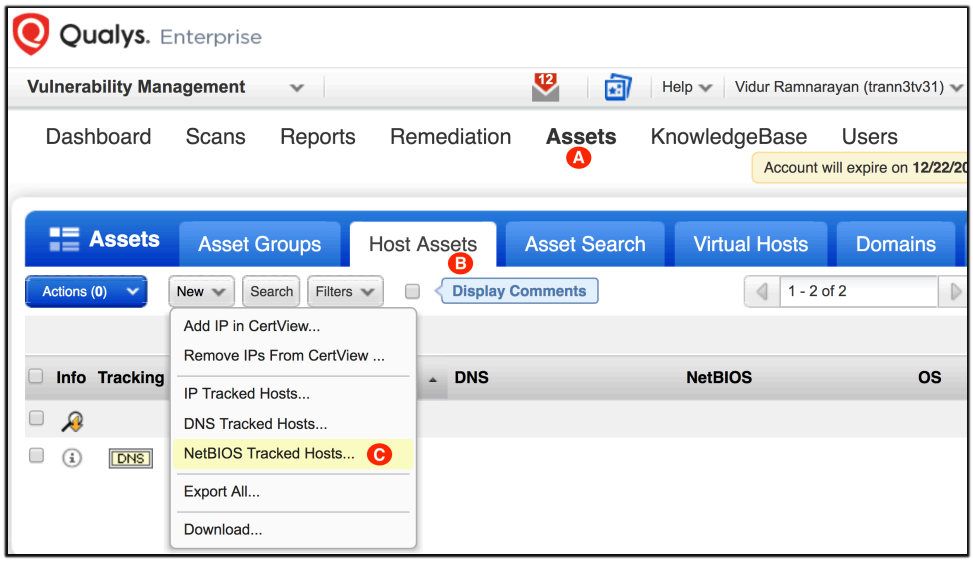
Important Notice about your student account

Using your student account, you have permission to scan only the demo IP addresses identified in this lab document. You do not have permission to scan any other IP addresses and/or web applications using your student account.

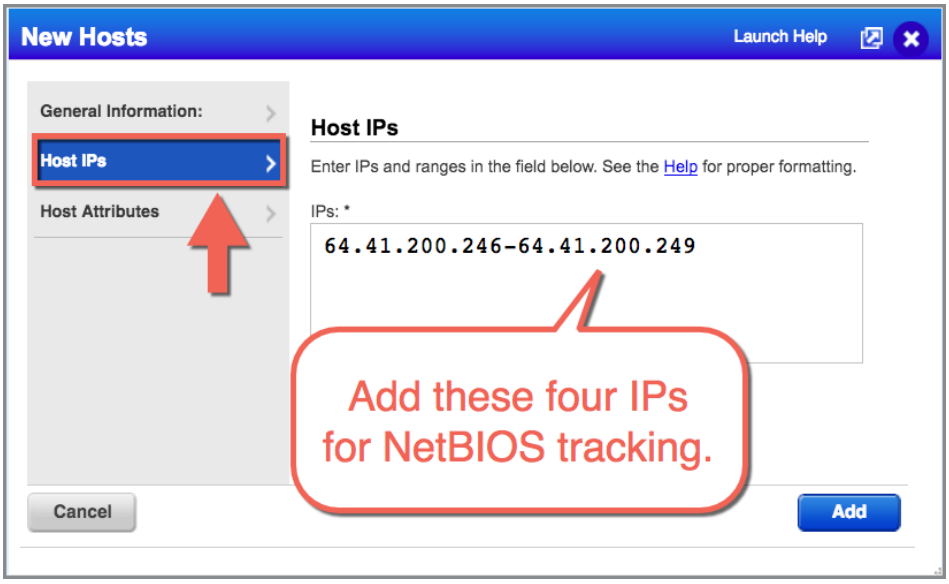
5. **Click the "Apply" button to acknowledge your scanning permission.**

NetBIOS Tracked Hosts

Use NetBIOS tracking for the Windows-based lab hosts.



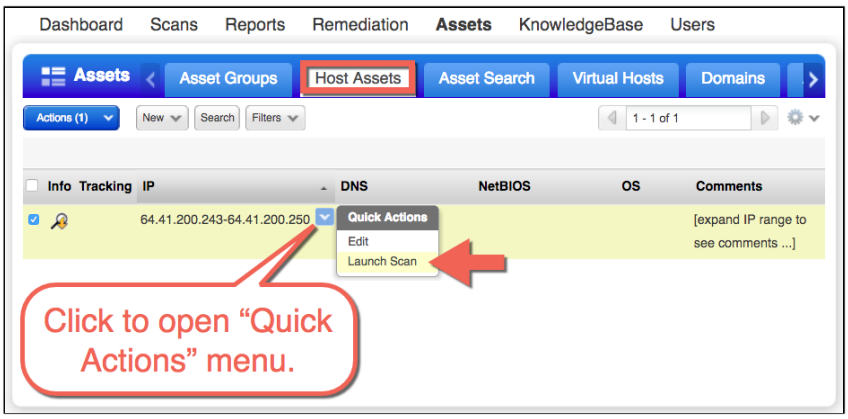
6. **Navigate to A) the "Assets" section, and click B) the "Host Assets" tab.**
7. **Click the "New" button and select C) NetBIOS Tracked Hosts.** Tracking host vulnerabilities by NetBIOS name maintains a consistent and accurate vulnerability history, even if the IP address changes.



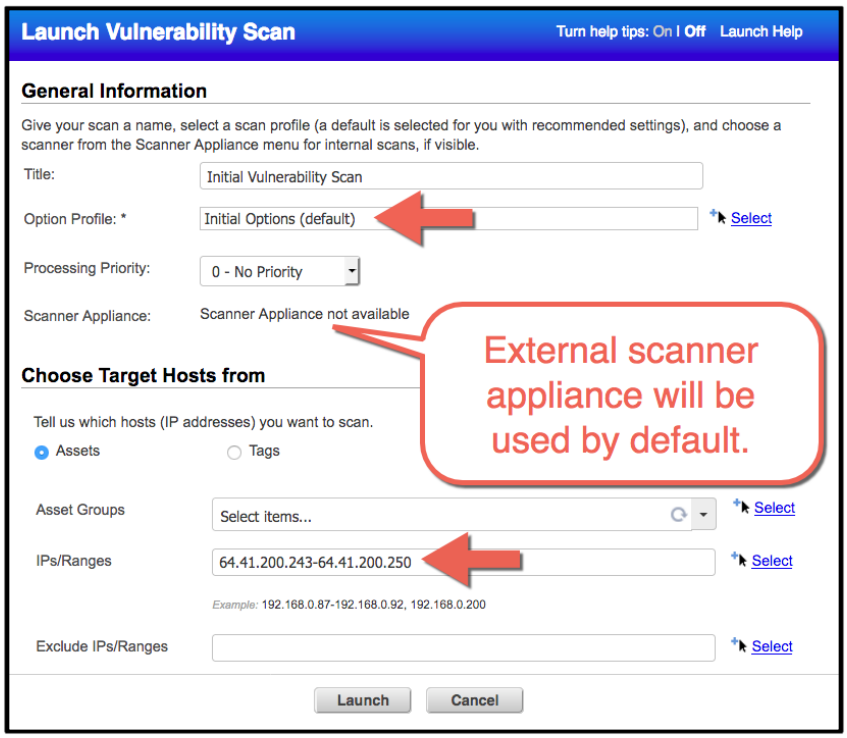
8. **Click the "Host IPs" section and type the following IP address ranges into the "IPs:" field: `64.41.200.246-64.41.200.249`.**
9. **Click the "Add" button, to add all four IP addresses to your account.**
10. **Click the "Apply" button to acknowledge your scanning permission.**

Launch Initial Scan

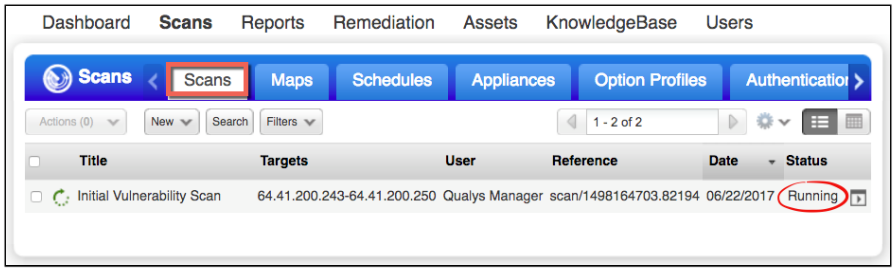
IPs that you add to the "Host Assets" tab are "Scannable" and may be targeted in successive vulnerability scans.



1. **From the "Host Assets" tab, use the "Quick Actions" menu to select the "Launch Scan" option.**



2. **Enter "Initial Vulnerability Scan" in the "Title" field.**
3. **Leave the "Option Profile" field set to the "Initial Options" default.**
4. **Verify the IP addresses targeted and click the "Launch" button.**
5. **Click the "Close" button, when the "Scan Status" window appears.**

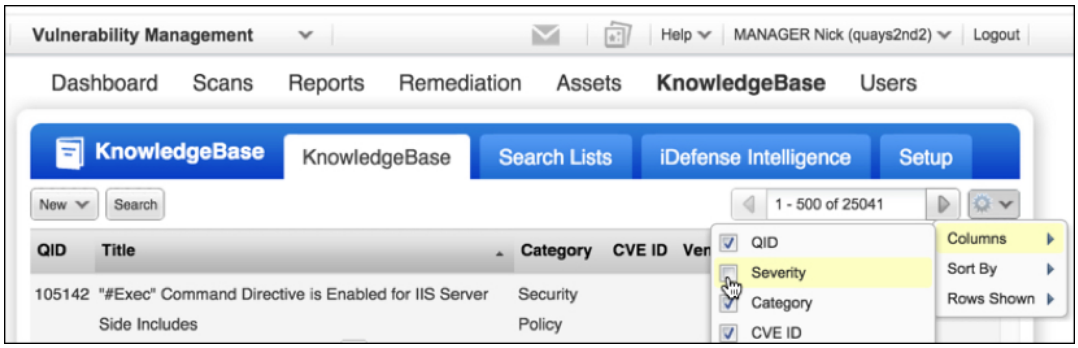


6. **To monitor the progress of your scan, navigate to the "Scans" section, and click the "Scans" tab.**

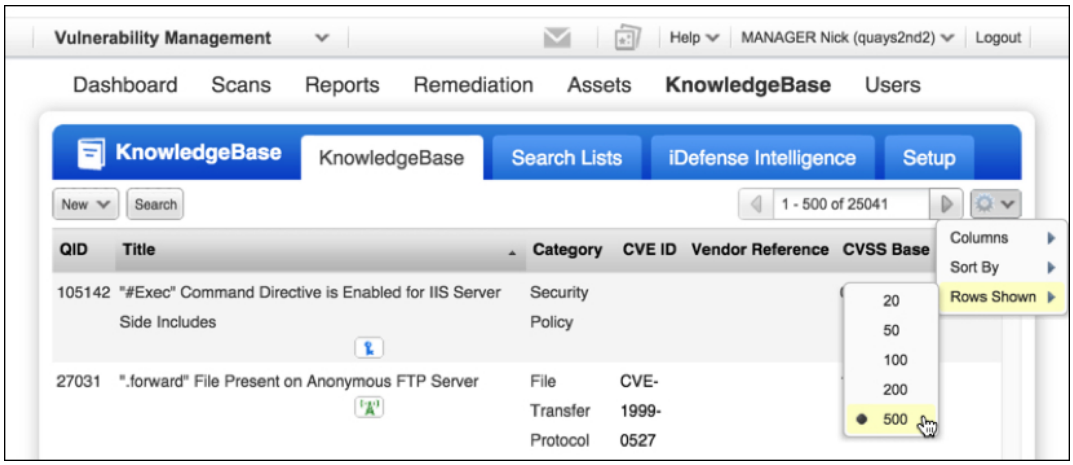
LAB 2: KnowledgeBase & Search Lists (10 min.)

Customize the KnowledgeBase

The Qualys KnowledgeBase provides the most current and comprehensive vulnerability and threat intelligence information. The next few steps will help you to personalize the KnowledgeBase settings.



1. **Go to the "KnowledgeBase" tab.**
2. **Click on the icon and add the "Severity" column to your default view.**



3. **Change the number of rows you can view to the maximum value.**

Search List

A "Search List" is an extension of the Qualys KnowledgeBase. It is one of the most powerful filtering and customization tools within the Vulnerability Management application. In the lab exercises that follow this one, you will:

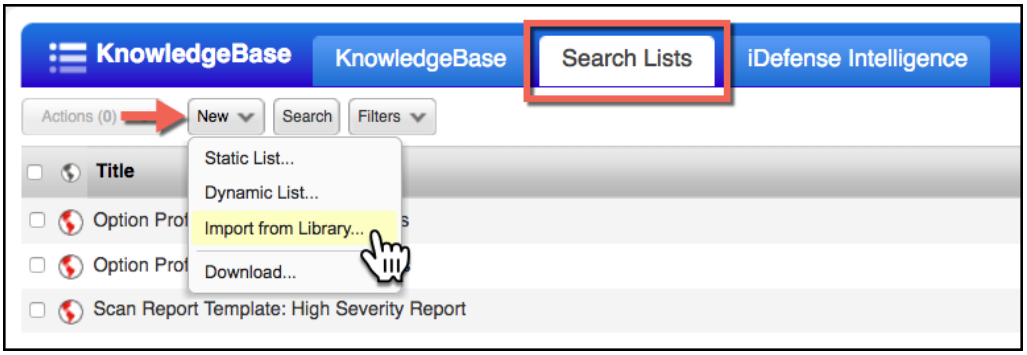
- Add a Search List to an Option Profile, to scan for Sev. 4 and Sev. 5 vulnerabilities, exclusively.
- Add a Search List to a Report Template, to focus on high severity vulnerabilities, that are also patchable.
- Add a Search List to a Remediation Policy, to automatically ignore "Low Risk" vulnerabilities.

The name "Search List" is derived from the KnowledgeBase "Search" tool that is often used to create a list of vulnerabilities.

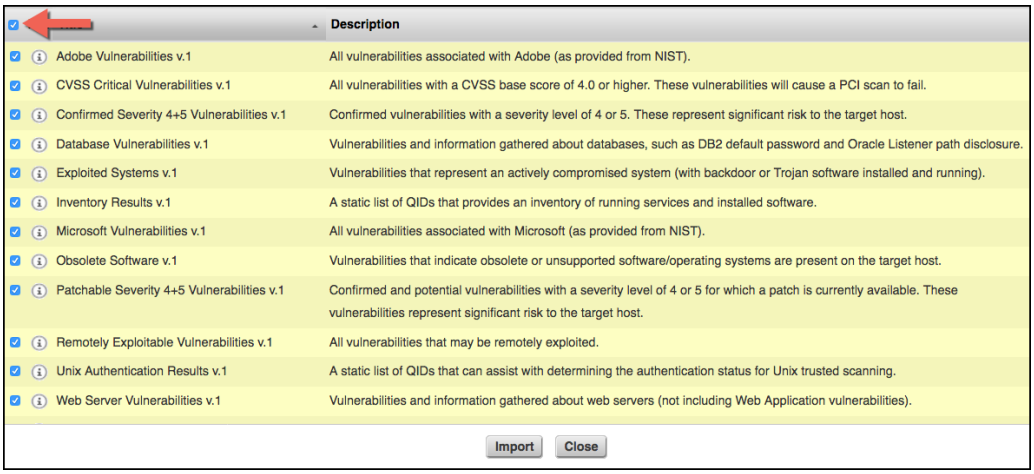
A Dynamic Search list is automatically updated by the Qualys service in conjunction with updates to the Qualys KnowledgeBase. A Static Search list does not receive automatic updates. Typically, static lists are used to collect vulnerabilities that do not have a common criterion.

Search List Library

Qualys has created a library of some very useful Search Lists. You'll find a "Search Lists" tab under the Scans, Reports, and KnowledgeBase sections. All three tabs perform the same function.



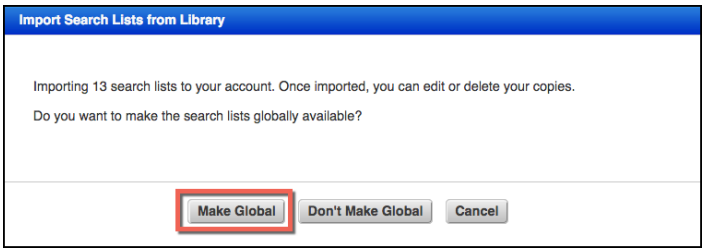
1. **Navigate to any one of the "Search Lists" tabs (i.e., Scans, Reports, or KnowledgeBase sections), click the "New" button and select the "Import from Library" option.**



	Description
Adobe Vulnerabilities v.1	All vulnerabilities associated with Adobe (as provided from NIST).
CVSS Critical Vulnerabilities v.1	All vulnerabilities with a CVSS base score of 4.0 or higher. These vulnerabilities will cause a PCI scan to fail.
Confirmed Severity 4+5 Vulnerabilities v.1	Confirmed vulnerabilities with a severity level of 4 or 5. These represent significant risk to the target host.
Database Vulnerabilities v.1	Vulnerabilities and information gathered about databases, such as DB2 default password and Oracle Listener path disclosure.
Exploited Systems v.1	Vulnerabilities that represent an actively compromised system (with backdoor or Trojan software installed and running).
Inventory Results v.1	A static list of QIDs that provides an inventory of running services and installed software.
Microsoft Vulnerabilities v.1	All vulnerabilities associated with Microsoft (as provided from NIST).
Obsolete Software v.1	Vulnerabilities that indicate obsolete or unsupported software/operating systems are present on the target host.
Patchable Severity 4+5 Vulnerabilities v.1	Confirmed and potential vulnerabilities with a severity level of 4 or 5 for which a patch is currently available. These vulnerabilities represent significant risk to the target host.
Remotely Exploitable Vulnerabilities v.1	All vulnerabilities that may be remotely exploited.
Unix Authentication Results v.1	A static list of QIDs that can assist with determining the authentication status for Unix trusted scanning.
Web Server Vulnerabilities v.1	Vulnerabilities and information gathered about web servers (not including Web Application vulnerabilities).

Import Close

2. **Click the top-level check box to select all lists in the library and click the "Import" button.**



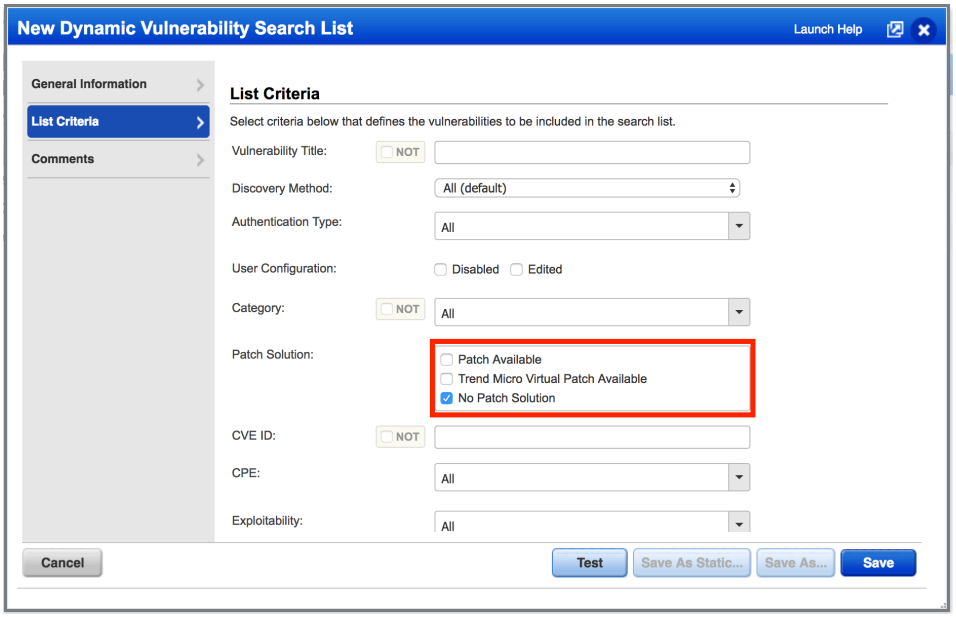
The "Global" option allows you to control the visibility of the objects you create or import. If you make an object "Global" it will be visible to other users (Scanners, Readers, etc…) within your Qualys subscription.

3. **Click the "Make Global" button.**

Create Dynamic Search List

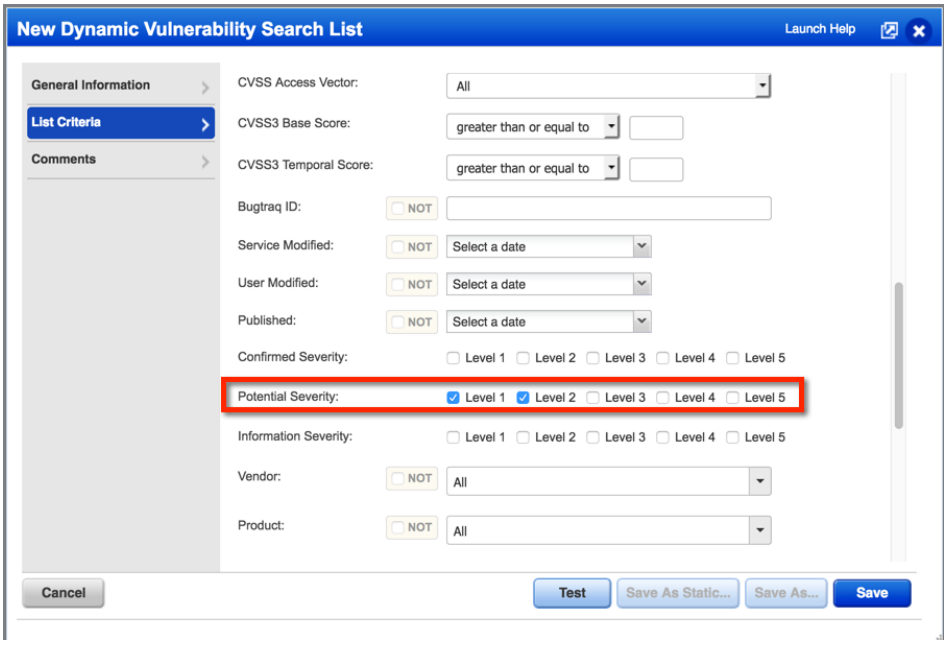
Objective: create a list of "Low Risk" vulnerabilities (i.e., severity 1 and 2) that have a potentially HIGH remediation cost. Later, during the Remediation lab exercises, you will use this custom list to create a Policy to ignore these "Low Risk – High Cost" vulnerabilities.

1. **Navigate to any of the three "Search Lists" tabs.**
2. **Click the New button and select the "Dynamic List" option.**
3. **In the "Title" section, give it the name "Low Severity Vulns (Sev. 1 and 2) no patch".**



4. **Select "List Criteria" in the navigation pane.**
5. **Scroll down and select the "No Patch Solution" check box.**

   Vulnerabilities that do not have a patch solution typically take more time to mitigate, and therefore cost more to resolve than vulnerabilities that already have a patch.



6. **Scroll down and choose Levels 1 and 2 for Potential Severities.** *Remember*: a potential vulnerability may require extra time for manual investigation.

7. **Save the List.**

   This list of "Low Impact" vulnerabilities will provide a good resource later, when you build a Remediation Policy that demonstrates the steps for "ignoring" a list of vulnerabilities.

LAB 3: Vulnerability Assessment (20 min.)

Qualys provides multiple technologies for collecting vulnerability assessment data:

- Qualys Scanner Appliance
- Qualys Cloud Agent
- Qualys Sensor

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

Alternatively, please see Appendix E for steps to install Qualys Cloud Agent.

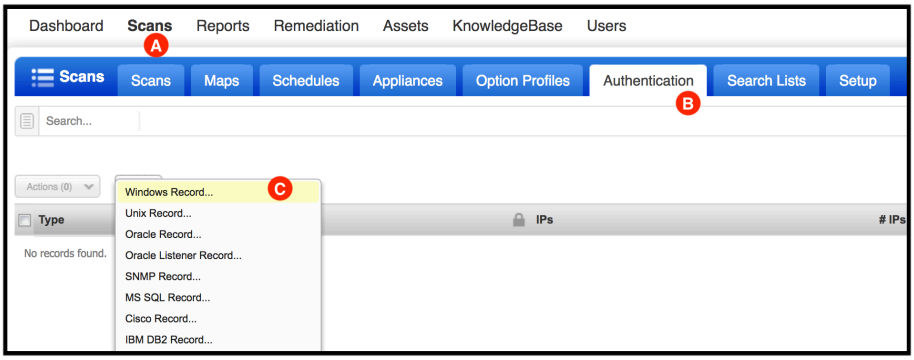
Trusted Scanning

Qualys recommends performing vulnerability scans in "authenticated" mode or what we call "trusted" scanning. Performing a "trusted" scan requires one or more authentication records.

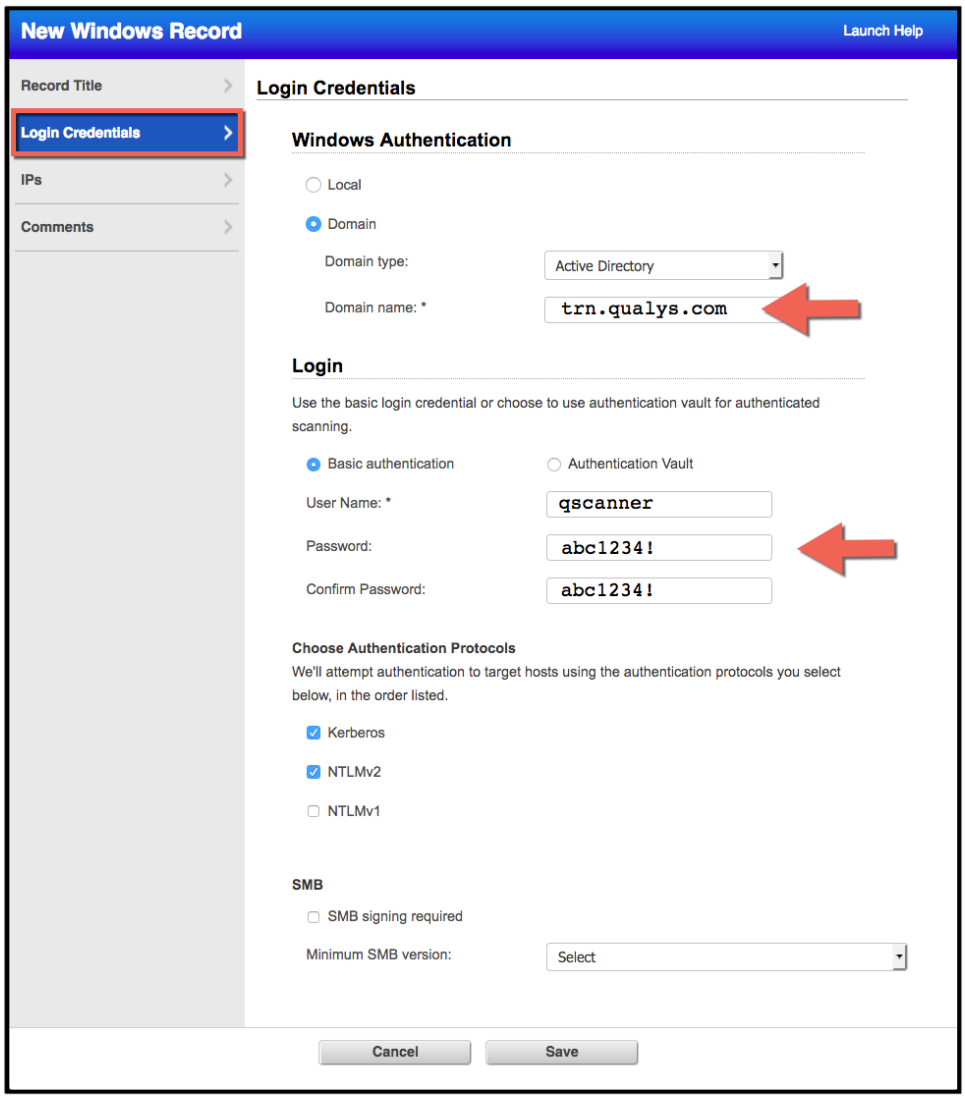
In this exercise, you'll create a Windows authentication record, a UNIX authentication record, and an Option Profile that uses them.

Windows Authentication Record

Create a Windows Active Directory authentication record with an account that is a member of the Domain Admins user group.



1. **Navigate to A) the "Scans" section, and click B) the "Authentication" tab.**
2. **Click the "Hide Graph" option, near the upper-right corner of the "Overview" pane.**
3. **Click the "New" button and select C) the "Windows Record…" option.**
4. **Enter "Domain Admin" as the "Title" for the Authentication Record.**



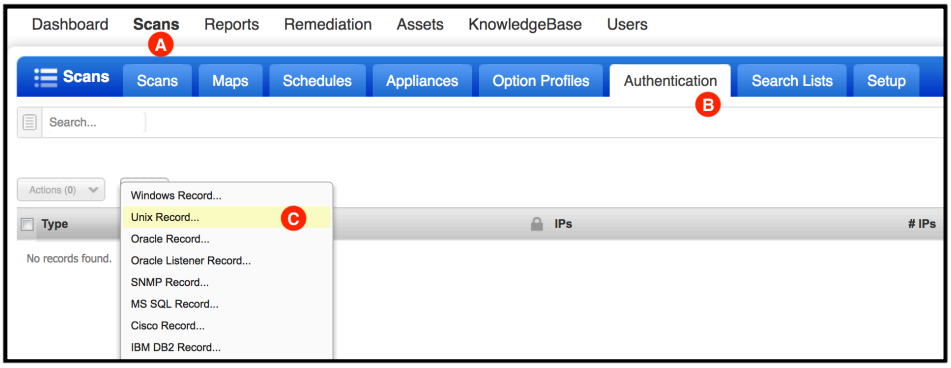
5. **Click "Login Credentials" in the navigation pane (left).**
6. **Leave the "Domain" radio button selected, and use the "Domain Type" drop-down menu to select the "Active Directory" option.**
7. **Enter "trn.qualys.com" (omit quotes) in the "Domain name" field.**
8. **Enter "qscanner" (omit quotes) in the "User Name" field and "abc1234!" (omit quotes) in the "Password" fields.**

   The "qscanner" user account is a member of the Domain Admins user group within the "trn.qualys.com" domain.
9. **Click the "Save" button to complete the creation of your new Authentication Record.**

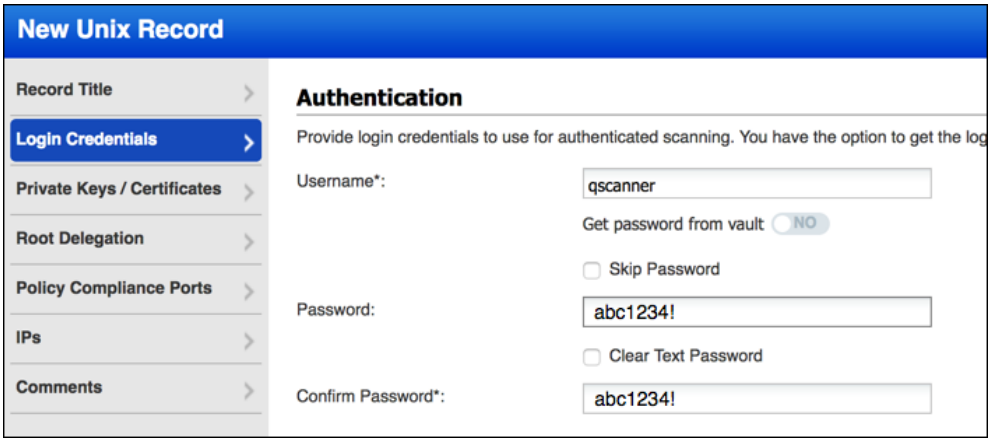
   IP addresses are not required for Active Directory authentication records. This information will be collected at scan-time, using an Active Directory API call.

Unix Authentication Record

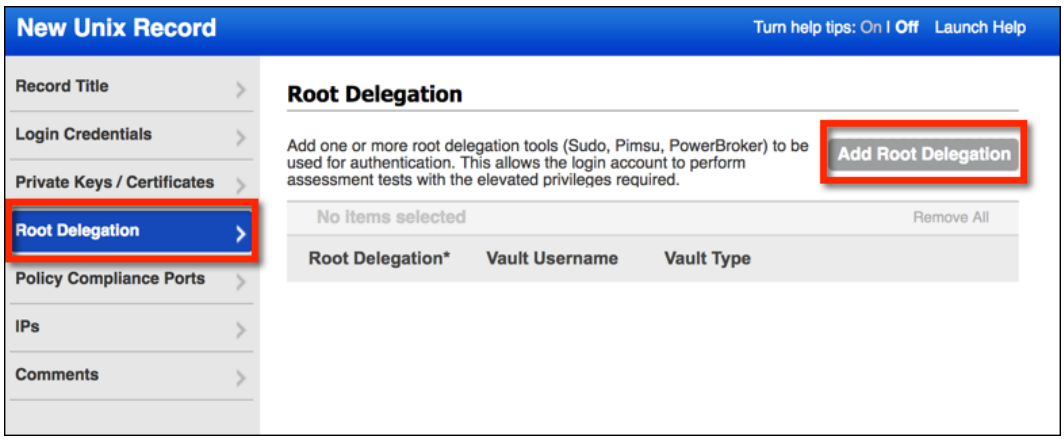
Create a Unix authentication record that uses “sudo” for root delegation.



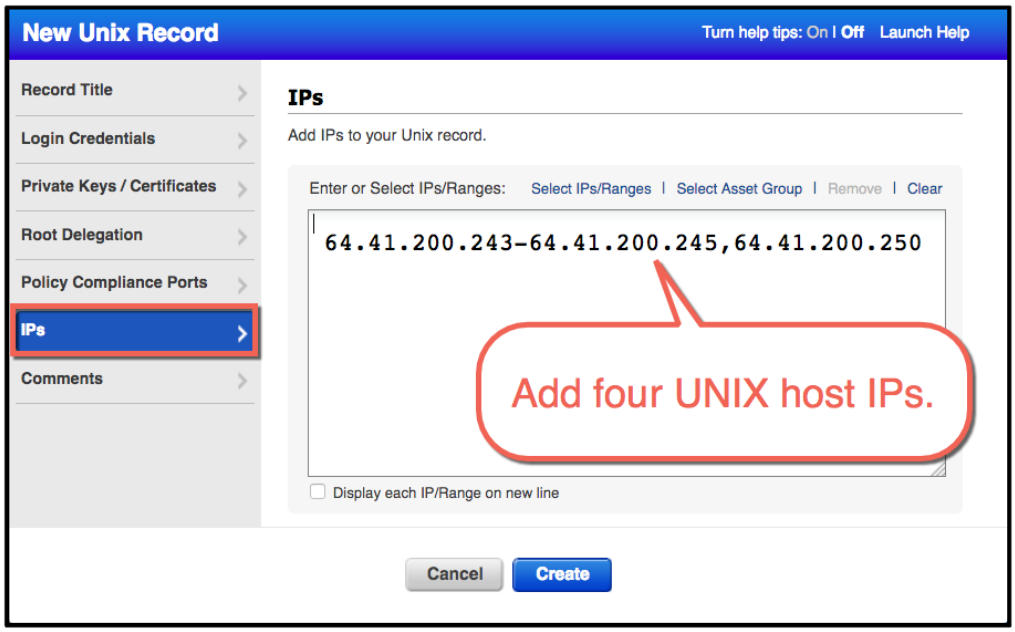
1. **Navigate to A) the “Scans” section and select B) the “Authentication” tab.**
2. **Click the “New” button and select C) the “Unix Record…” option.**
3. **Type “qscanner with Sudo” in the “Title” field.**



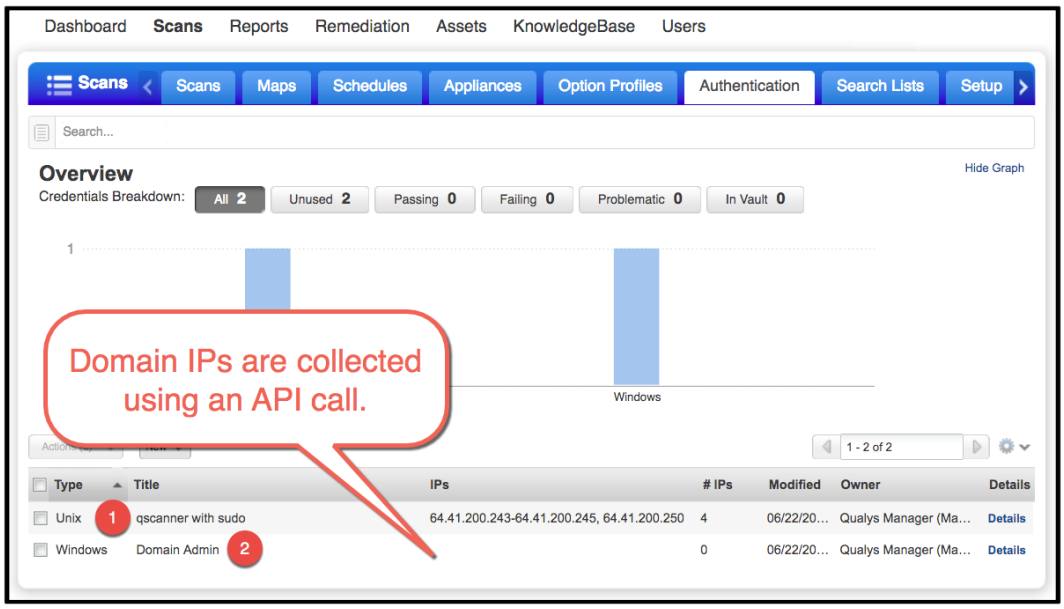
4. **Click “Login Credentials” in the navigation pane, and enter “qscanner” (omit quotes) in the “User Name” field and “abc1234!” (omit quotes) in the “Password” fields.**



5. **Click "Root Delegation" in the navigation pane and click the "Add Root Delegation" button on the right.**
6. **Select "Sudo" from the dropdown menu for "Root Delegation".**
7. **Enter "abc1234!" (omit quotes) in the "Password" field.**
8. **Click the "Save" button.**



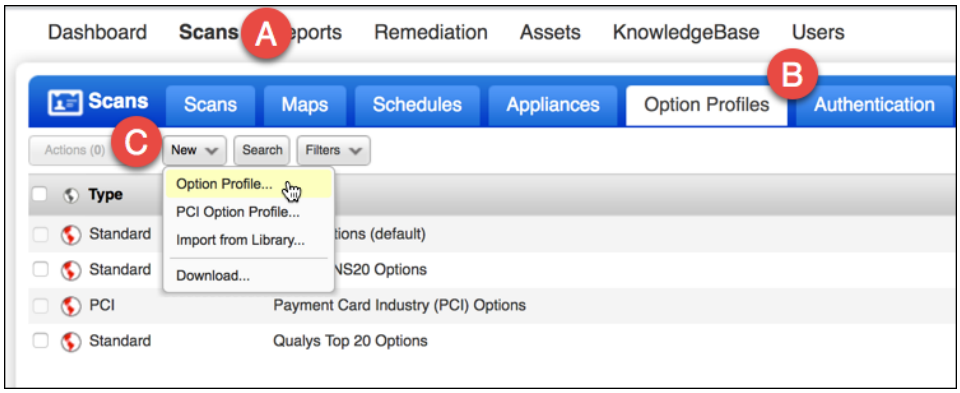
9. **Click "IPs" in the navigation pane (left), and enter the four IPs of your Unix-based host assets: `64.41.200.243-64.41.200.245,64.41.200.250`.**
10. **Click the "Create" button to complete the creation of your new Authentication Record.**



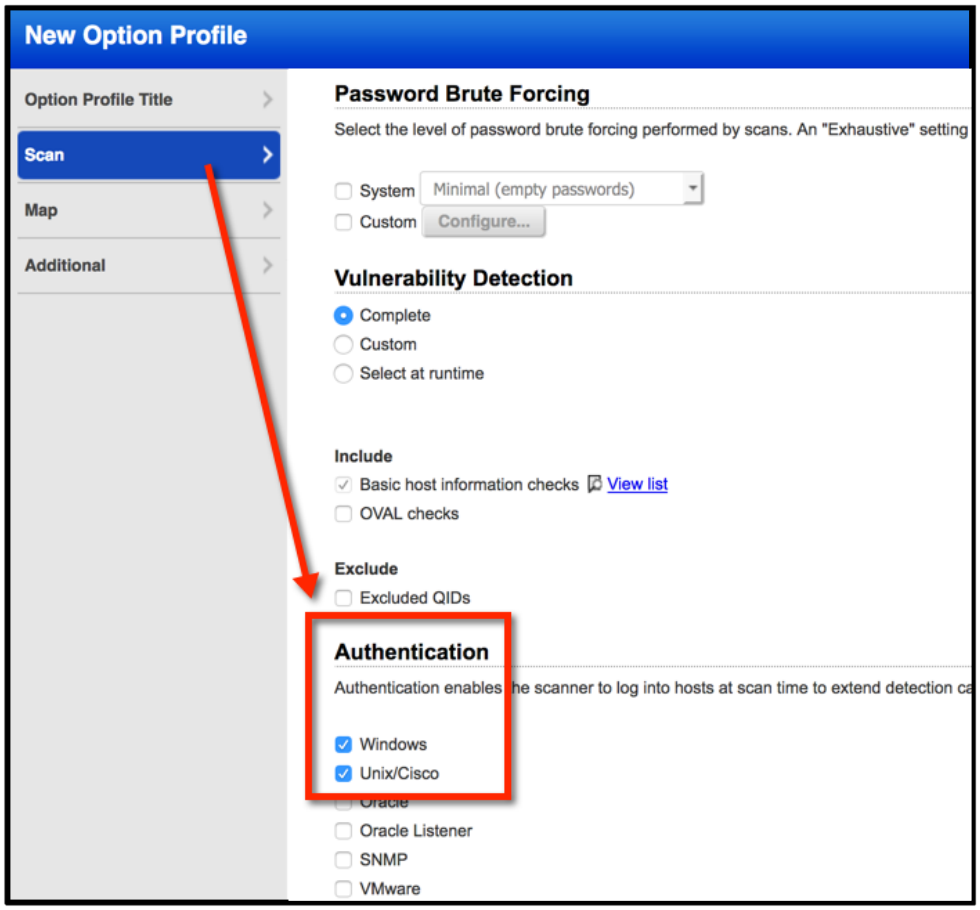
A distinction between these two auth. records is the noticeable lack of IP addresses from the Windows Domain record. The IPs for a Windows Domain authentication record are collected at scan-time, using an API call to the Windows Domain service.

Create Option Profile

Authentication isn't enabled by default and must be selected within an Option Profile.

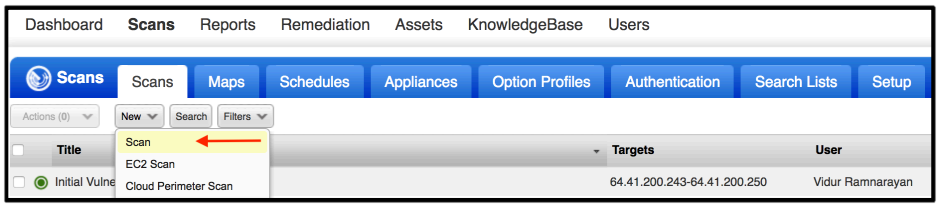


1. **Navigate to A) the "Scans" section, and click B) the "Option Profile" tab.**
2. **Click C) the "New" button and select the "Option Profile" option.**
3. **Enter "Custom Authentication" in the "Title" field.**
4. **Click "Scan" in the left navigation panel.**

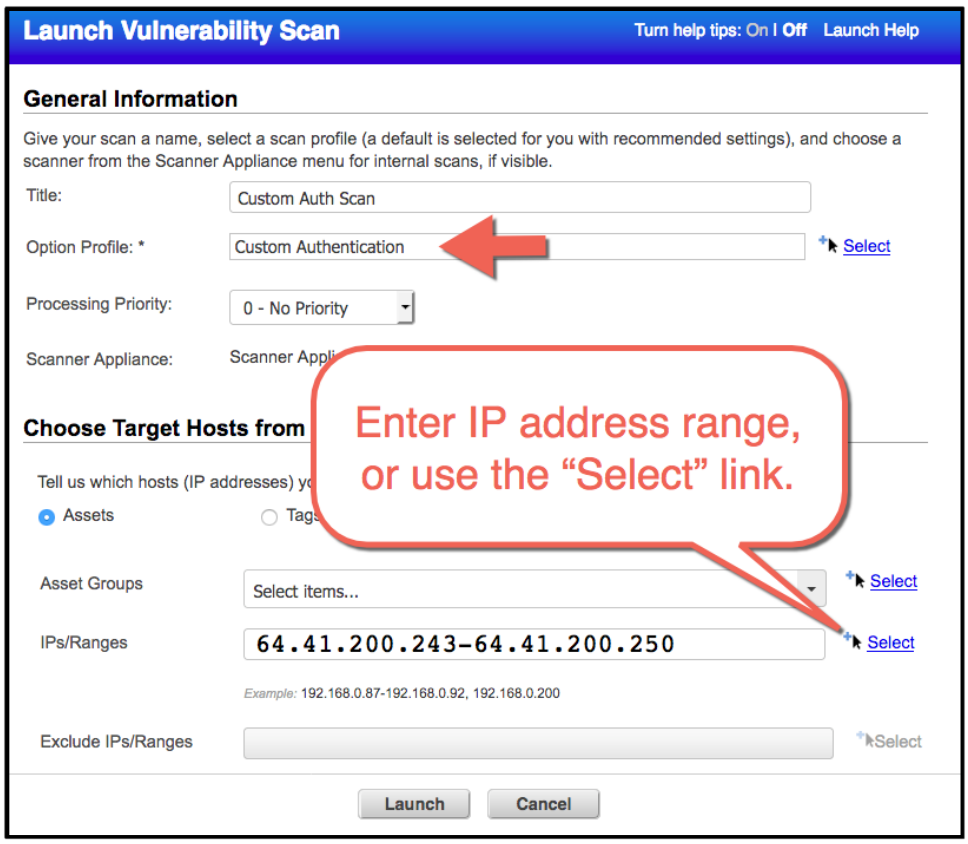


5. **Scroll down and locate the "Authentication" section and enable the Windows and Unix/Cisco authentication methods.**
6. **Scroll down further and click the "Save" button.**

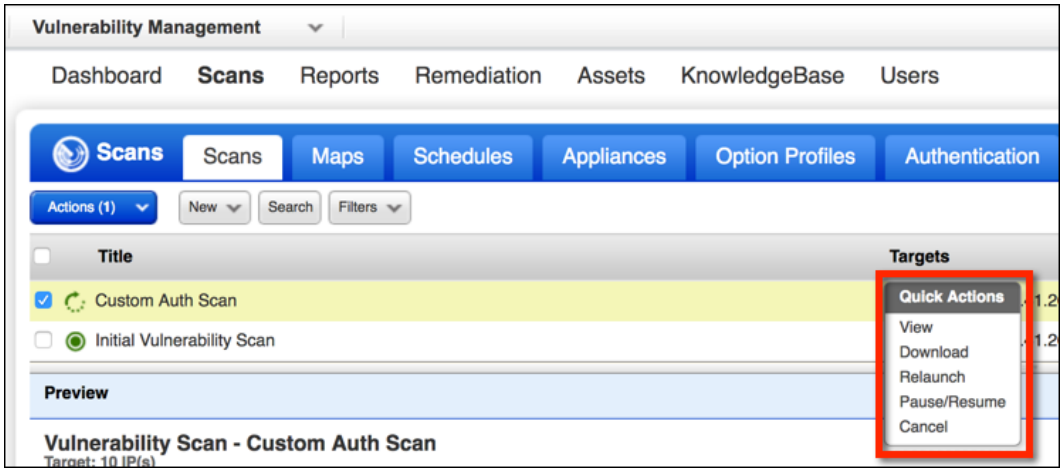
Launch Authenticated Scan



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



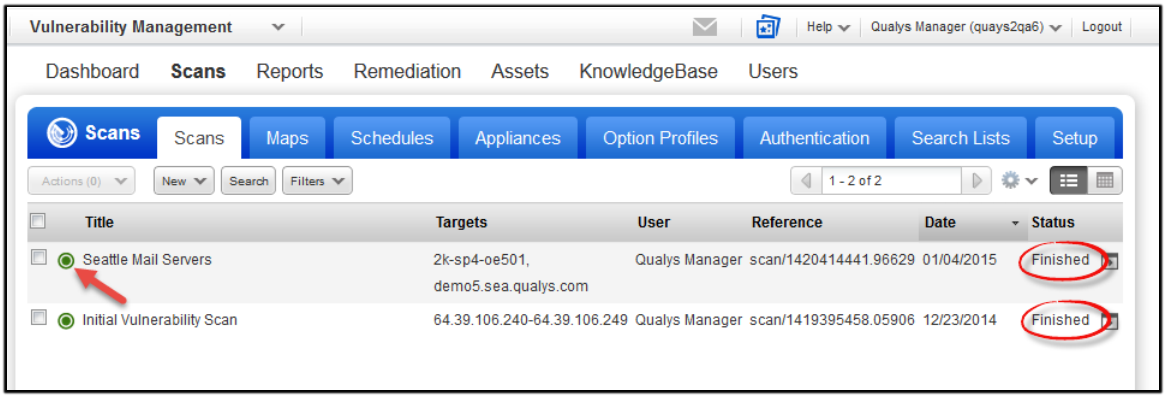
2. **Enter the Title: Custom Auth Scan.**
3. **Select the "Option Profile" you just created (Custom Authentication).**
4. **In the "Choose Target Hosts from" section, enter the IP address range for all host IPs (64.41.200.243-64.41.200.250), or click the "Select" link to select all IPs from a list.**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

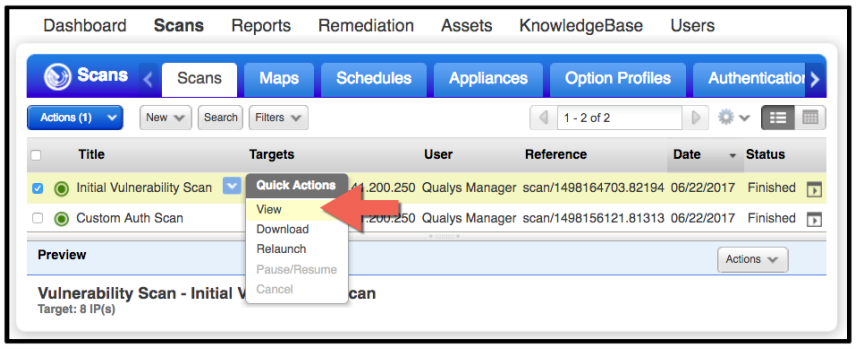
When a Scanner Appliance has finished performing a vulnerability scan, the scan results are sent to the Qualys Secure Operations Center (SOC). The raw scan data is then processed and integrated with the "Host Based Findings" within your subscription.



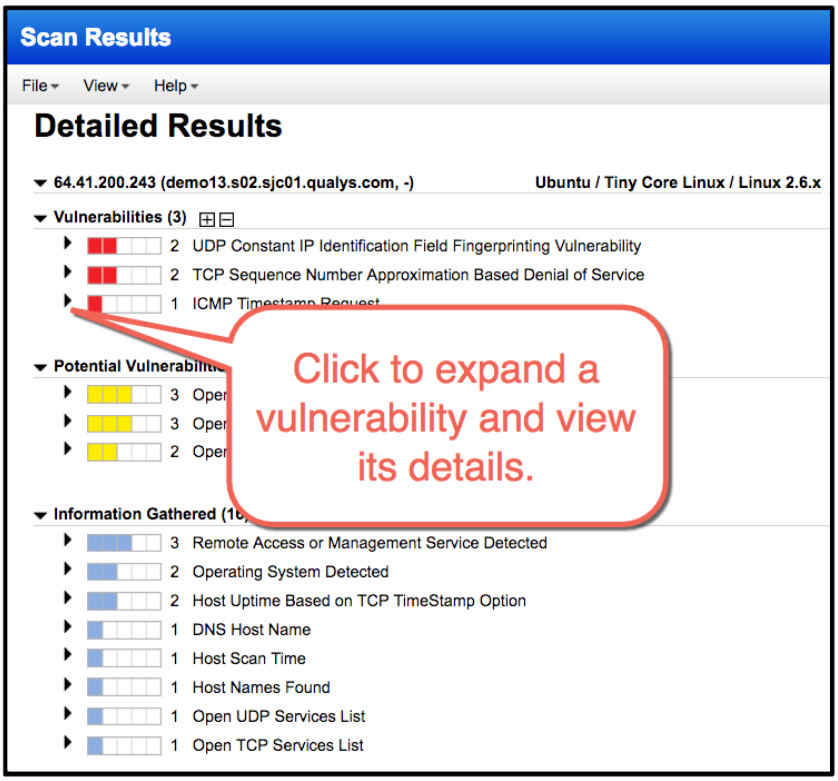
Although the "Status" column may display the "Finished" status, your scan results will not be available for use until the ○ icon changes to the ◉ icon (as illustrated above).

View Scan Results

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



1. **Choose any "Finished" scan and use its "Quick Actions" menu to select the "View" option.**
2. **Scroll down past the "Report Summary" and graphic illustrations, until you reach the "Detailed Results" section.**



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.

3. **You may close the scan results, when you are finished viewing its findings.**

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

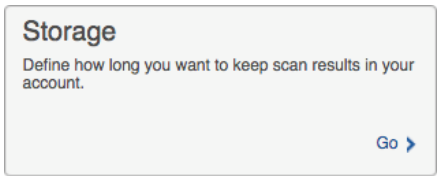
Severity Levels

Level 5	Remote root/administrator privileges	Remote control over system with Admin
Level 4	Remote user privileges	Remote control over system with user
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

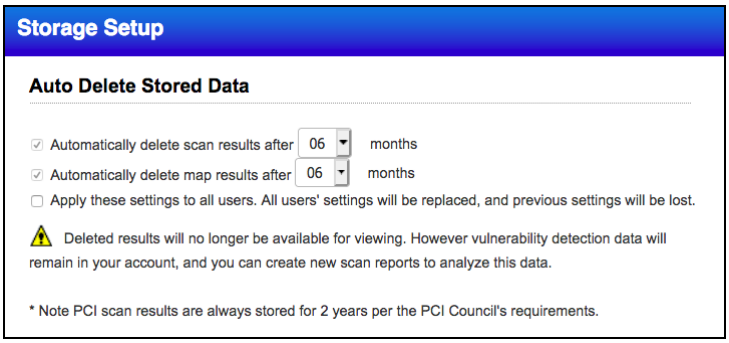
Storage

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.**

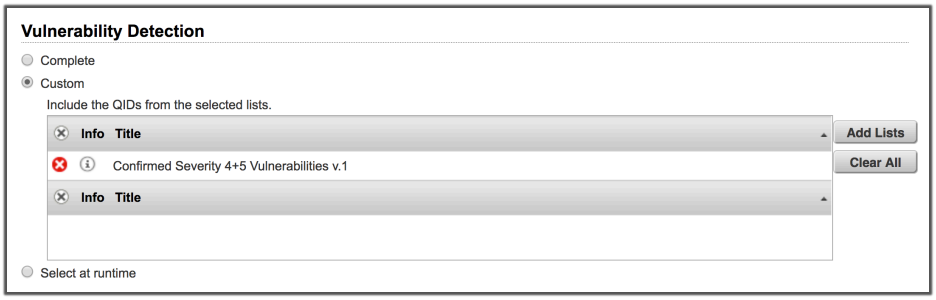
Custom Vulnerability Detection Scan

Goal: Choose the vulnerabilities to be tested in a vulnerability scan.

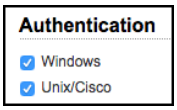
Normally, scans are configured to detect *all* vulnerabilities using the "Complete" option. That said, there are times when you may want to scan for a specific type of vulnerability.

The steps that follow use a Search List to perform a custom scan that will only target severity 4 and 5 vulnerabilities that can be confirmed:

1. **Under the "Scans" section, click the "Option Profiles" tab.**
2. **Click the New button and select "Option Profile…".**
3. **Enter the title "Confirmed Severity 4+5 Vulnerabilities".**
4. **Click the "Make this a globally available option profile" checkbox** (so other Qualys users can use this profile).
5. **In the left navigation pane, click the "Scan" tab.**
6. **Scroll down to the "Vulnerability Detection" section and select the "Custom" radio button.**



7. **Click the "Add Lists" button.**
8. **Select the check box next to the "Confirmed Severity 4+5 Vulnerabilities v.1" list, and then click the "OK" button.**



9. **Scroll-down to "Authentication" and select the check boxes for both Windows and Unix/Cisco.**
10. **Scroll to the bottom of the Option Profile and click "Save".**
11. **Use the "Launch Authenticated Scan" steps listed earlier to launch a scan using this new Option Profile.**

    When this Option Profile is used to perform a vulnerability scan, only the QIDs in the "Confirmed Severity 4+5 Vulnerabilities" Search List will be targeted and tested. The raw scan results will only reflect these vulnerabilities.

Low Bandwidth Scan

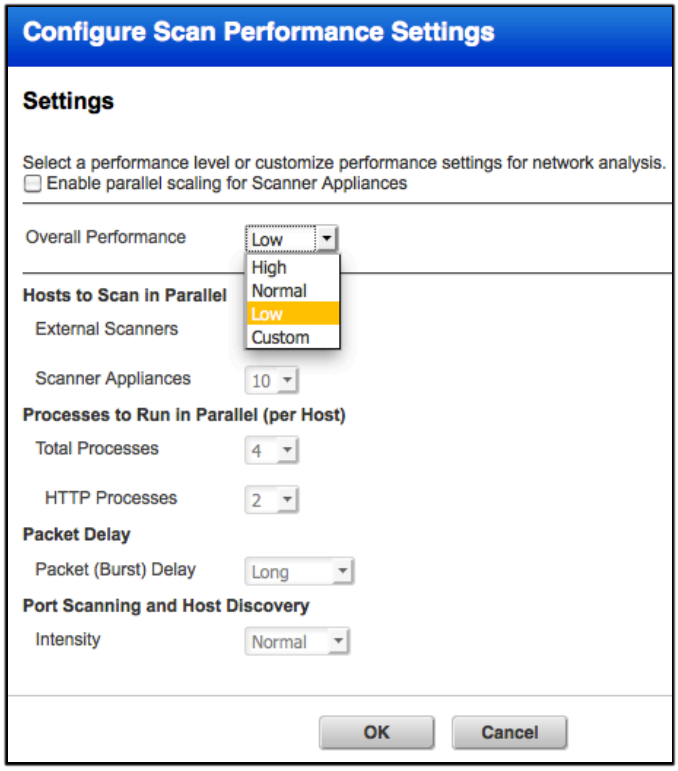
Goal: *Adjust your scan performance for different network and bandwidth conditions.*

Qualys has three scan performance options (pre-sets) and a "custom" option.

- The "Low" option reduces scan performance and should be used for bandwidth restricted networks or heavy traffic environments.
- "Normal" provides the best balance between scan performance and bandwidth usage.
- "High" provides the best scan performance and works best in network environments with ample bandwidth or light traffic.

A Qualys Scanner Appliance will automatically adjust its packet rate based on detected network load.

1. **Create a new Option Profile titled "Low Bandwidth Scan - Option Profile".**
2. **In the navigation pane on the left, choose the "Scan" tab.**
3. **Scroll down to the "Performance" section and click the "Configure…" button.**



4. **Choose "Low" from the "Overall Performance" drop menu.**

   Experiment with the other performance options and observe how each selected option (High, Normal, or Low) changes the "Hosts to Scan" and "Processes to Run" settings

5. **Leave "Overall Performance" set to "Low" and click "OK" to close the performance window.**
6. **Scroll down and "Save" the Option Profile.**

LAB 4: Assets (30 min.)

There are many ways to organize the host assets within your Qualys subscription:

- Geographical location
- Service or function
- Device type or operating system
- Asset owner
- IP address or netblock
- and more …

Although the methods listed above are commonly used, you may choose other methods or techniques that are unique to your company or organization.

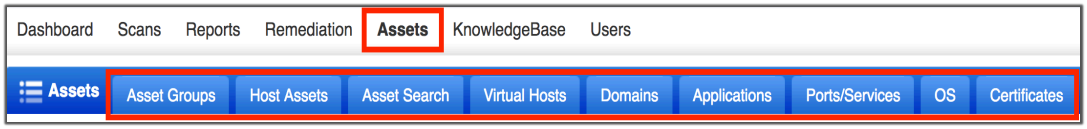
The proper use of Asset Groups and Asset Tags will allow you to effectively organize and manage host assets. Asset Groups and Asset Tags can be combined to accomplish numerous objectives, such as:

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

This lab will begin in the Vulnerability Management application with a discussion of Asset Groups, and then move to the AssetView application to demonstrate Asset Tags and Asset Search.

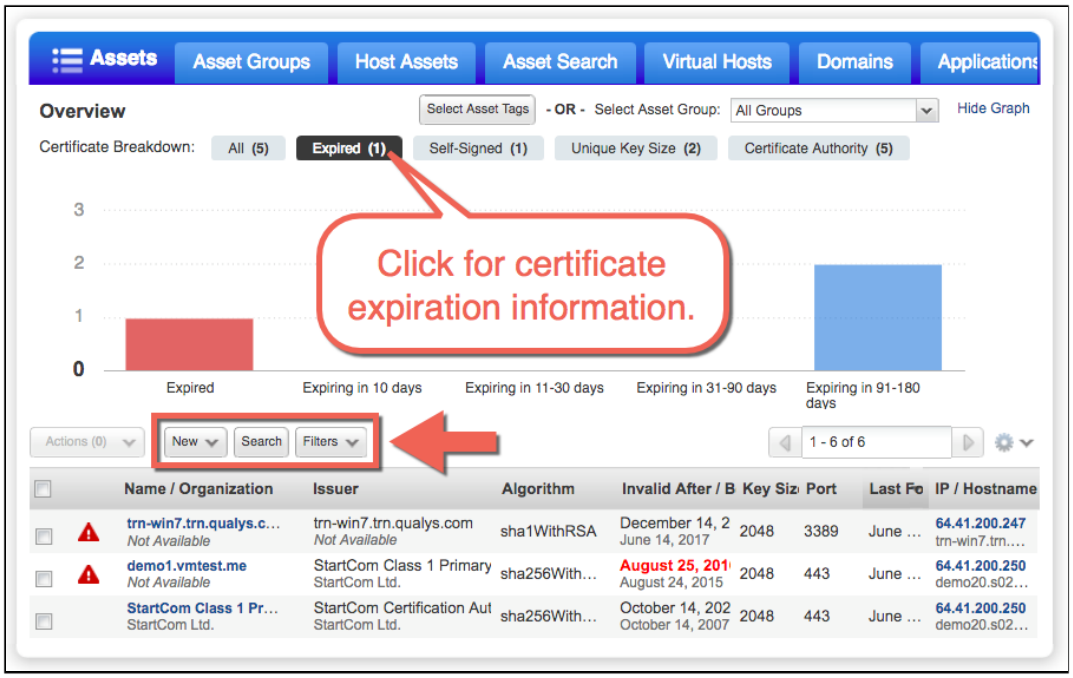
Vulnerability Management Assets

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.



1. **From the Vulnerability Management application, navigate to the "Assets" section.**
2. **Click the "Applications" tab and use the "Search" field to locate instances of database applications in your subscription (HINT: type 'sql' in the "Application" search field).**

   You can use the "Download CSV" button, to export any application list you generate.
3. **Click the "OS" tab to view a list of different operating systems within your subscription.**



4. **Click the "Certificates" tab and click the "Expired" button to 'breakdown' your certificates by expiration.**

5. **Click any of the graphic images in the bar chart to view specific host certificate data.**

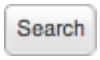
   Other certificate 'breakdown' options include: Self-Signed, Unique Key Size, and Certificate Authority.

6. **Click the**

button to download certificate data into different file formats, such as CSV or XML.

7. **Click the**

button to view hosts with Heartbleed and/or Poodle vulnerabilities.

8. **Click the** 

button to locate a specific certificate: Issued Date, Expiration Date, Key Size, Issuer, or Host.

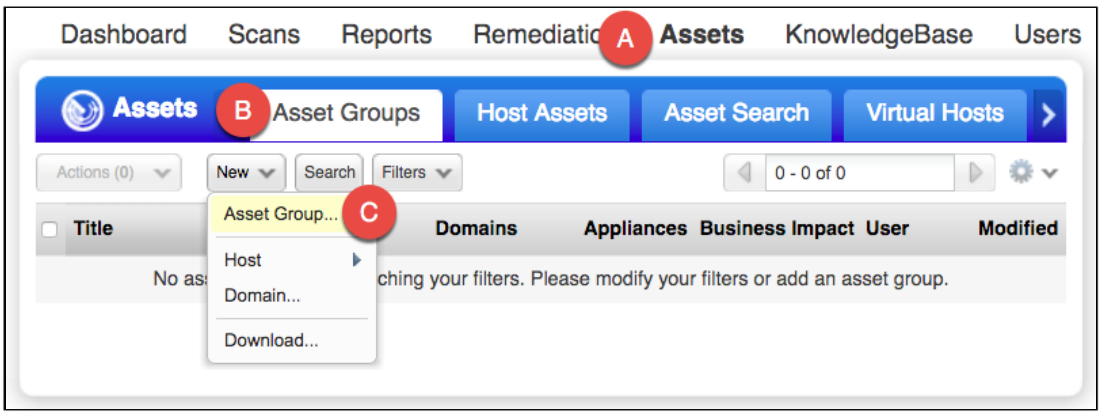
Create Asset Group

Asset Groups provide a mechanism for collecting or grouping host assets in your subscription. Simply create an Asset Group, give it an appropriate name, and add host IP addresses. Here are some important characteristics of an Asset Group:

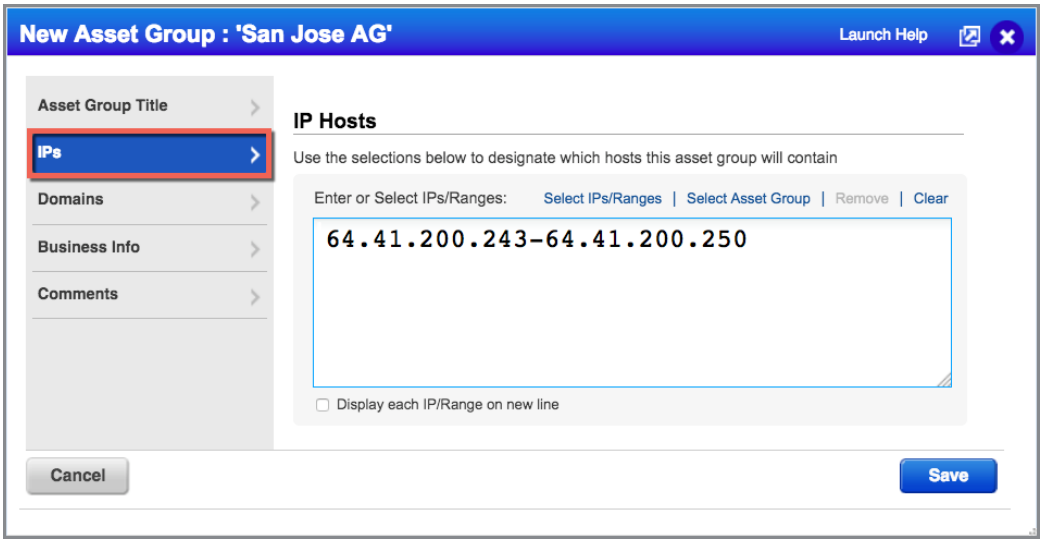
- Used to assign access privileges (hosts, scanners, and domains) to individual user accounts.
- Contains a "Business Impact" setting that is used to calculate Business Risk.
- Can be used as a target for mapping, scanning, reporting, and remediation.
- A single host can be a member of multiple Asset 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).

In the next few steps, you'll create an Asset Group that contains our training lab target IPs.



1. **From the Vulnerability Management application, navigate to A) the "Assets" section, and click B) the "Asset Groups" tab.**
2. **Click the "New" button, and select C) the "Asset Group…" option.**
3. **Type "AG: San Jose" in the "Title" field (representing the geographic location of our training lab host assets).**

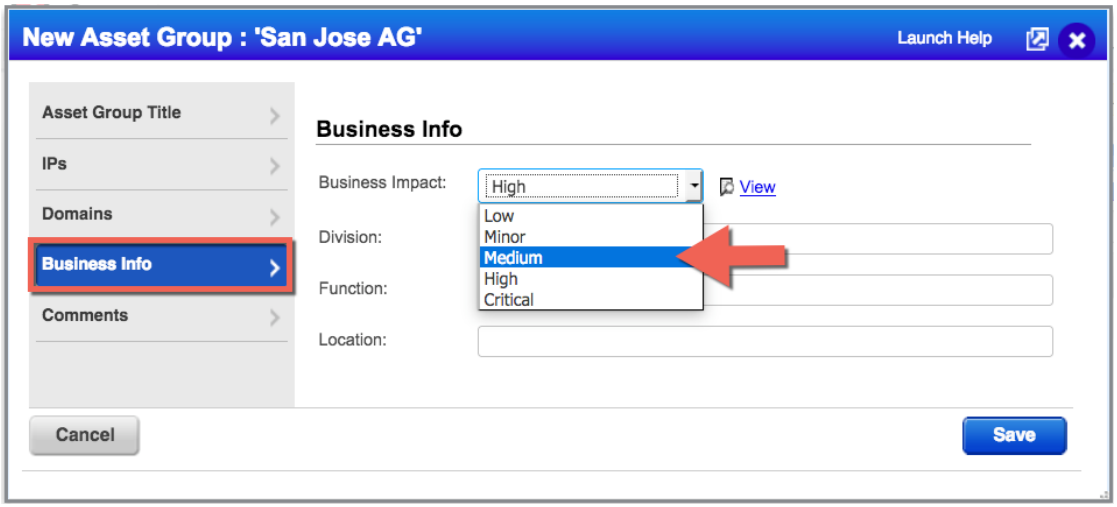


4. **Click "IPs" in the navigation pane (left) and enter the IP address range for the lab host assets: `64.41.200.243-64.41.200.250`.**

   Alternatively, you can click the "Select IPs/Ranges" option to select the IP addresses from a list.

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

   By default, Asset Groups are created with "Business Impact" set to High.



5. **Click "Business Info" in the navigation pane (left)and use the drop-down menu to change the "Business Impact" setting from High to Medium.**

6. **Click the "View" Link (just right of Business Impact).**

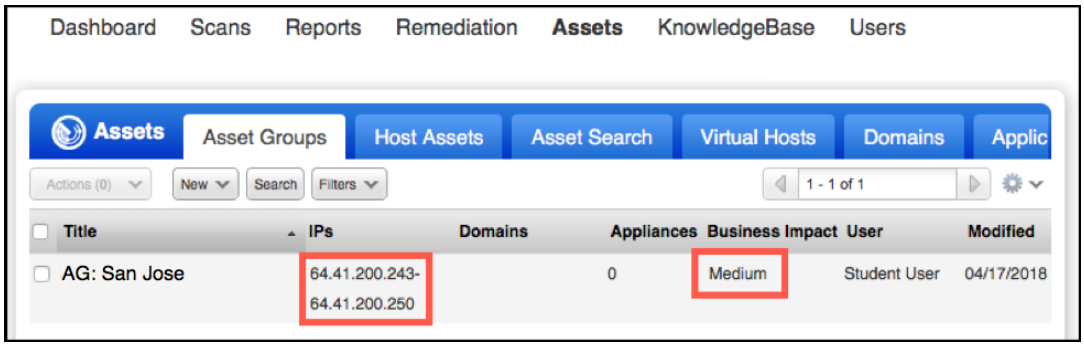
   Business risk is the product of an Asset Group's "Average Security Risk" and its "Business Impact" setting. Once an Asset Group's Average Security Risk is calculated, its associated Business Risk can then be determined.

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.

7. **Click the "Close" button, followed by the "Save" button.**

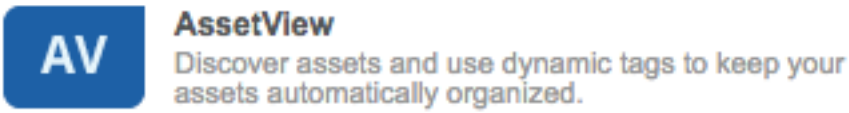


AG: San Jose, can now be used as a scanning or reporting target. It can also be used to provide access privileges to other Qualys user accounts that need to scan or build reports for the "San Jose" IPs.

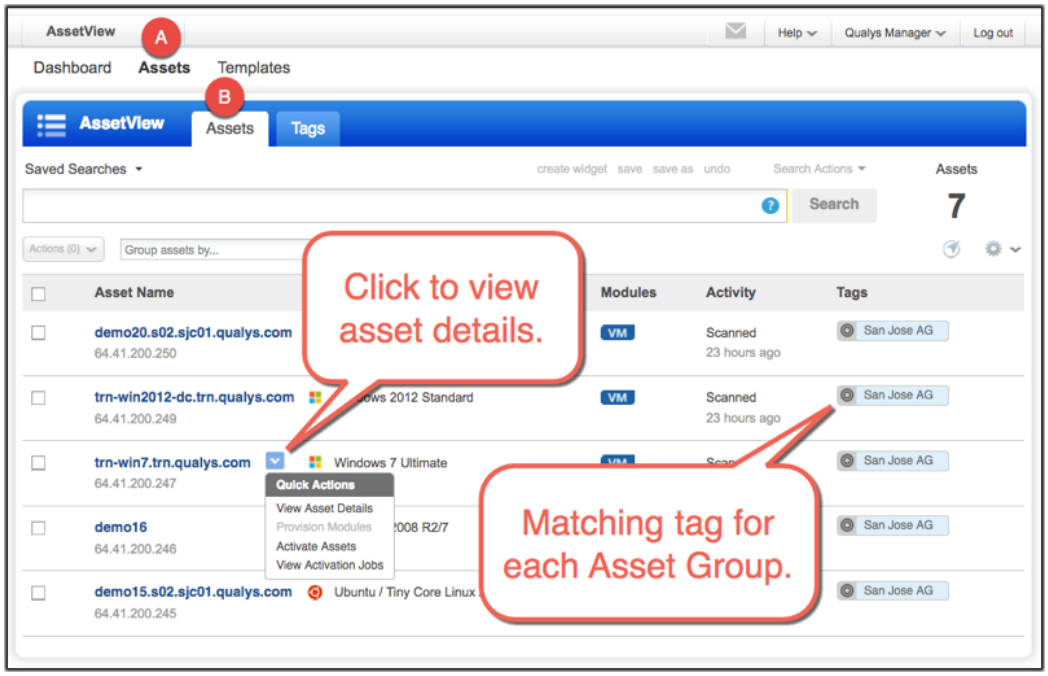
AssetView

AssetView is a core component of the Qualys Cloud Platform, providing a continuously updated inventory of asset details. It's a centralized spot for viewing all your asset details, creating asset tags, querying asset data, and managing customizable dynamic dashboards, all within the Qualys Cloud Platform.

As you complete the exercises that follow, please note that some lag time may occur between the point where an Asset Tag is initially created and the point where it is eventually applied to its respective asset(s). The same lag time may exist between the point where a host is added to the Vulnerability Management application, and the point where it appears in the AssetView application.



1. **Use the application drop-down menu to switch to the AssetView application.**



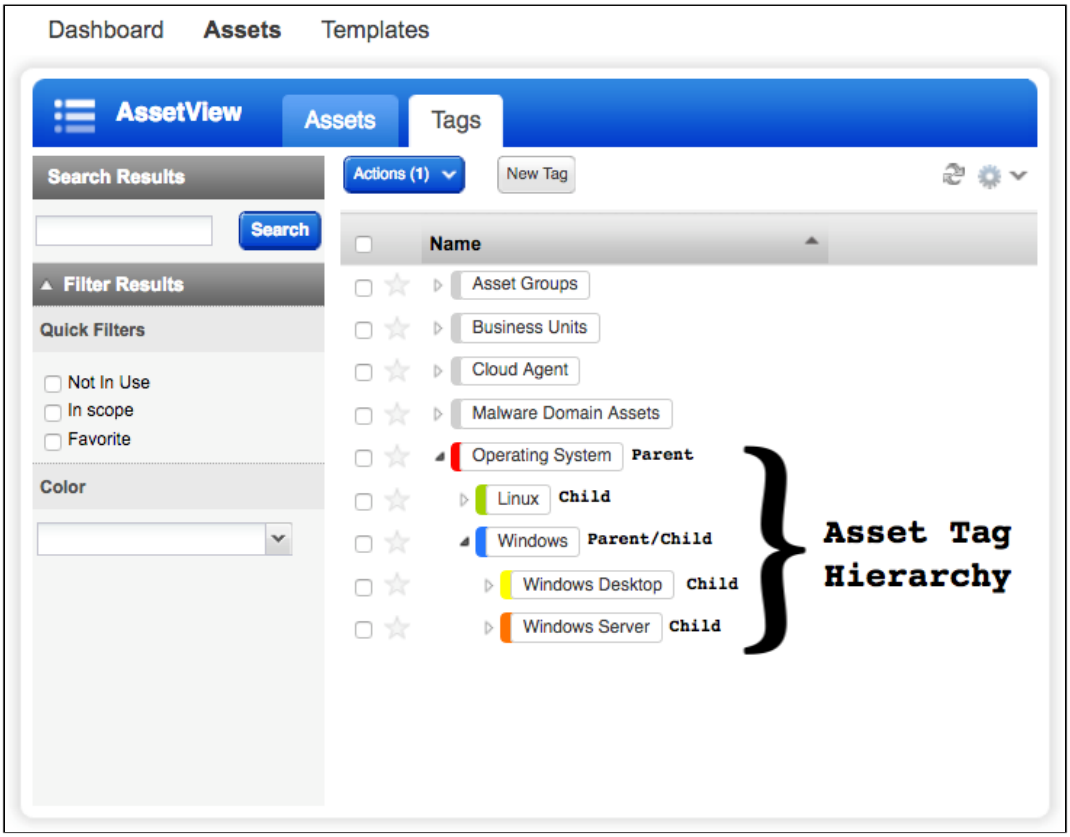
2. **Navigate to A) the "Assets" section followed by B) the "Assets" tab.**

   Here you will find useful host information, and you can use the "Quick Actions" menu to "View host details." A single host asset can have multiple tags, simultaneously.

Asset Tagging

Mobile devices, virtualization, cloud-based services, and remote employees are just a few of the reasons why it is important to have tools to monitor our rapidly and continuously changing IT and systems environments.

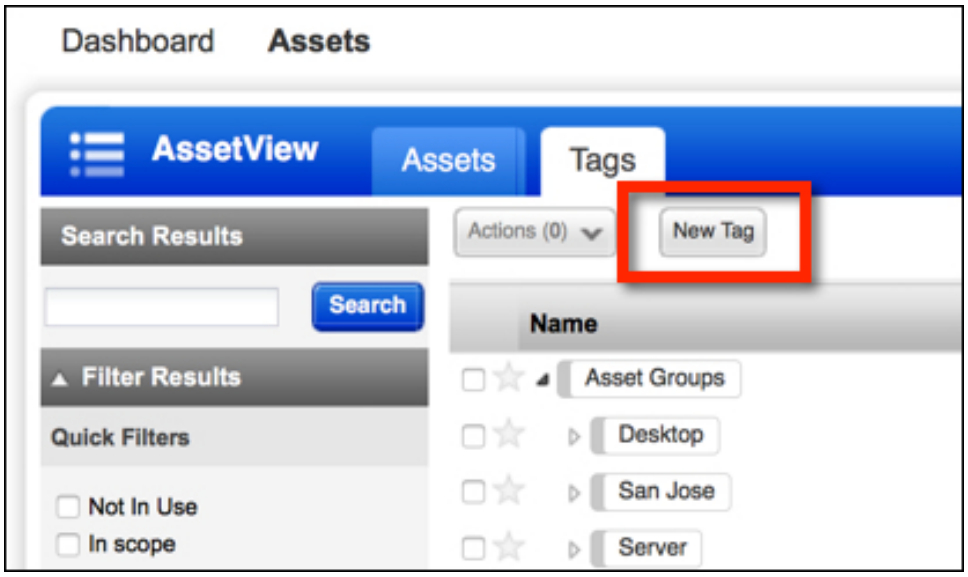
Asset Tags provide a flexible, scalable, and dynamic solution to help you target changes in host assets; making data readily available to Qualys applications and services. Asset tags are continuously updated, when new data and information is provided by a Qualys Scanner Appliance or Qualys Cloud Agent.



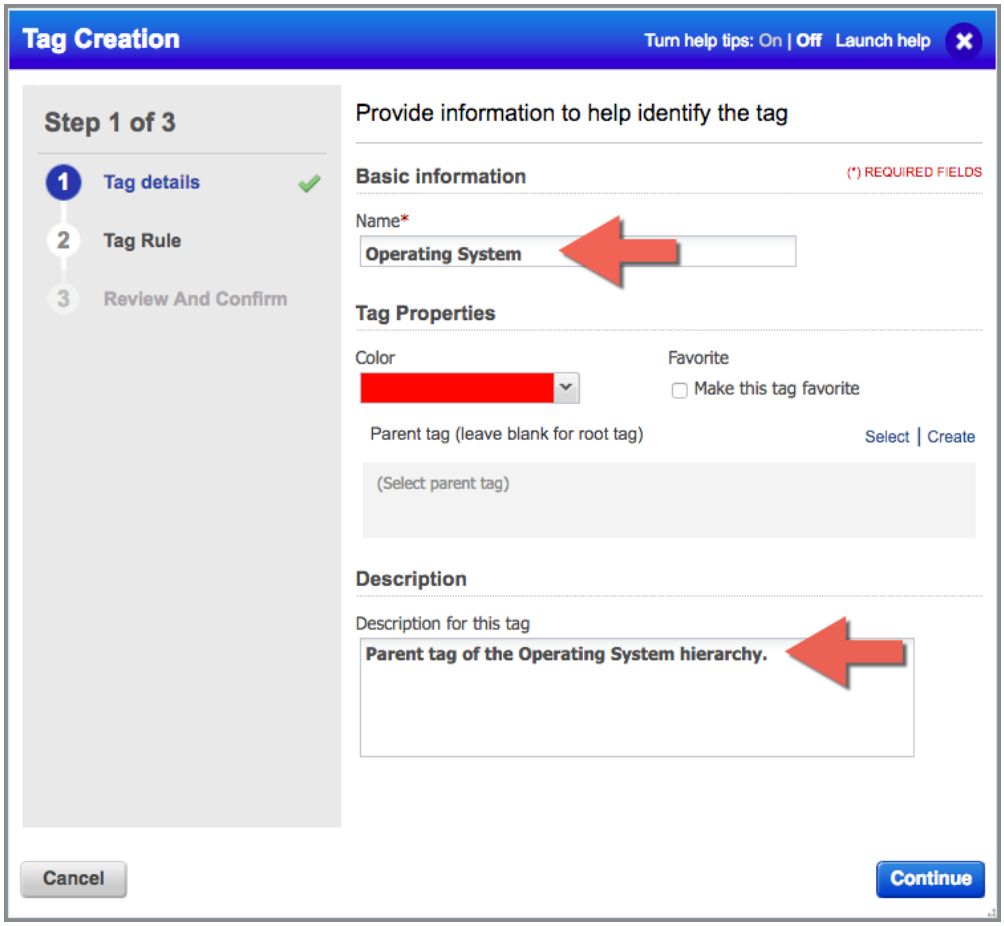
Asset Tags are organized into hierarchical structures or parent/child relationships. Some tags serve both a Parent and Child role. Tags located at higher levels of the hierarchy reflect a broader scope of host assets, while tags at lower levels of each hierarchy represent a more finite set of assets.

Create Operating System Hierarchy

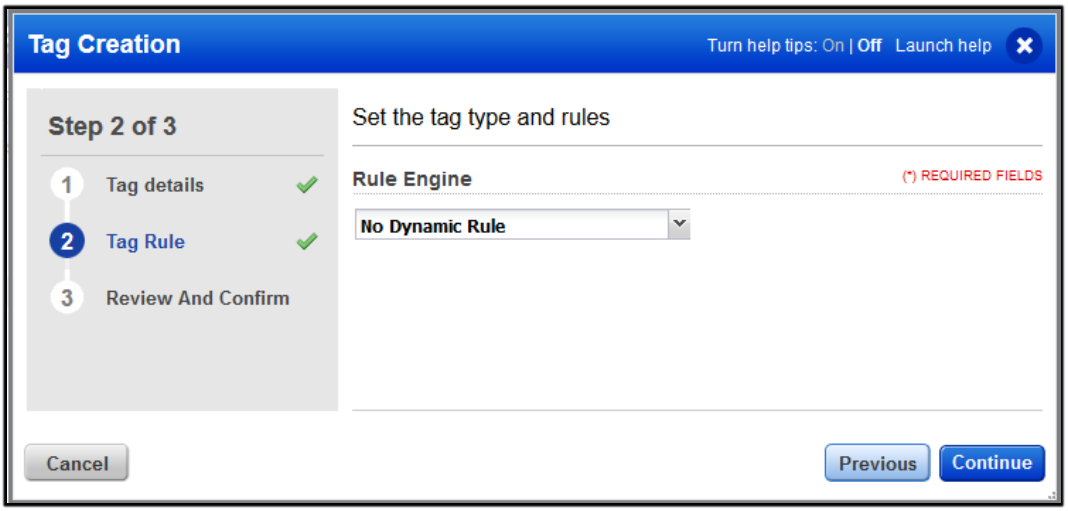
Many tag hierarchies begin with a static "parent" that serves as a "placeholder" for its dynamic "child" tags. This principle will be demonstrated with a static, parent called: Operating System.



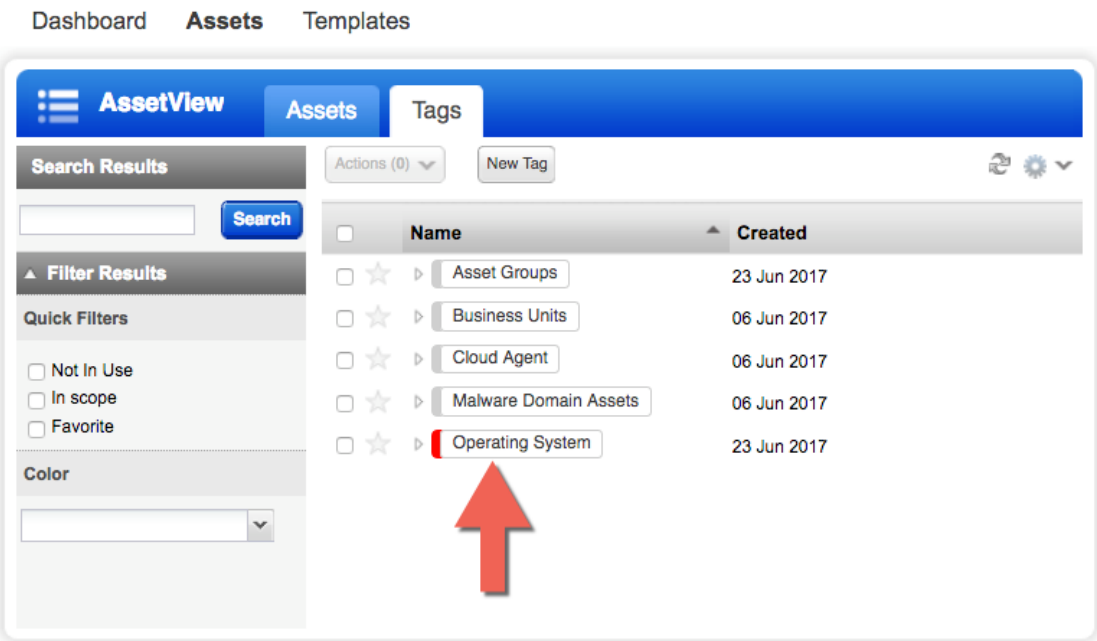
1. **Navigate to the "Tags" tab, and click the "New Tag" button.**



2. **Name this tag: "Operating System".**
3. **Select the color of your choice.**
4. **Type "Operating System Hierarchy Parent Tag" in the "Description" field, and click the "Continue" button.**



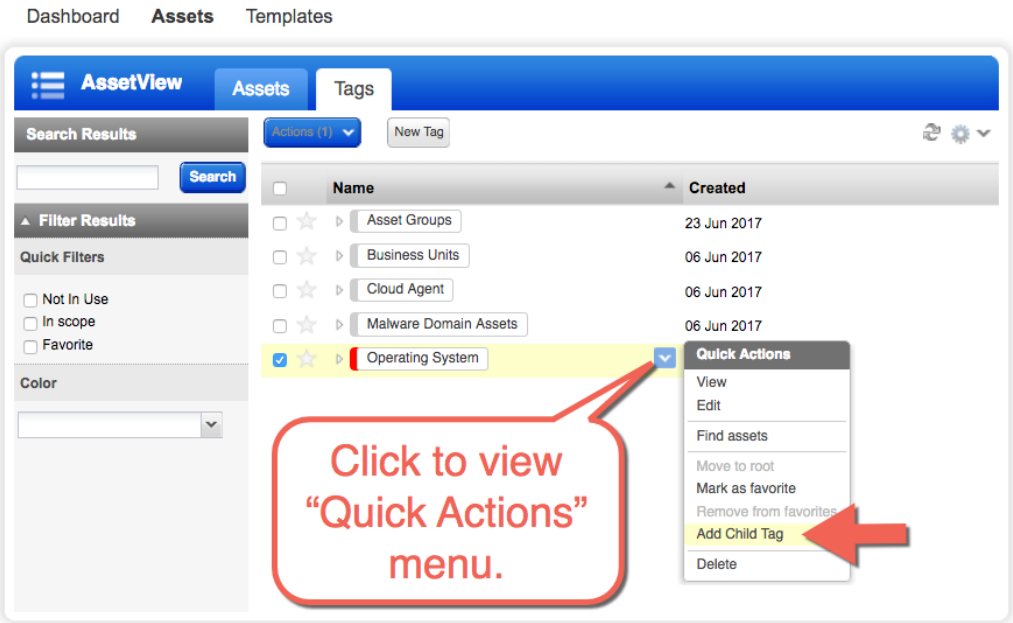
5. **Leave the "Rule Engine" field set to "No Dynamic Rule".** This is typical for top level tags that form the base of a new hierarchy.
6. **Click the "Continue" button, followed by the "Finish" button.**



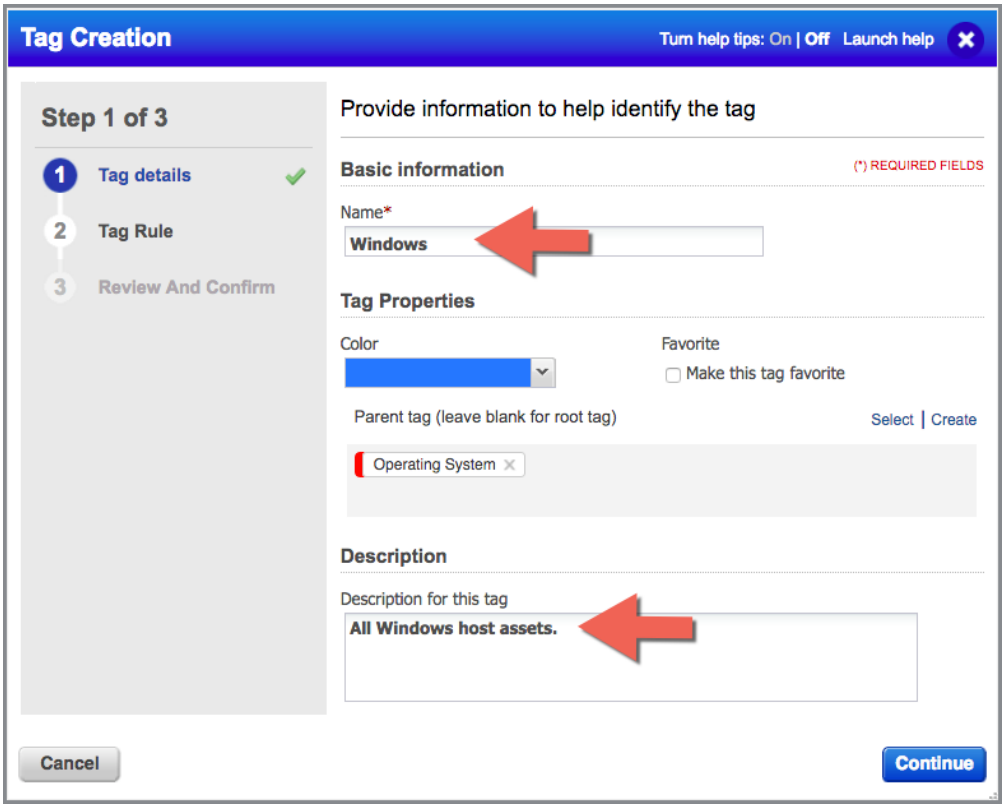
The "Operating System" tag should now be viewable as a "root" element in your Tag Tree. This tag marks the beginning of the "Operating System" hierarchy. Other tags added to this hierarchy will also target host OS. Dynamic tags will be created to identify and reflect changes to host OS.

Windows Tag

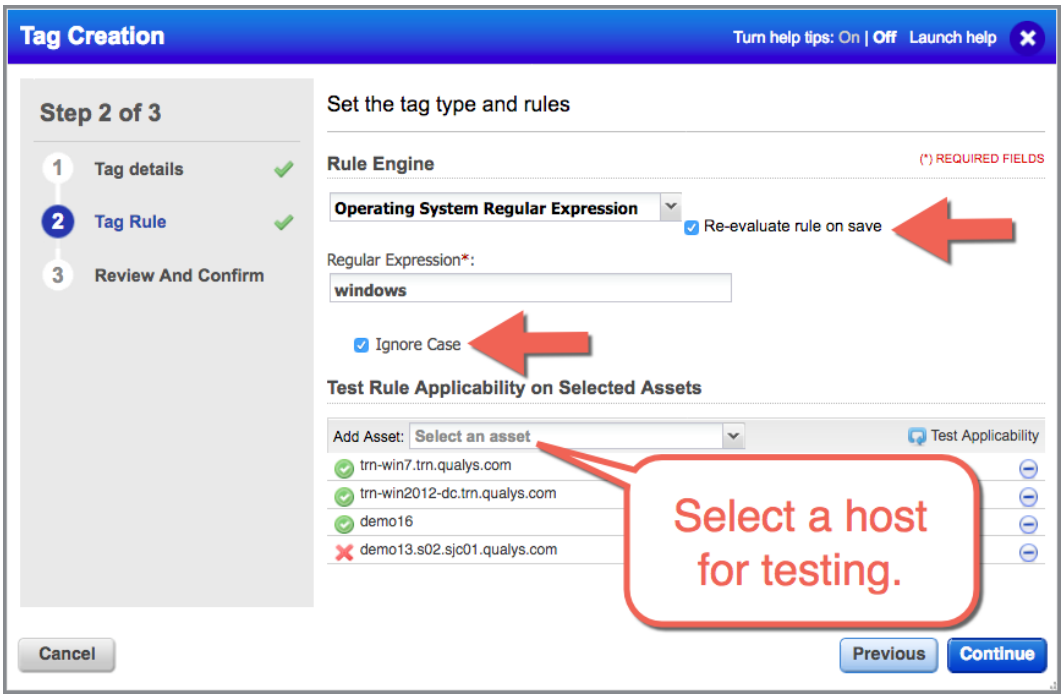
This exercise will nest a Windows tag (child) below the Operating System tag (parent) in the "Operating System" hierarchy.



1. **Select the "Add Child Tag" option, using the "Quick Actions" menu for the "Operating Systems" tag.**



2. **Type “Windows” in the “Name” field.**
3. **Select a color.**
4. **Type “All Windows host assets.” In the “Description” field, and click the “Continue” button.**
5. **Select the “Operating System Regular Expression” Rule Engine.**



6. **Select the "Re-evaluate rule on save" check box.**
7. **Type "windows" in the "Regular Expression" field and select the "Ignore Case" check box.**

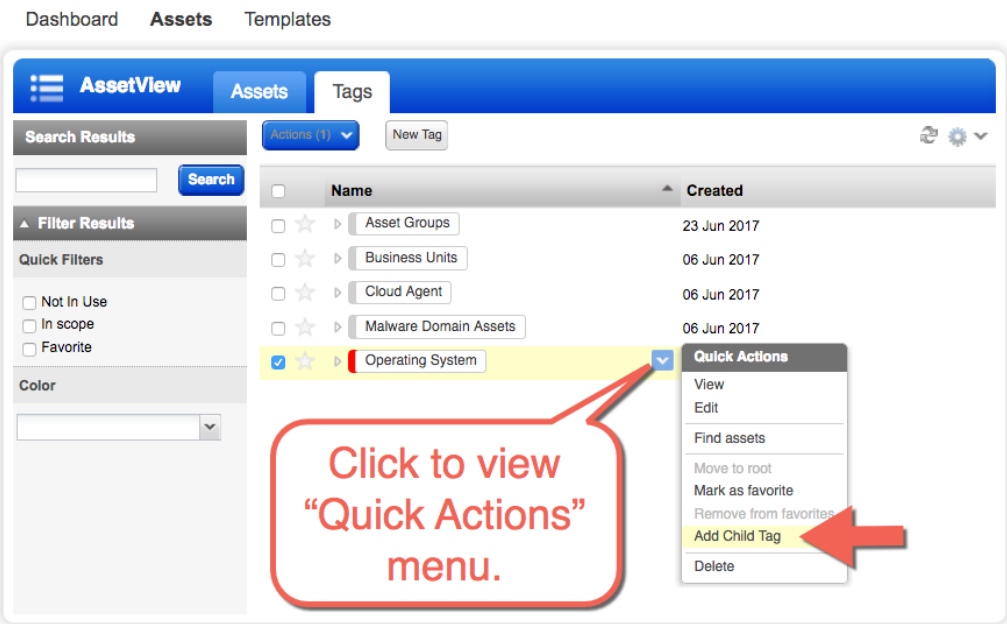
   This Asset Tagging example does not use regular expression metacharacters. A regex example will be provided later.

8. **Try testing this rule against host assets in your account.** Host operating systems that match the regular expression receive . Host operating systems that do not match the regular expression receive .
9. **Click the "Continue" button, followed by the "Finish" button.**

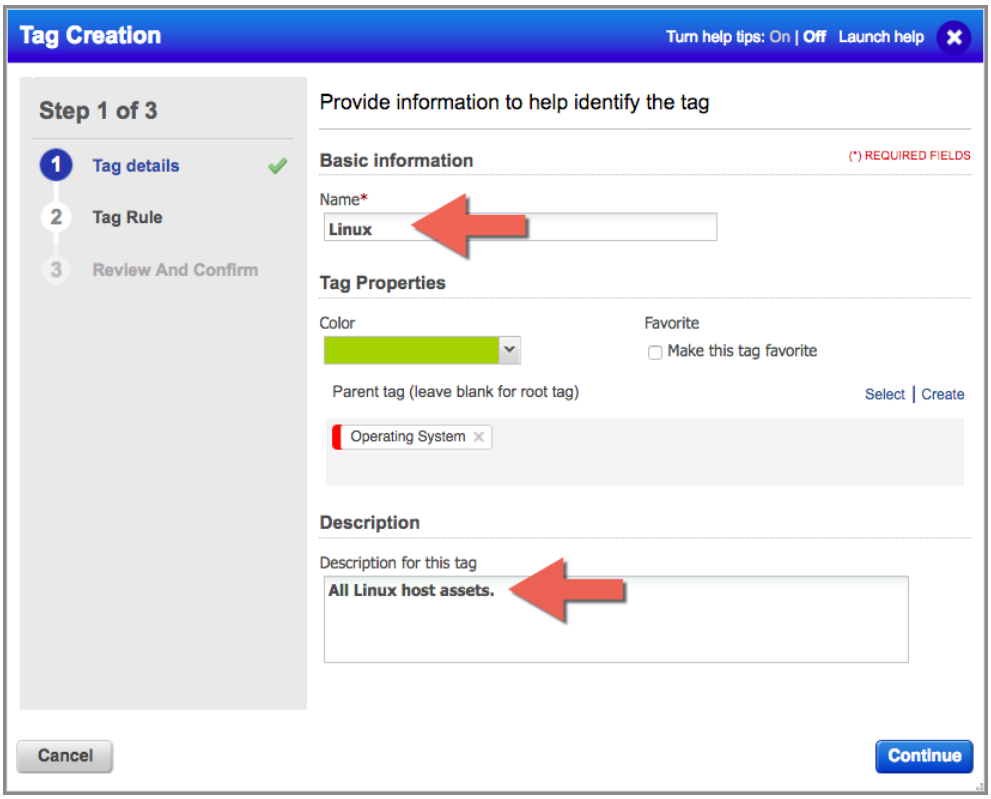
   Asset Tags that are submitted for re-evaluation may require a few minutes to complete the re-evaluation process.

Linux Tag

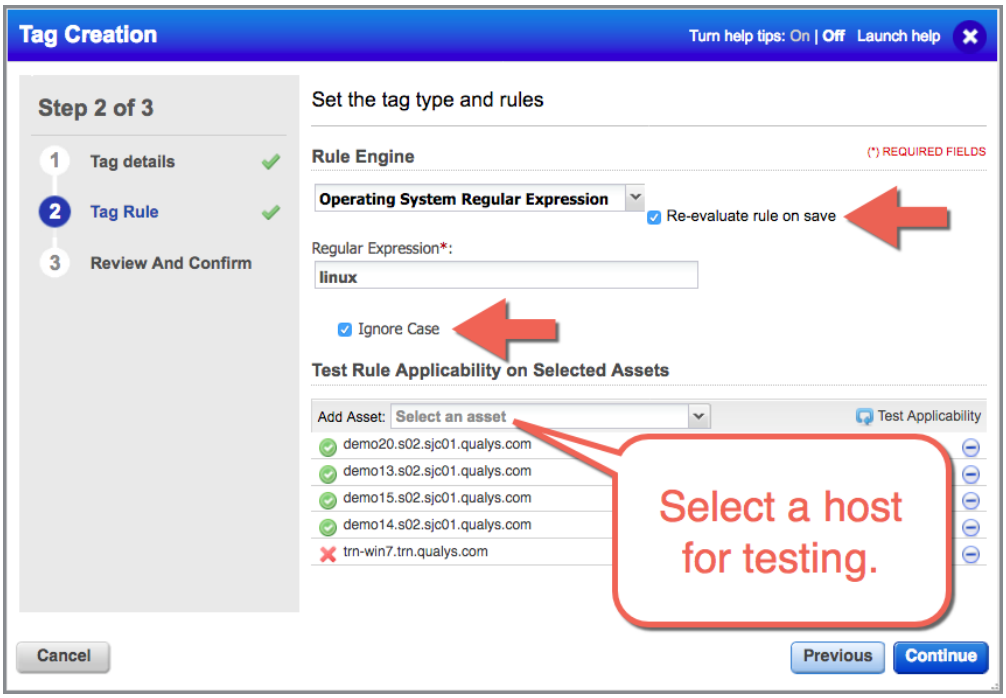
This exercise will nest a Linux tag (child) below the Operating System tag (parent) in the "Operating System" hierarchy.



1. **Select the "Add Child Tag" option from the "Quick Actions" menu of the "Operating Systems" tag, you just created.**



2. **Type “Linux” in the “Name” field.**
3. **Select a color.**
4. **Type “All Linux host assets.” In the “Description” field and click the “Continue” button.**
5. **Select the “Operating System Regular Expression” Rule Engine.**

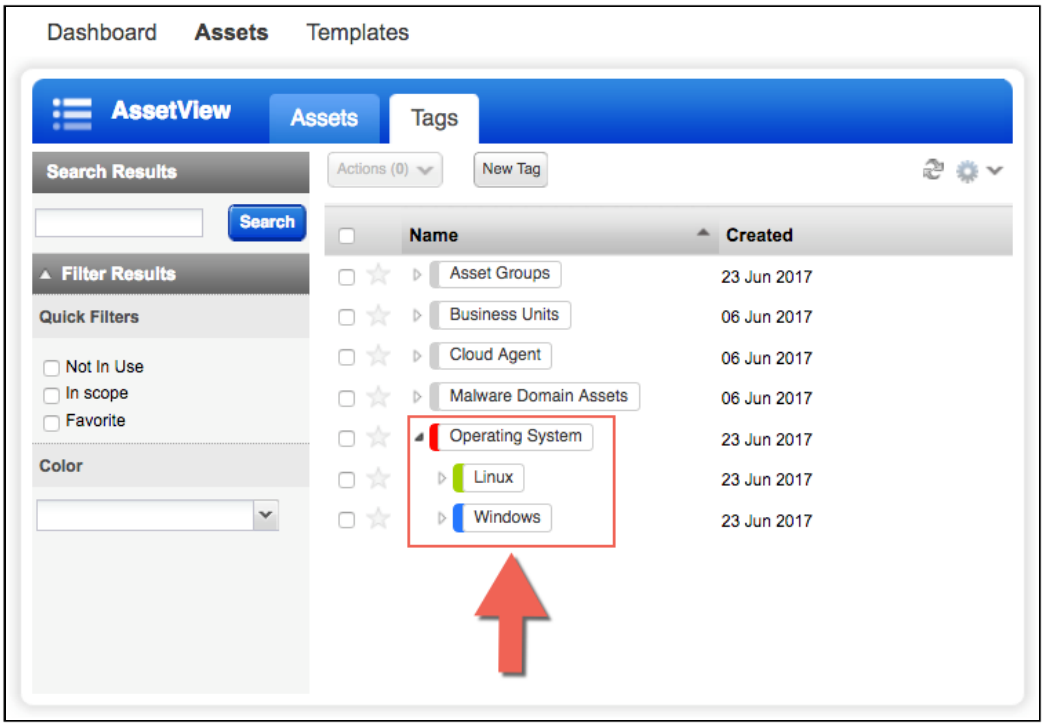


6. **Select the “Re-evaluate rule on save” check box.**
7. **In the “Regular Expression” field, type “linux” (omit quotes) and then select the “Ignore Case” check box.**

   This Asset Tagging example does not use regular expression metacharacters. A regex example will be provided later.

8. **Try testing this rule against host assets in your account.** Host operating systems that match the regular expression receive ✓. Host operating systems that do not match the regular expression receive ✗ .
9. **Click the “Continue” button, followed by the “Finish” button.**

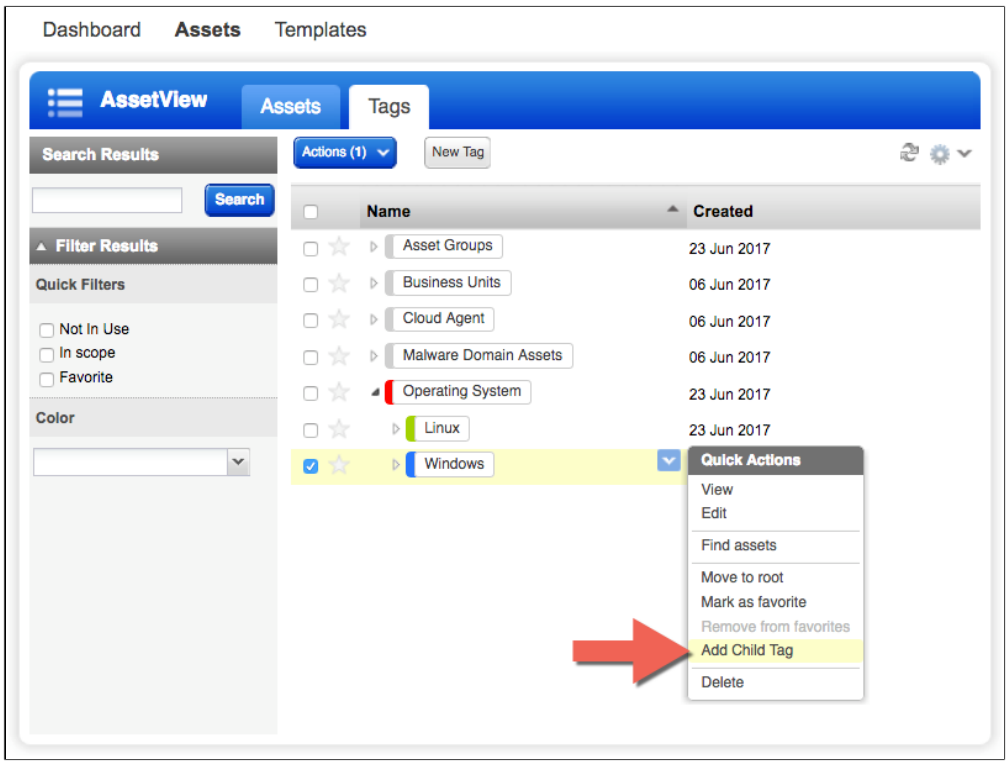
   Asset Tags that are submitted for re-evaluation may require a few minutes to complete the re-evaluation process.



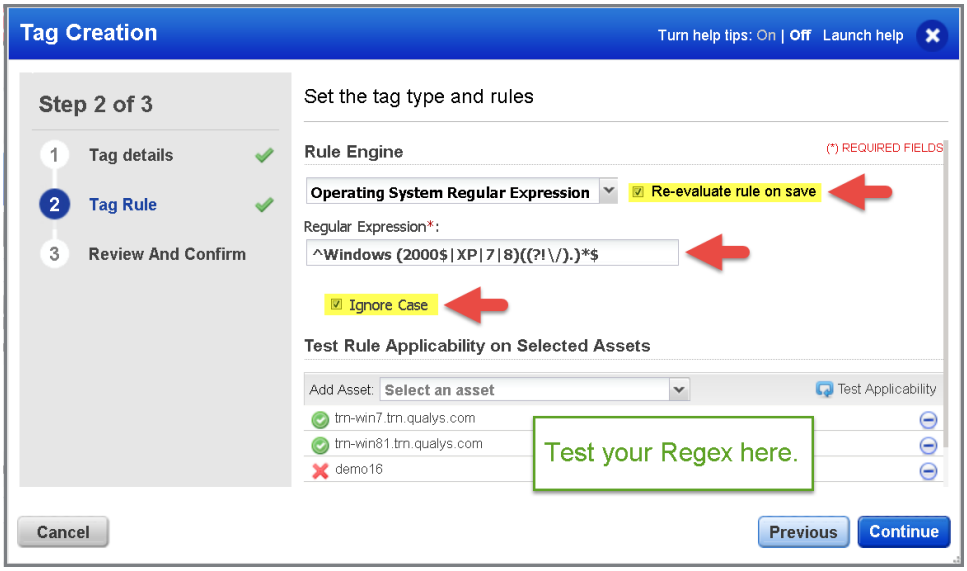
Your "Operating System" hierarchy should now have two child tags (Linux and Windows) nested below the "Operating System" parent tag.

Extending the Operating System Hierarchy

This next set of exercise steps will add child tags below the existing “Windows” tag, making the “Windows” tag both parent and child at the same time. This next generation of tags will create an additional nested layer in the “Operating System” hierarchy that differentiates between Windows desktops and Windows servers.



1. **Expand the “Operating System” hierarchy and select the “Add Child Tag” option from the “Quick Actions” menu of the “Windows” tag.**
2. **Type “Windows Desktop” in the “Name” field.**
3. **Select a color, provide a short description, and click the “Continue” button.**
4. **Select “Operating System Regular Expression” from the “Rule Engine” drop-down menu.**



This example was derived from the OS Regular Expression Library, found on the Qualys Community (https://community.qualys.com/docs/DOC-4029).

5. **Click the "Re-evaluate rule on save" checkbox.**

6. **Enter the following expression, into the "Regular Expression" field:**

```
^Windows (XP|7|8|10)((?!\/).)*$
```

7. **Select the "Ignore Case" checkbox.**

   NOTE: If using copy & paste, make sure you remove any blank space at the beginning or end of your regular expression. Blank space in your regex will typically create tag rule errors.

8. **Use the "Test Rule…" section to validate your expression.**

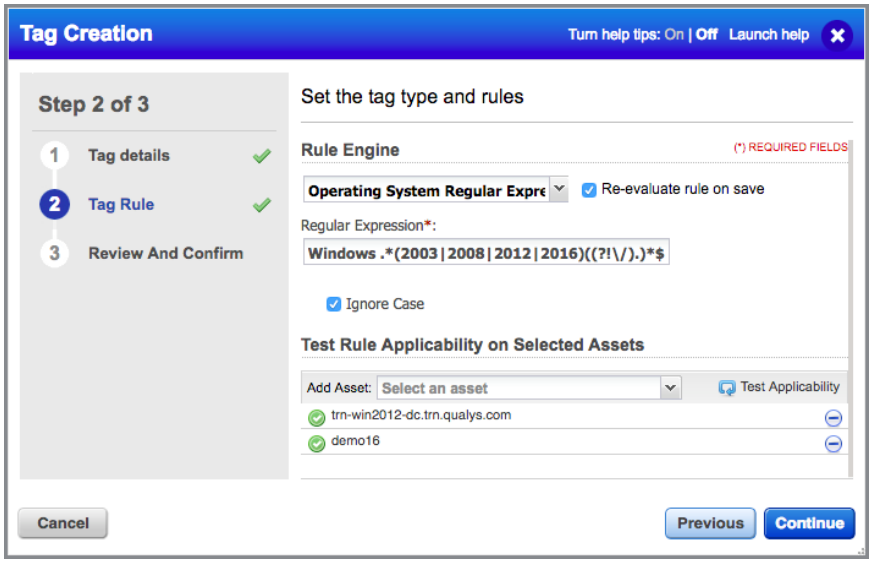
   A properly constructed regex will place tags only on hosts with a Windows desktop OS.

9. **Click "Continue" and "Finish".**

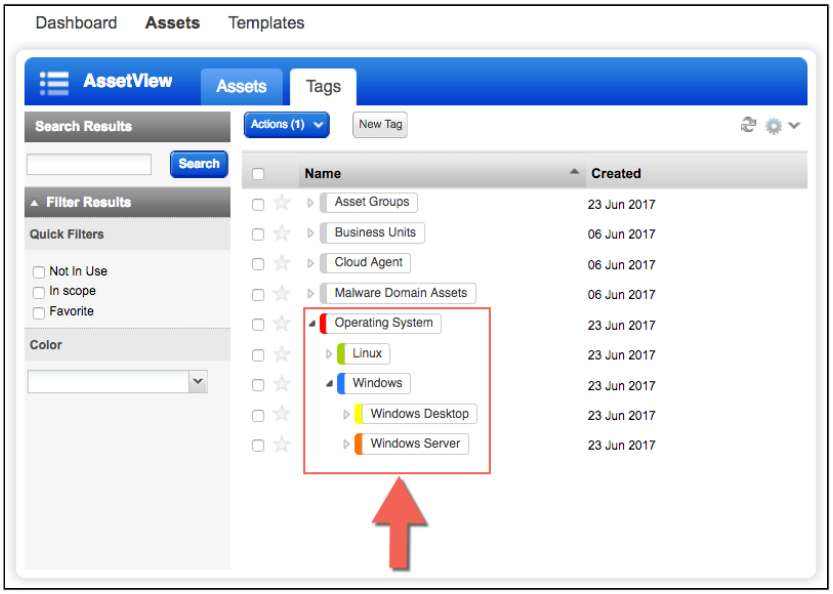
   Asset Tags that are submitted for re-evaluation may require a few minutes to complete the re-evaluation process.

10. **Using the previous example as a guide, add one more Asset Tag to the "Windows" hierarchy:**

Windows Server: `^Windows.*(2003|2008|2012|2016)((?!\/).)*$`



Make sure you click the "Re-evaluate rule on save" and "Ignore Case" checkboxes. Also ensure you've removed extra white-space from your regex.



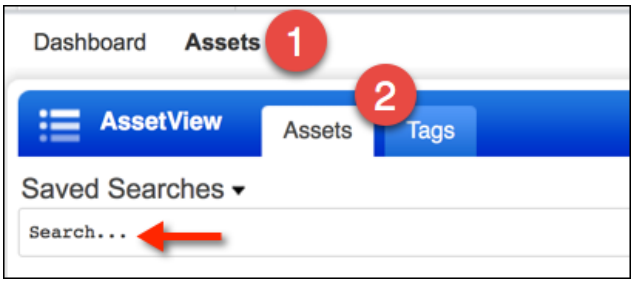
Your "Operating System" hierarchy should now have two more child tags nested below the "Windows" tag that distinguish between desktops and servers. Notice that the "Windows" tag now serves the roles of both parent and child.

Attempt to keep your Asset Tag hierarchies highly-cohesive, where each hierarcy contains Asset Tags of similar type or function.

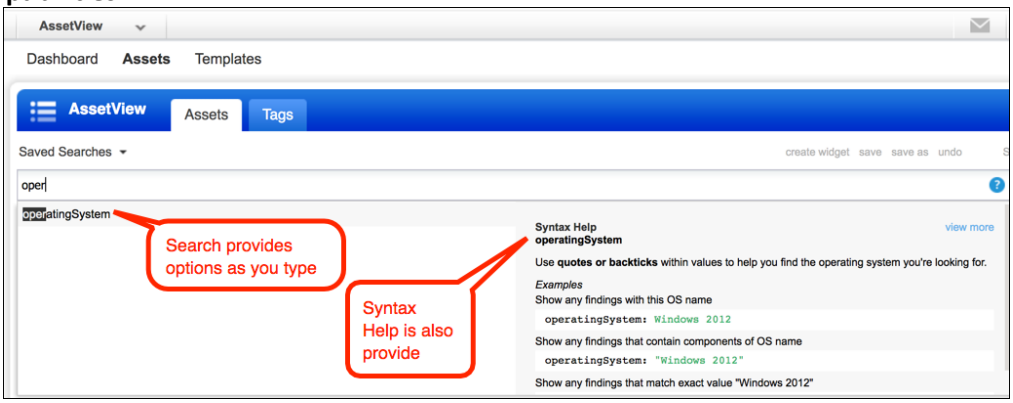
You'll find more Asset Tag examples and illustrations in Appendix B, "Asset Tag Examples."

AssetView Search

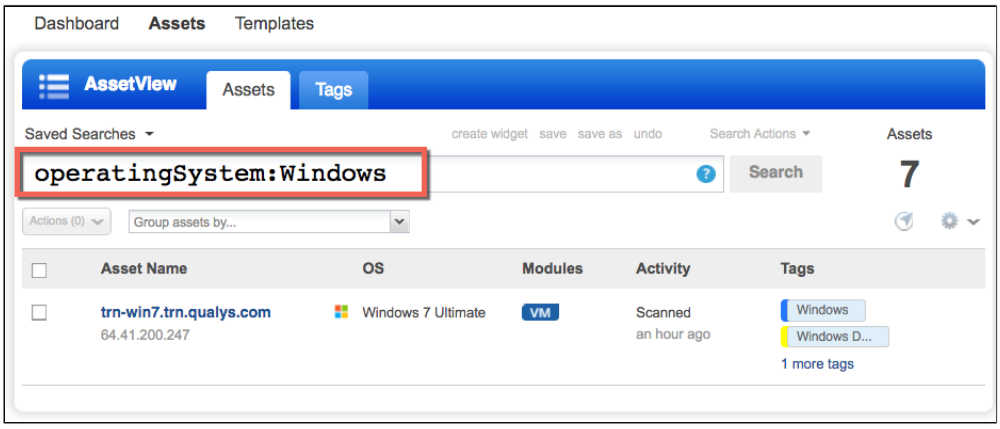
AssetView provides a very powerful method to query all your asset data in one location. You can search through the asset data obtained from a Qualys Scanner Appliance and Qualys Cloud Agent. With AssetView, you can export your query results, view them in a topological graph, or build widgets from your queries in your own Dashboard.



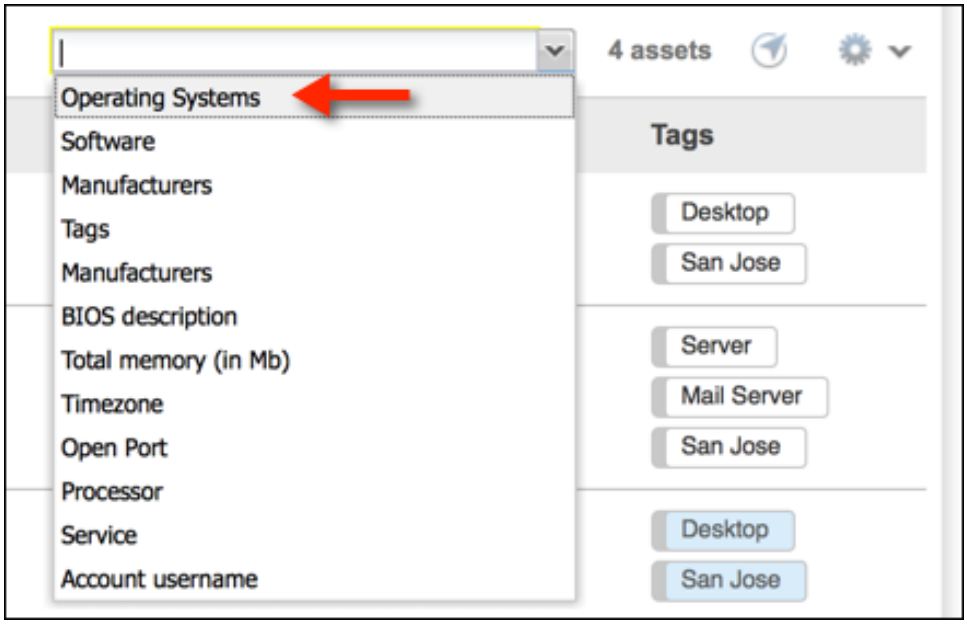
1. **Navigate to the "Assets" section and the "Assets" tab, to utilize AssetView's search capabilities.**



2. **Begin typing "operatingSystem" into the Search field.**
3. **Click on "operatingSystem" in the dropdown options you are provided.**

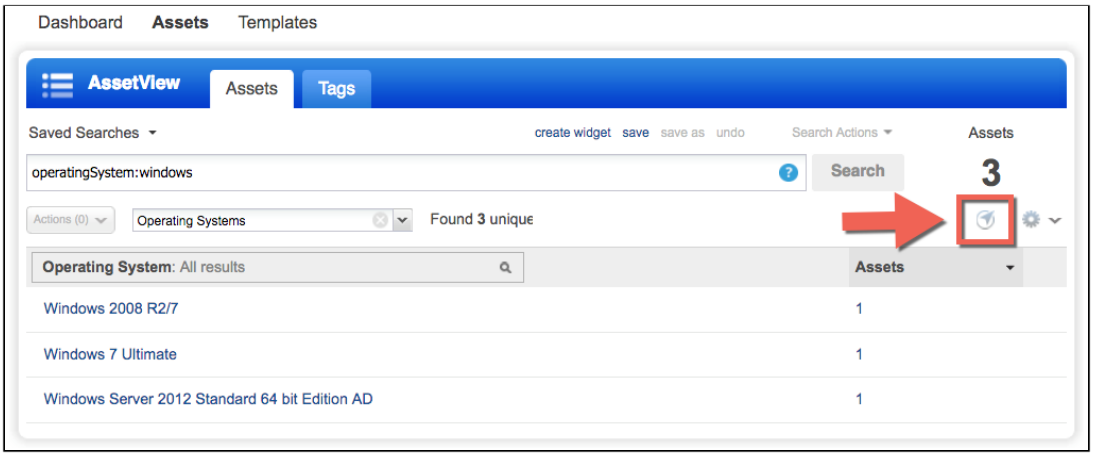


4. **Type "Windows" (without quotes), and press the "Enter" key on your keyboard.**



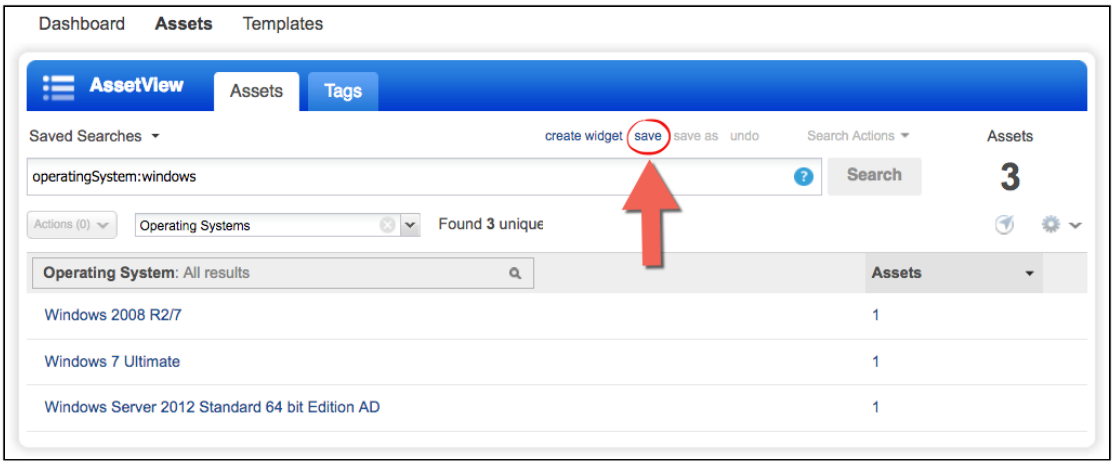
5. **Under the "Group asset by…" dropdown menu, select "Operating Systems".**

   This will give you a breakdown of all your different Windows Operating Systems based on information collected from your Vulnerability Management Scans and Cloud Agents.

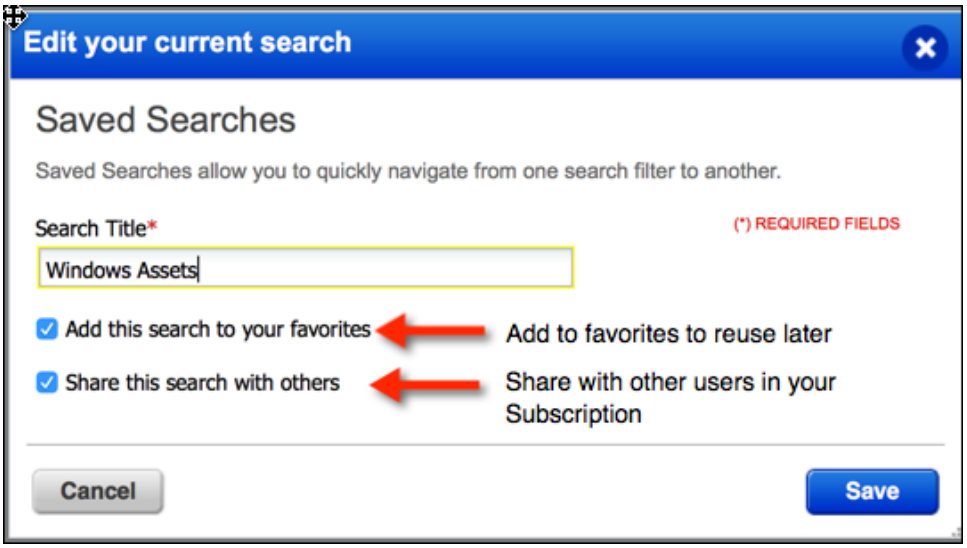


6. **Click the "View Network Graph" icon to view a topology of your assets from these search results. You can click on assets from within the graphical representation and view their details.**

7. **Once done viewing the graphic, close the topology view.**

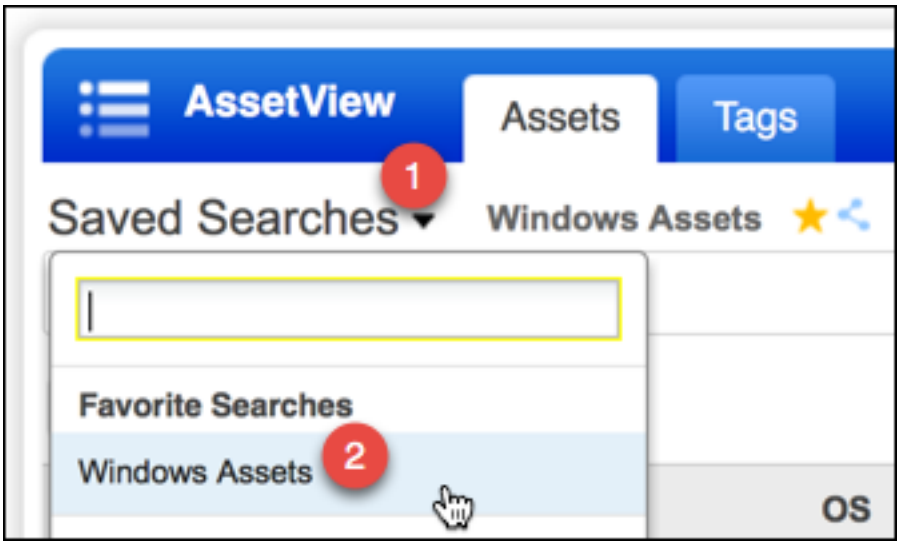


8. **Click the "save" link above the Search box.**



9. **Give it a Search Title of "Windows Assets" and check the boxes next to "Add this search to your favorites" and "Share this search with others".**
10. **Click the "Save" button.**

This gives you the ability to come back to your searches you use often, without having to retype the whole search. By sharing with others, other users will also be able to use your saved query.



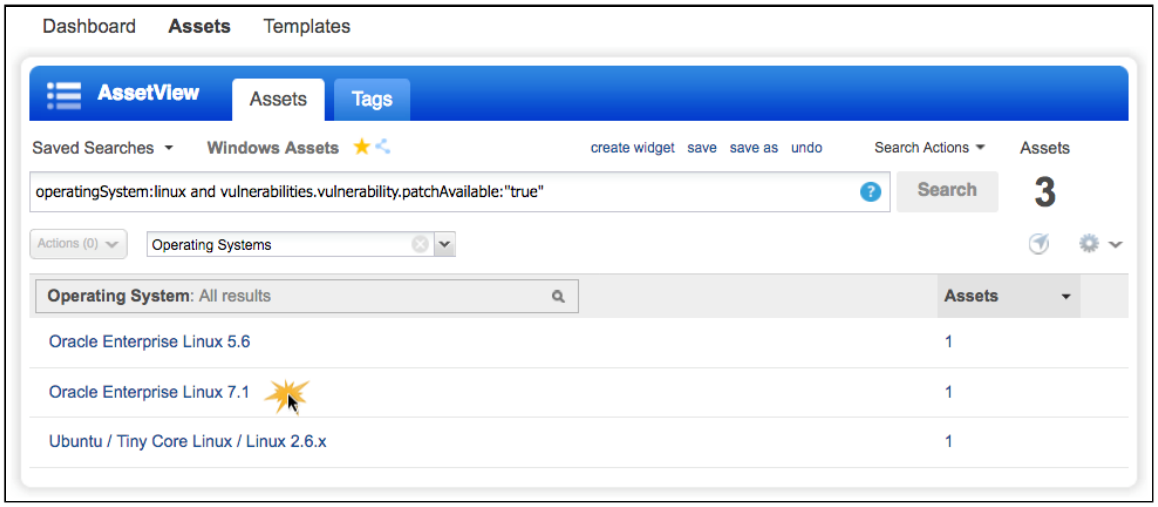
11. **Click on "Saved Searches" and view your recently saved search.**

12. **Replace your existing search with the following query to find all your Linux systems that also have vulnerabilities where there is a patch available:**

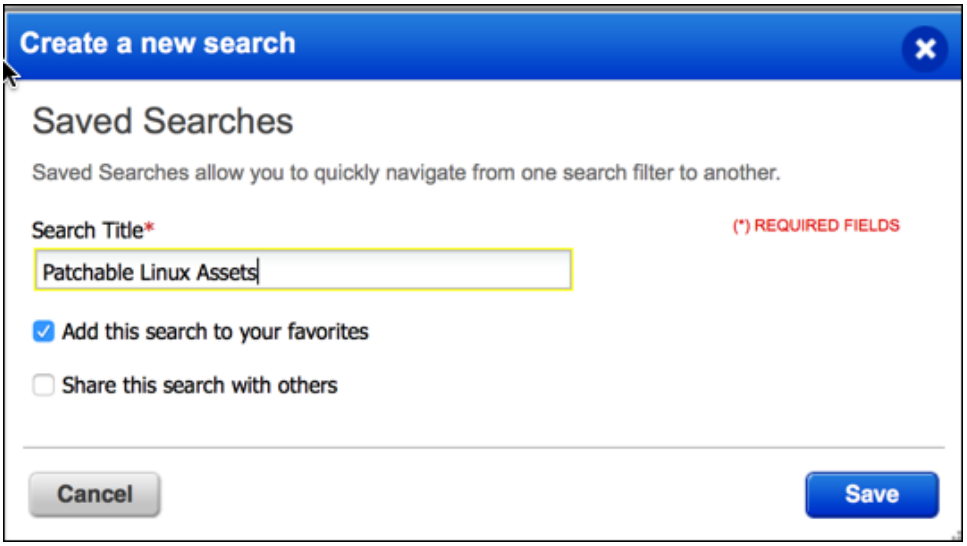
****

```
operatingSystem:linux and vulnerabilities.vulnerability.patchAvailable:"true"
```

****



13. **Click any of the operating systems listed, to view specific assets.**



14. **Use the "Save As…" link to save this as "Patchable Linux Assets" as well as "Add this search to your favorites".**

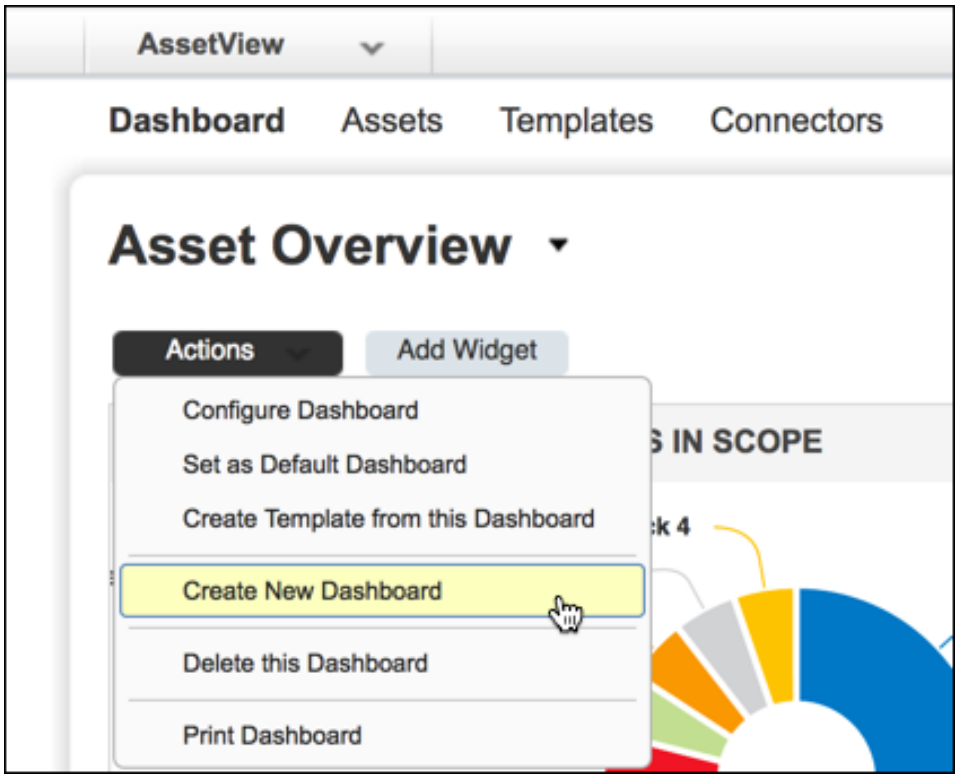
15. **Click the "Save" button.**

    The capabilities of the search feature in AssetView are nearly endless. Use the "Help" menu to find all the different Asset Search fields you can use to filter your data.

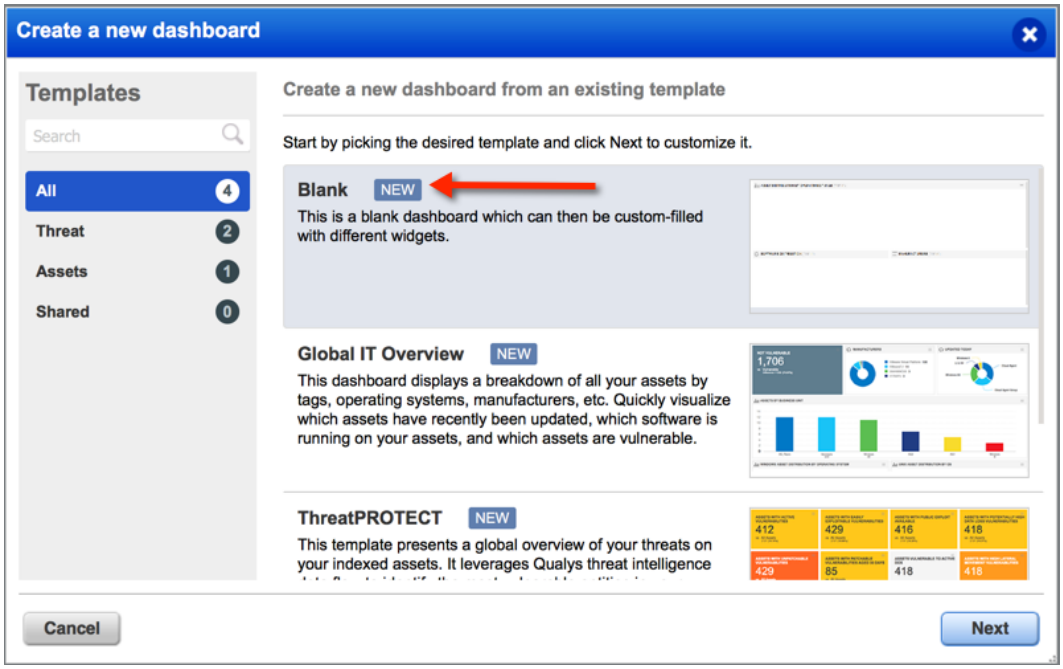
AssetView Dashboard

AssetView enables you to build unlimited, dynamic dashboards to view your IT and security data in many ways. Dashboards in AssetView will save you time because they will contain customizable, up-to-date views of your data without having to manage API scripts and spreadsheets. You can build as many dashboards as you need.

1. **From within AssetView, click on the "Dashboard" section.**

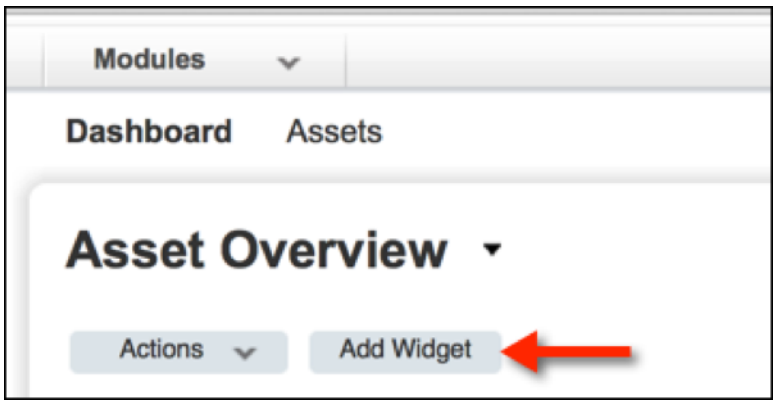


2. **Click the "Actions" button and select the "Create New Dashboard" option.**

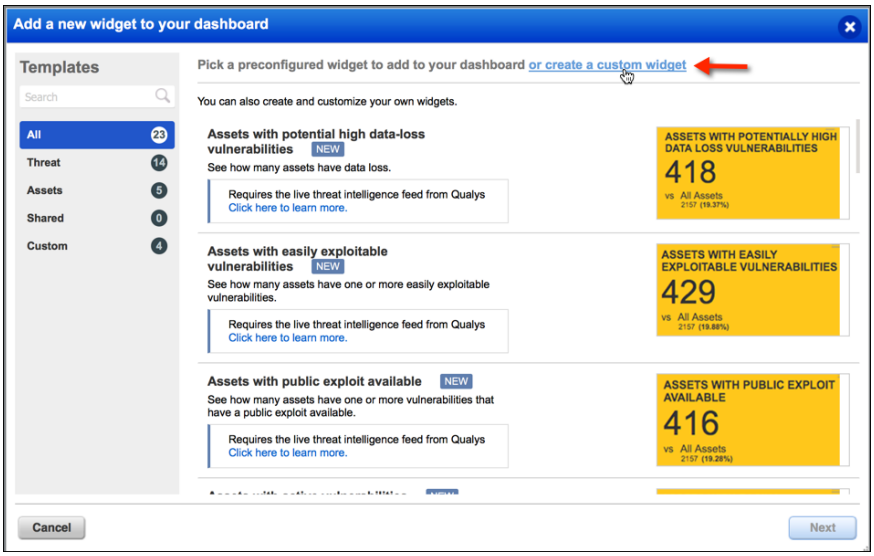


3. **Click the "Blank" option, and click "Next".**
4. **Give it the name of "First Dashboard".**
5. **Click the checkbox to "Make this dashboard my default".**
6. **Click "Create".**

   This creates a blank canvas for you to build your own widgets. Your widgets will use elastic search and enable you to customize your own Dashboard(s).



7. **Click the "Add Widget" button.**



8. **Click the link to "create a custom widget".**
9. **Give it a title "Sev 4 and 5 Vulns by OS".**
10. **Enter the following query to find hosts with vulnerabilities that have severity 4 or 5:**

****

```
vulnerabilities.vulnerability.risk:40 or 50
```

****

11. **Click the "Pie" option, and the "Show Labels" checkbox.**
12. **Under the "Categories" click on "operatingSystem".**
13. **Under "Limit to" select "Top 5".**
14. **Click the "Add to Dashboard" button.**
15. **View your new widget in your Dashboard.**

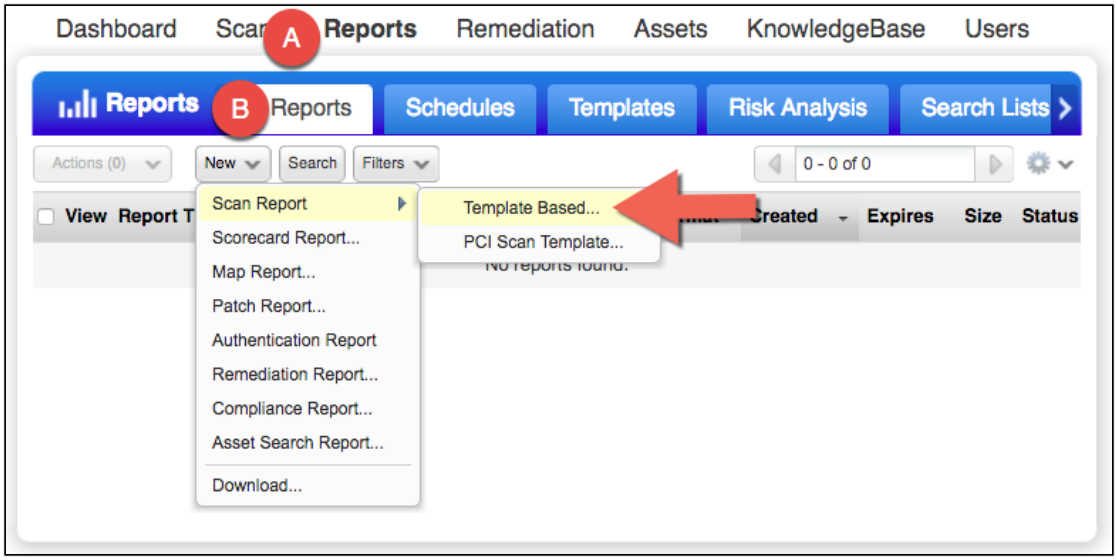
LAB 5: Reporting (25 min.)

Qualys stores your generated reports for a week. This is handy when you generate a large report that you want to share with your colleagues. Qualys only needs to process the data when you create the report; your colleagues can simply click to view the generated report.

High Severity Report

As we've seen, using raw scan data can be overwhelming. It's better to generate a report to consolidate, organize, filter and generally make scan data usable for reviewing. Let's begin by creating a High Severity Report. The High Severity report is useful for showing only the most severe vulnerabilities, levels 4 and 5 (confirmed).

1. **Use the application drop-down menu to open the Vulnerability Management application.**



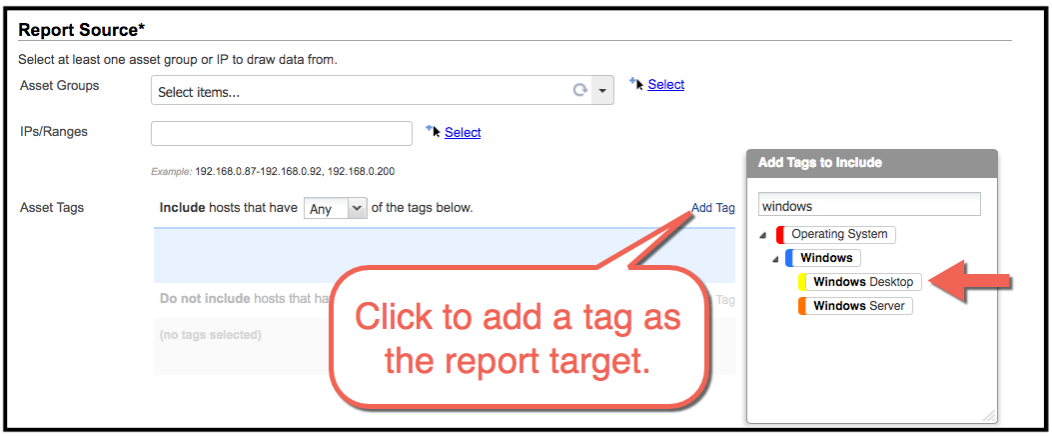
2. **From A) the Reports section, click B) the Reports tab.**

3. **Click the "New" button followed by "Scan Report >" and then select the "Template Based…" option.**

4. **Type "Confirmed High Risk Vulnerabilities" in the "Title" field.**

5. **Select "High Severity Report" in the "Report Template" field.**

6. **Select "HTML pages" in the "Report Format" field.**



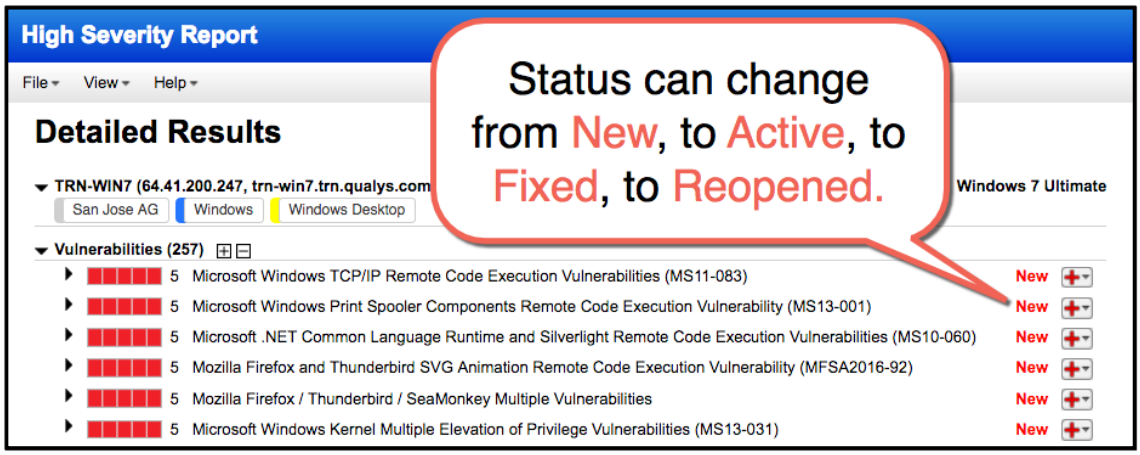
7. **Scroll down to the "Report Source" section, click the "Add Tag" link and enter "windows" in the "Search" field.**

8. **Select the "Windows Desktop" tag as the report source/target.**

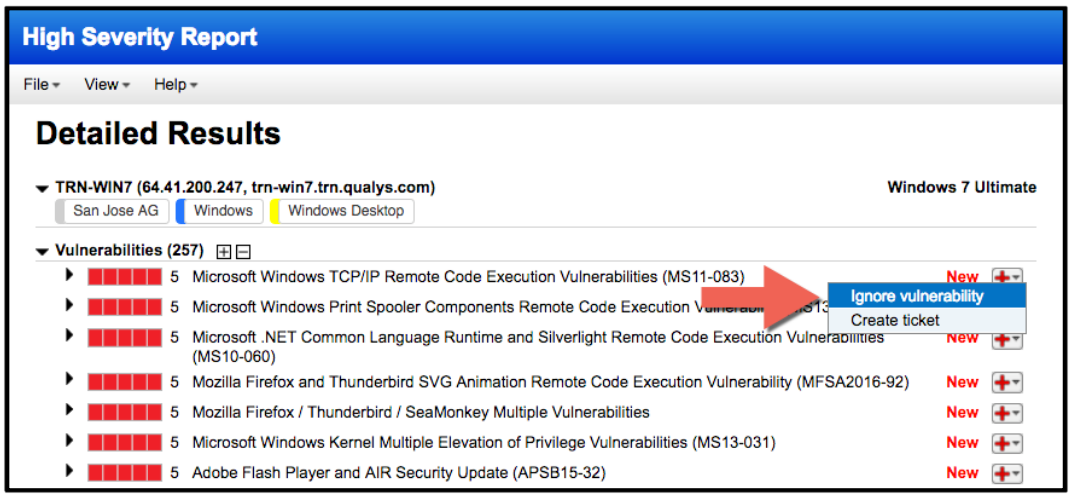
9. **Click the "Run" button to view the report and scroll down to the "Detailed Results" section.**

Integrated Workflow Actions

When the "HTML pages" report format is used, additional functionality is integrated into the High Severity and Technical Reports using the icon. Using "workflow actions" you can ignore vulnerabilities, create remediation tickets, or view remediation tickets that already exists.



Notice the vulnerability status next to the action icon. The first time a vulnerability is found the word "New" will appear in the report. When a vulnerability is discovered more than once, its status will change to "Active." If the vulnerability has been fixed, the word "Fixed" appears.



1. **Using the first host in the report, mouse-over the menu of the first vulnerability, and choose the option to "Ignore vulnerability".**

2. **Enter an appropriate reason, such as "Host has been retired" and click the "OK" button.**

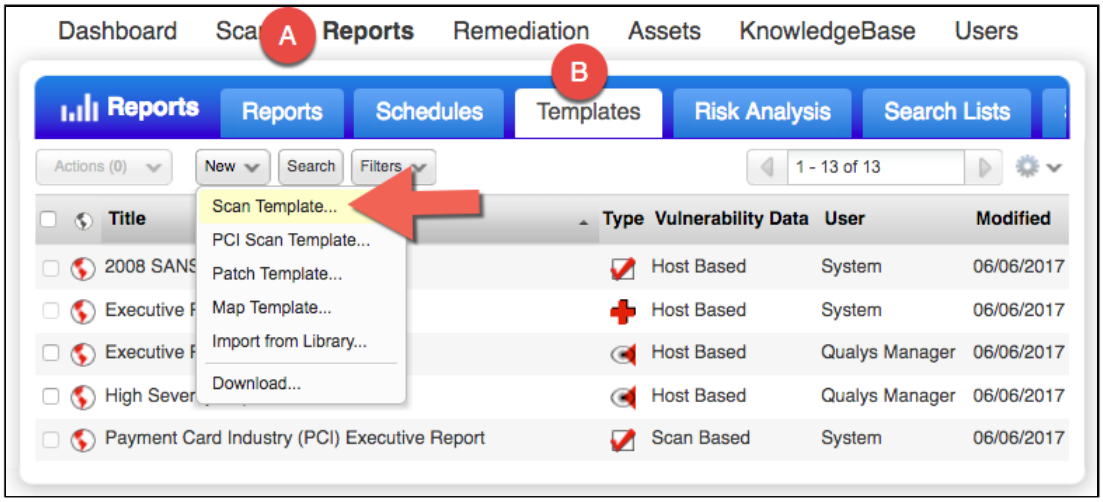
   It is important to note that the steps above will ignore one vulnerability specifically for one host. Other host devices that might have this same vulnerability will not be affected by these actions.

3. **Close the report.**

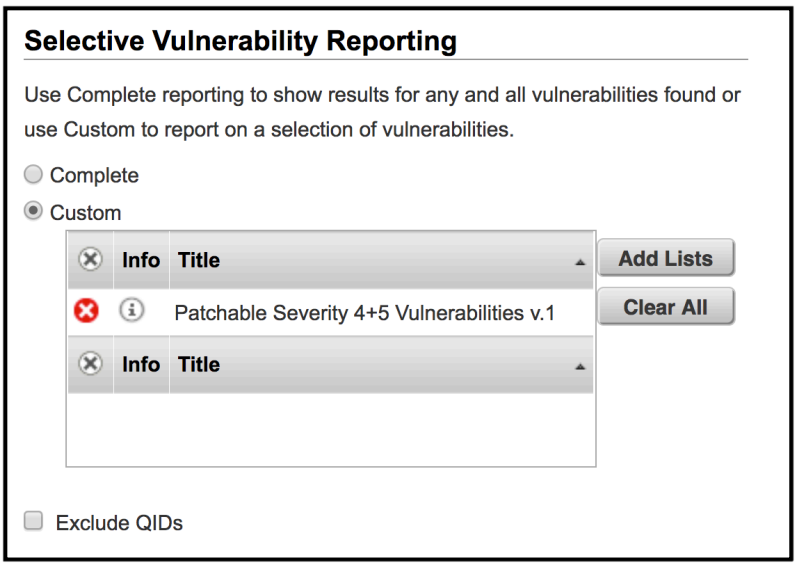
Selective Vulnerability Reporting

Best Practice: Scan for everything, and then be selective (customize) in your reporting.

The last exercise used an "out-of-the-box" report template. This exercise will have you create a custom report template that targets one group of vulnerabilities, while excluding a second group of vulnerabilities.



1. **Navigate to A) the "Reports" section, and click B) the "Templates" tab.**
2. **Click the "New" button and select the "Scan Template…" option.**
3. **Title the report "Patchable Severity 4+5 Vulnerabilities".**
4. **Click "Findings" in the navigation pane (left) and select the "Windows" Asset Tag as the target for this report.**
5. **Click "Display" in the navigation pane (left) and scroll down to the "Detailed Results" section. Choose the option to sort by vulnerability and select the check box to include the Vulnerability Details.**



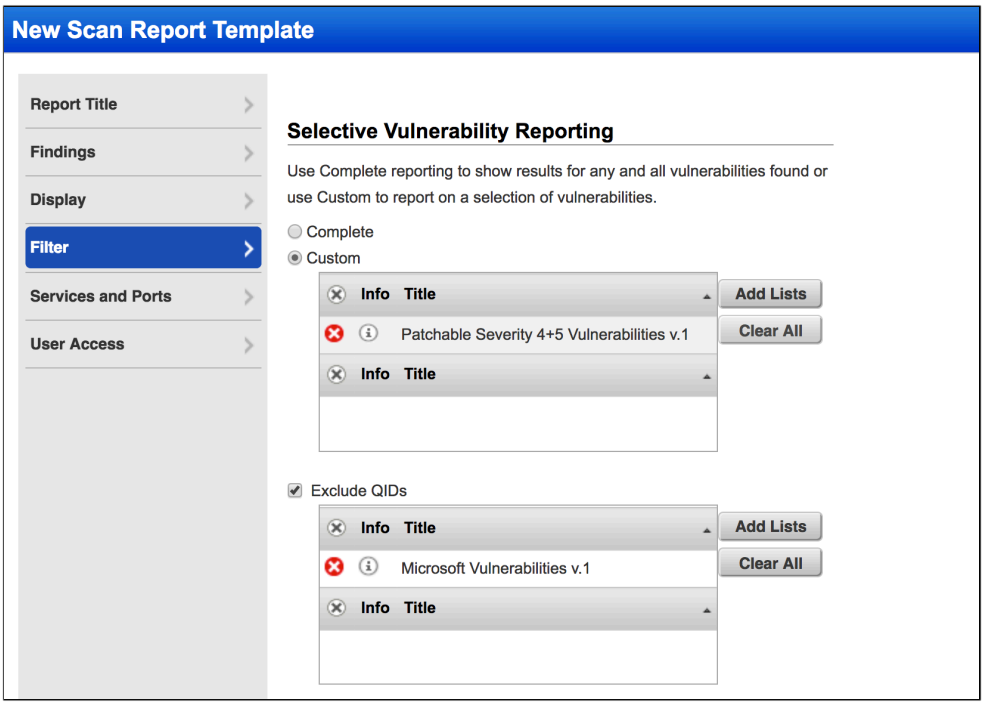
6. **Click "Filter" in the navigation pane (left) and click the "Custom" radio button in the "Selective Vulnerability Reporting" section.**

7. **Click the "Add Lists" button and select the "Patchable Severity 4+5 Vulnerabilities v.1" Search List. Click "OK."**

8. **Click the**

button to test your custom filter.

9. **Close the report, returning to the "New Scan Report Template" window.**



10. **Click the "Exclude QIDs" checkbox, and then click the "Add Lists" button.**

11. **Select the "Microsoft Vulnerabilities v.1" Search List.**

    If the list of "Critical Vulnerabilities with Vendor Patches" contains "Microsoft Vulnerabilities" they will be excluded from the report.

12. **Click the**

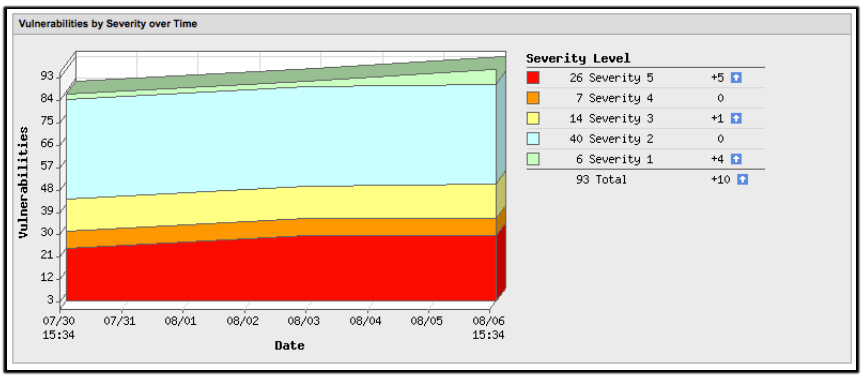
button again to test your custom filter with the new exclusion list.

13. **Close the report and "Save" the report template.**

Scheduled Reporting

Like with mapping and scanning, users can schedule reports to run automatically at a scheduled time, or recurring basis. Users can also set options to notify select distribution groups when a report is complete and ready for viewing.

In the steps that follow, a new template-based scan report will be scheduled using the "Executive Report" template.

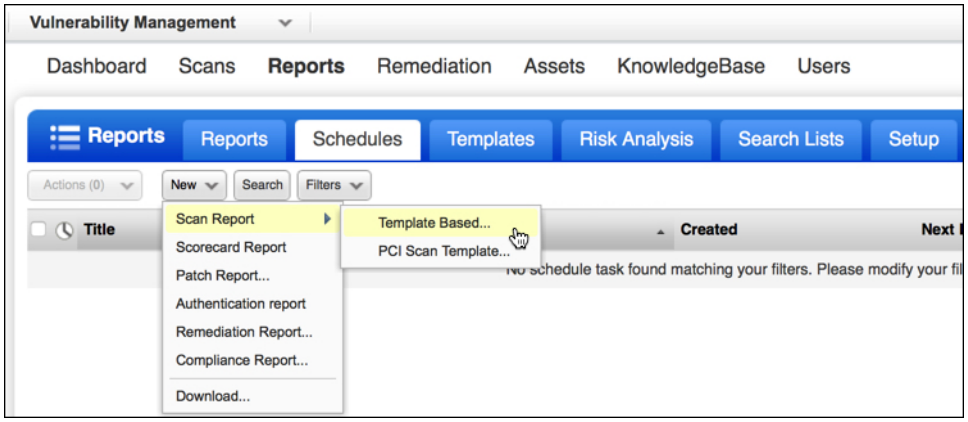


The Executive Report is a high-level trend report. It identifies changes to the vulnerability exposure of your network over time.

5 Biggest Categories

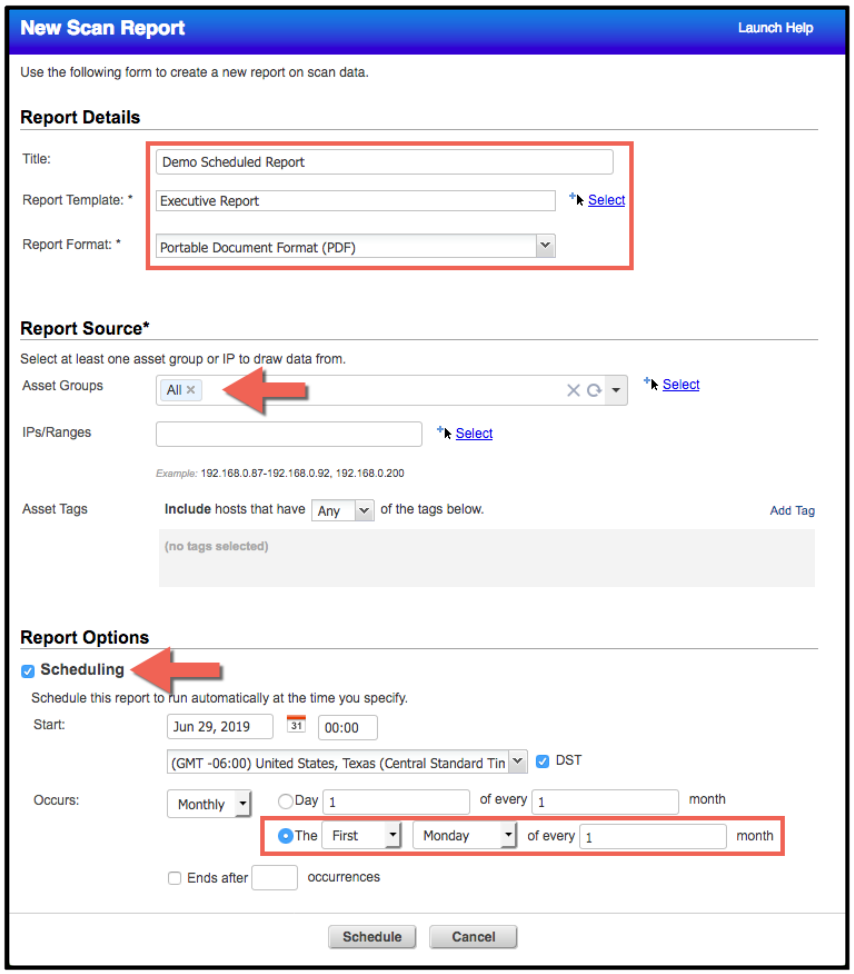
Category		Confirmed (Trend)	Potential (Trend)	Information Gathered	Total (Trend)	
Windows	34	(+4)	-	-	34	(+4)
Web server	14	(0) –	-	-	14	(0) –
TCP/IP	12	(+4)	-	-	12	(+4)
SMB / NETBIOS	10	(+1)	-	-	10	(+1)
RPC	8	(+1)	-	-	8	(+1)
Total	**78**	**(+10)**	**-**	**-**	**78**	**(+10)**

The "Top Vulnerability Categories" table in the Executive Report, illustrates the areas that need the most work, and how much the exposure has changed, so you can allocate resources to cover your most critical needs.



1. **Within the Reports section, navigate to the "Schedules" tab.**

2. **Click the New button and select Scan Report > Template Based.**



3. **Type "Demo Scheduled Report" in the "Title" field.**

4. **Select "Executive Report" in the "Report Template" field.**

5. **Select “Portable Document Format (PDF)” in the “Report Format” field.**

6. **Under Report Source, select the “All” Asset Group.**

7. **Under Report Options, click the “Scheduling” check box.**

8. **Leave the start date and time at their default values.**

9. **Select a time zone of your own preference.**

10. **Select “Monthly” in the “Occurs” field, along with the radio button option for the first Monday of every month (see the illustration above).**

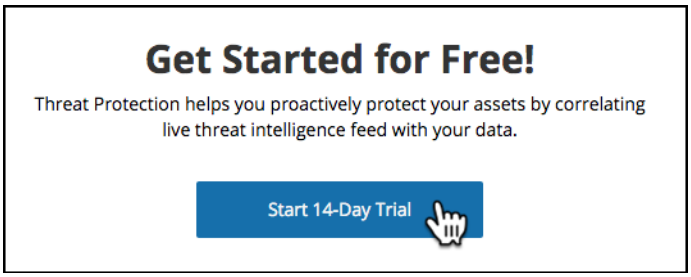
11. **Click the Schedule button to finish.**

LAB 6: Threat Protection (20 min.)

Activate Threat Protection

When activated, the Qualys Threat Protection application provides additional features to VM that will help you create reports to identify vulnerabilities associated with various Real-Time Threat Indicators:

1. **From within the Application Picker, click the Threat Protection option.**



2. **Click the "Start 14-Day Trial" button, "Confirm", and then "Close and Continue" button.**

Reporting with Threat Protection RTIs

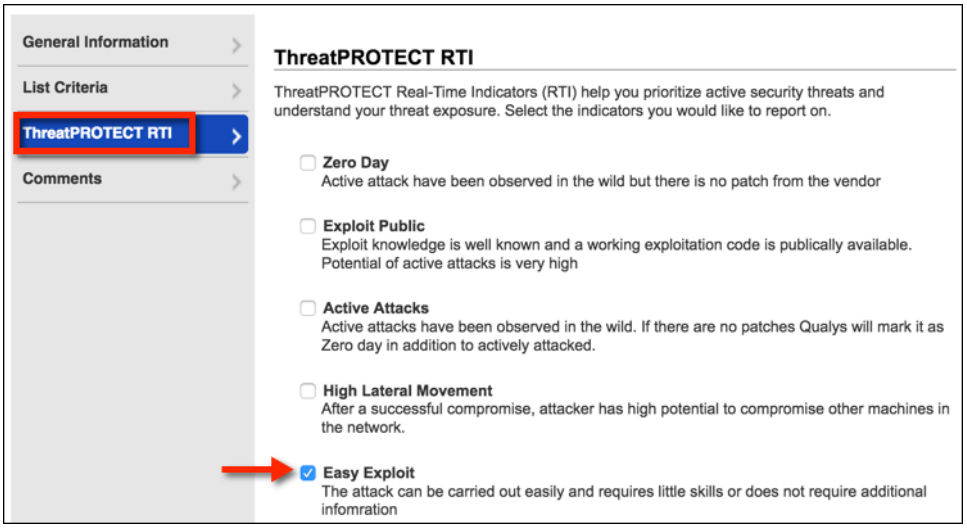
A vulnerability becomes a greater risk when it has an associated threat. Qualys Threat Protection will help you identify the vulnerabilities associated with the following Real-Time Threat Indicators:

> Public Exploit – Zero Day – Actively Attacked – High Lateral Movement – Exploit Pack – Easy Exploit – No Patch Available – High Data Loss – Denial of Service – Malware.

Search Lists with Threat Protection RTIs

You can use Threat Protection RTIs in a report to drive remediation of your assets under immediate threat.

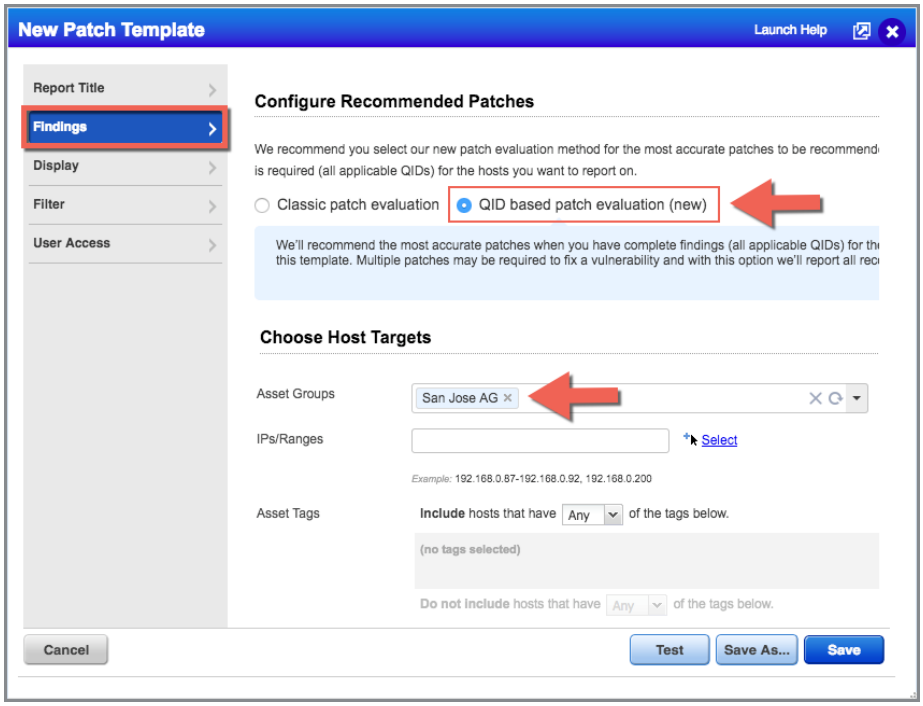
1. **Use the application drop-down menu to open the Vulnerability Management application**
2. **Click on the "Reports" section followed by the "Search Lists" tab.**
3. **Click the "New" button and select the option for "Dynamic List…".**
4. **Type "Easy Exploit" in the "Title" field.**



5. **Under the "Threat Protection RTI" tab, click the option for "Easy Exploit".**
6. **Click the "Save" button.**

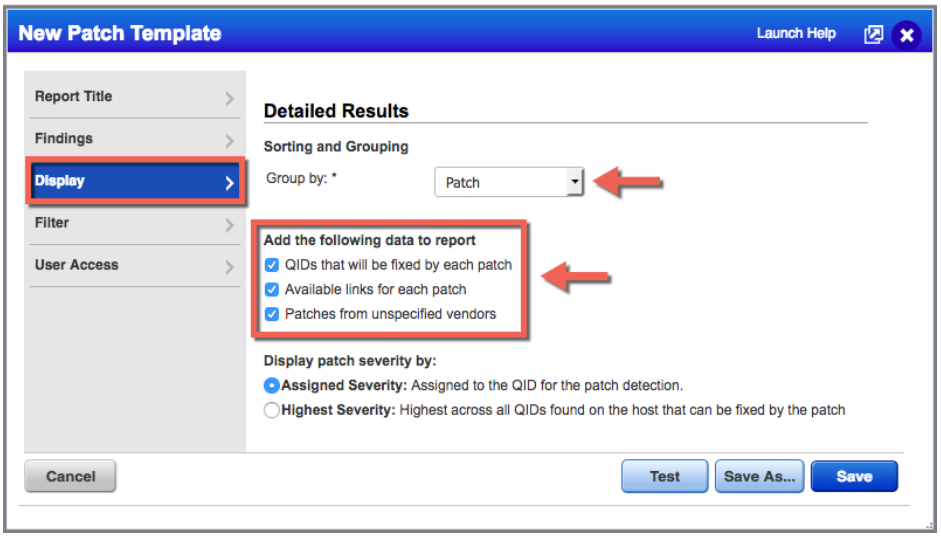
Create Patch Report with Threat Protection RTI

1. **Click the "Reports" section and the "Templates" tab.**
2. **Click "New" and select "Patch Template…".**
3. **Type "Patchable Vulnerabilities - Easily Exploited" in the "Title" field.**



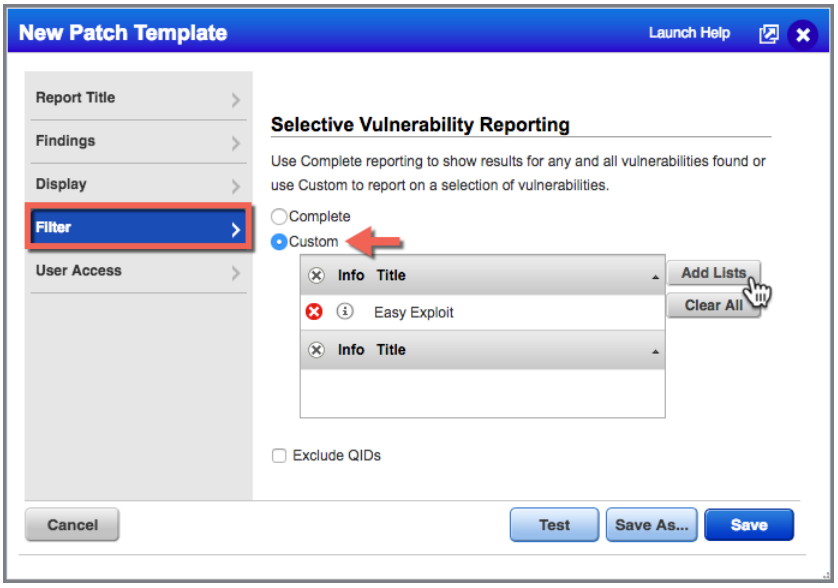
4. **Click "Findings" in the navigation pane (left) and select the option for "QID based patch evaluation (new)".**

5. **Choose "AG: San Jose" as the host target.**



6. **Click "Display" in the navigation pane (left) and select "Patch" using the "Group by" drop-down menu.**

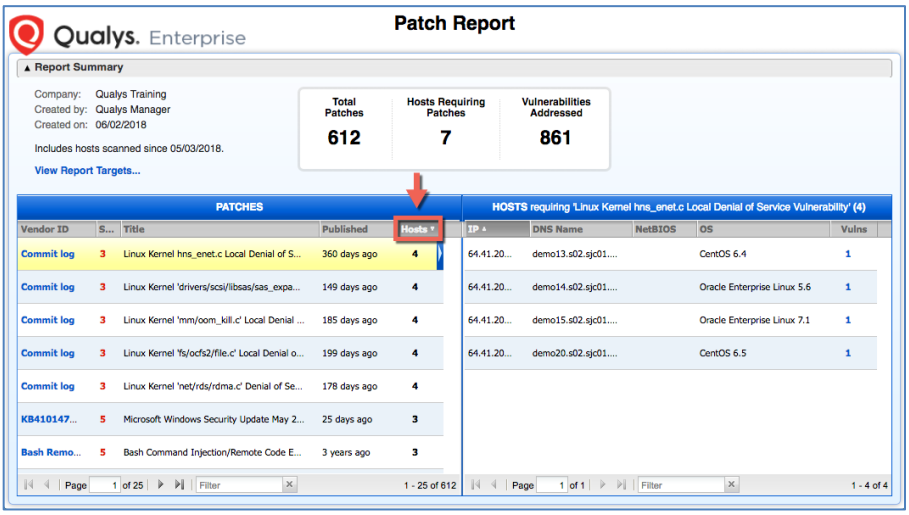
7. **Check all the boxes under "Add the following data to report."**



8. **Click "Filter" in the navigation pane (left) and click the "Custom" radio button.**

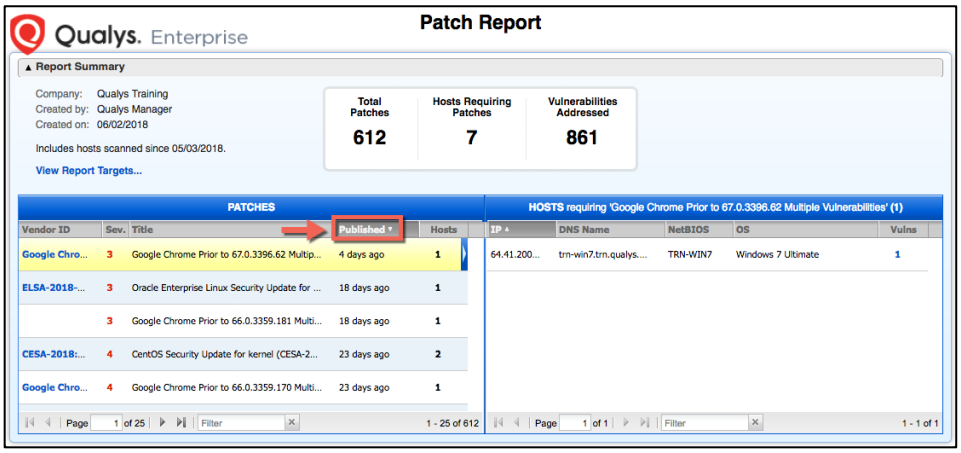
9. **Click the "Add Lists" button and select the checkbox next to the "Easy Exploit" Search List you built in the previous section, and then click "OK".**

10. **Click the "Test" button to preview your report configuration settings.**



11. **Click the "Hosts" column header in the left pane, until patches with the greatest number of hosts appear at the top of the list.**

    Knowing which patches impact the greatest number of hosts can be useful information, when creating patch deployment schedules.



12. **Click the "Published" column header in the left pane, until the most recently published patches appear at the top of the list.**

    These are the latest threats impacting your host assets.

13. **Click the "Published" column header again, until the oldest patches appear at the top of the list.**

    Outdated patches should be investigated to determine and record the reason for failing to apply timely patches. Patchable vulnerabilities still remain the preferred targets of active exploits.

14. **Close the report and return to the "New Patch Template" editor.**

15. **Click the "Save" button.**

LAB 7: User Management (10 min.)

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.

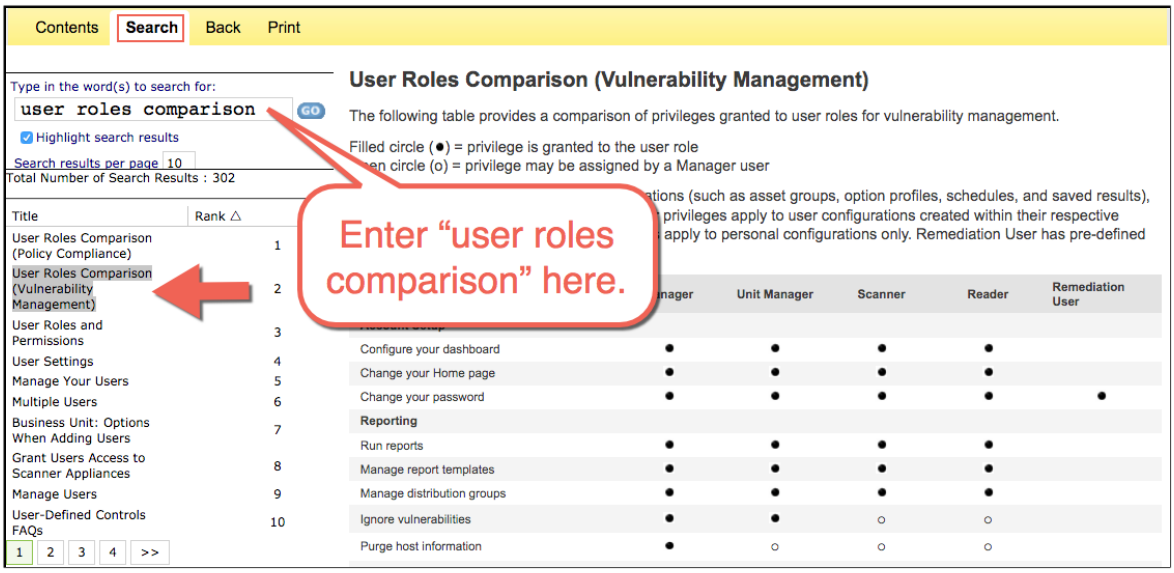
User Roles

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.



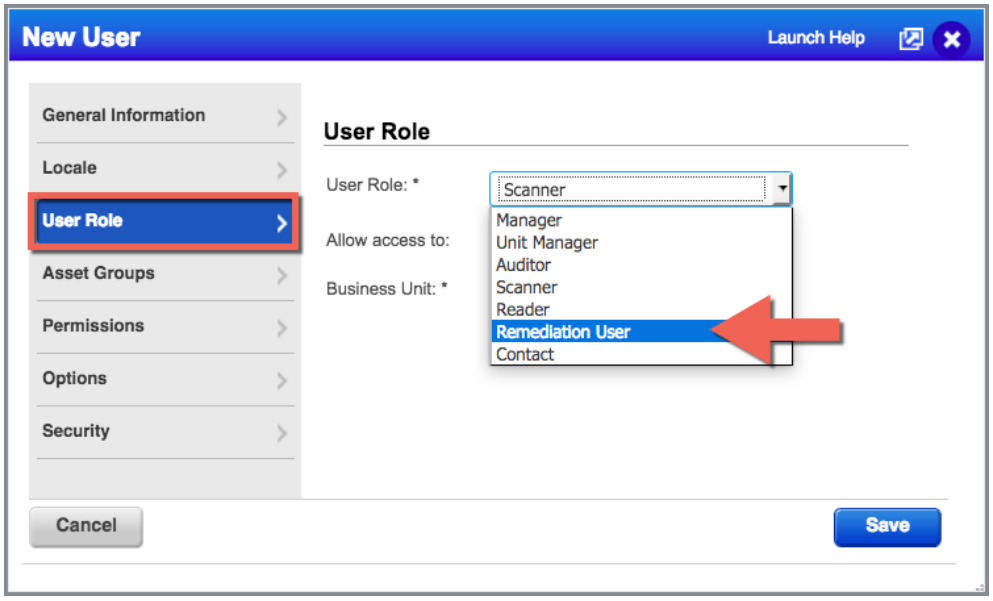
To view a comprehensive comparison of all Vulnerability Management user roles:

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.**

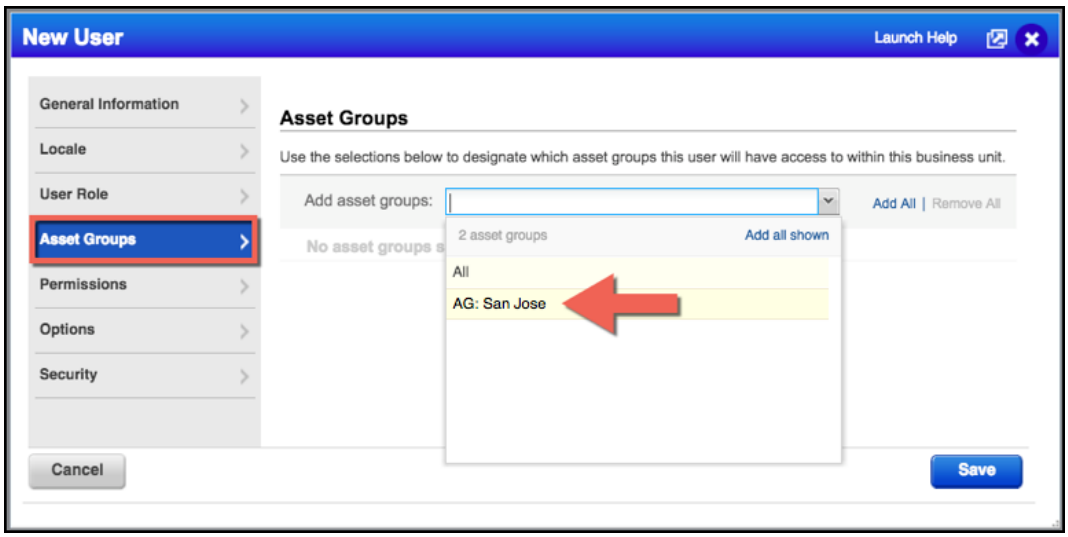
Create User Account

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.**

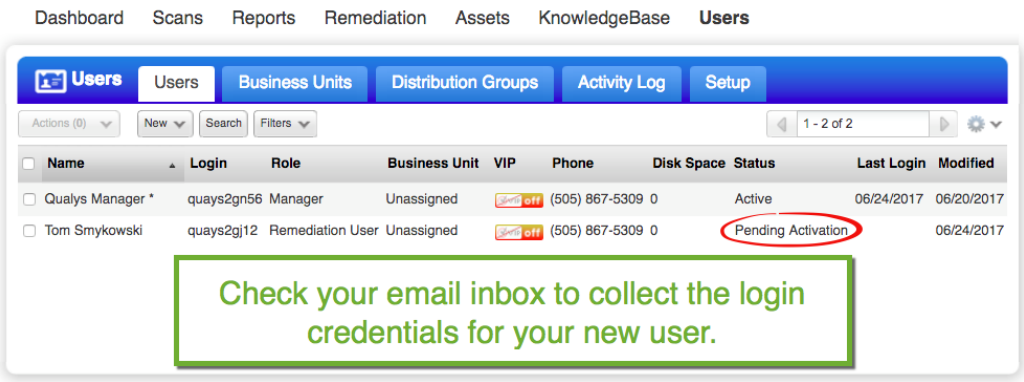


4. **Click "User Roles" in the navigation pane (left) and choose "Remediation User" as your User Role.**



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.**

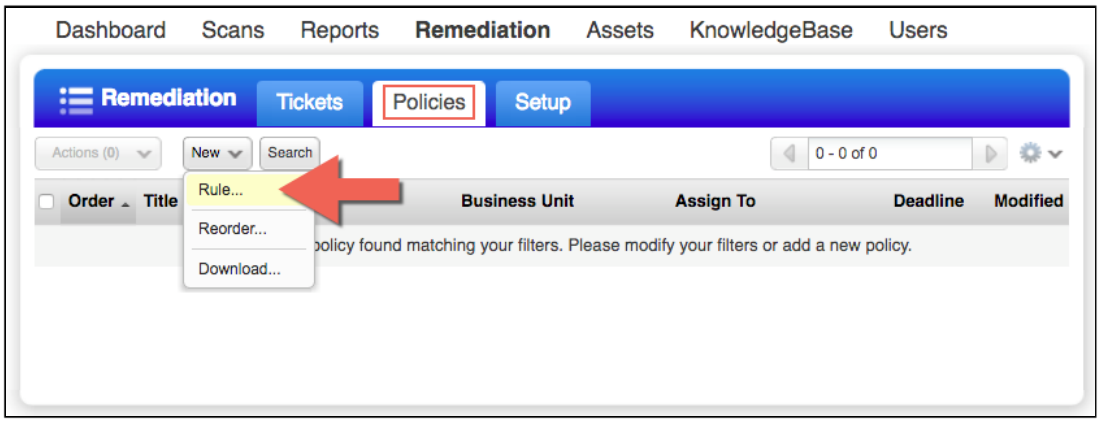
   The email activation link can only be used once, so make sure you save the credentials.

LAB 8: Remediation (15 min.)

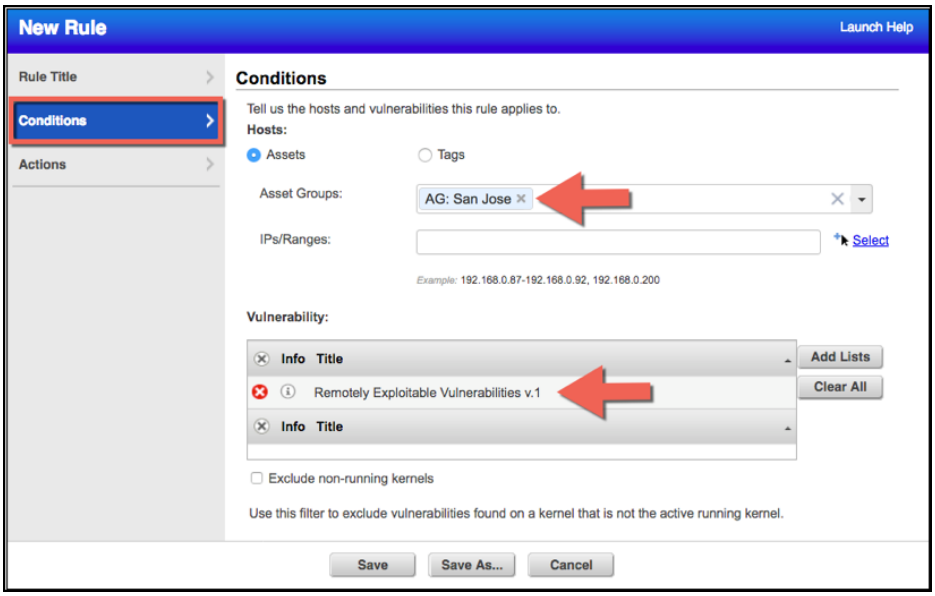
In this lab, you will create a Remediation Policy that assigns vulnerabilities to a specific user, and a second policy that ignores vulnerabilities that will not be addressed or resolved.

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.

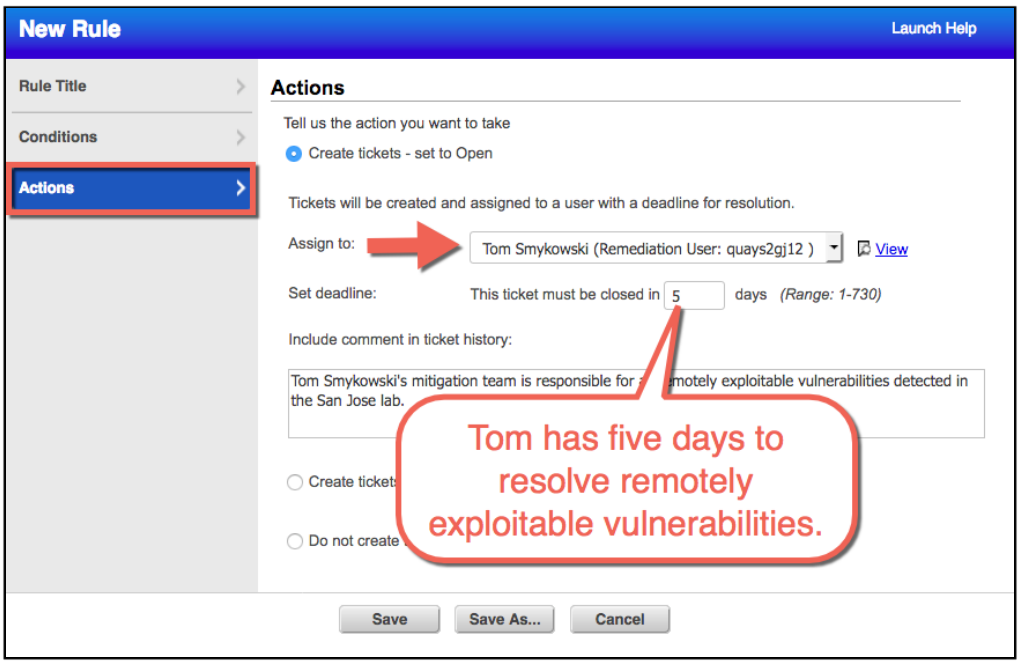


1. **Navigate to the "Remediation section, and click the "Policies" tab.**
2. **Click the "New" button and select the "Rule…" option.**
3. **Type "Remotely Exploitable Vulnerabilities" in the "Title" field.**



4. **Click "Conditions" in the navigation pane (left) and replace "All" with "AG: San Jose" as the host asset target for this policy.**
5. **Click the** Add Lists **button, just to the right of the "Vulnerability" dialog box.**

6. **Scroll down, select the "Remotely Exploitable Vulnerabilities v.1" check box, and click the "OK" button.**



7. **Click "Actions" in the navigation pane (left), and assign all detected, remotely exploitable vulnerabilities to the "Remediation User" account created in the "User Management" lab.**

8. **Change the value of the "Set deadline" field from 7 to 5 days.**

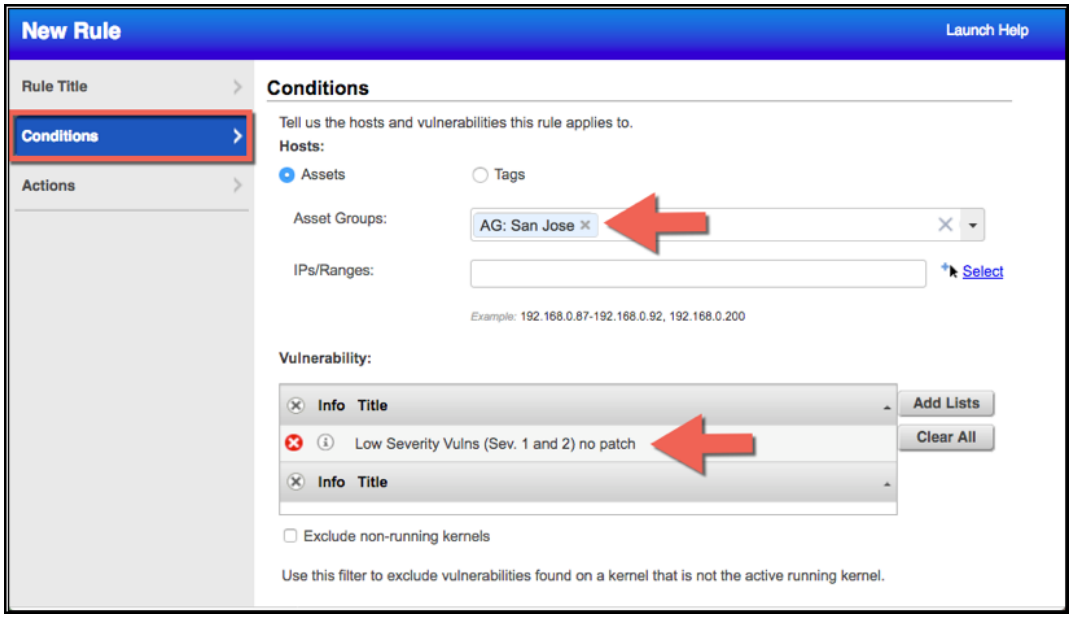
   Vulnerabilities that have not been mitigated or resolved within 5 days will be flagged as overdue.

9. **Click the "Save" button.**

Ignore Low Risk Vulnerabilities

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

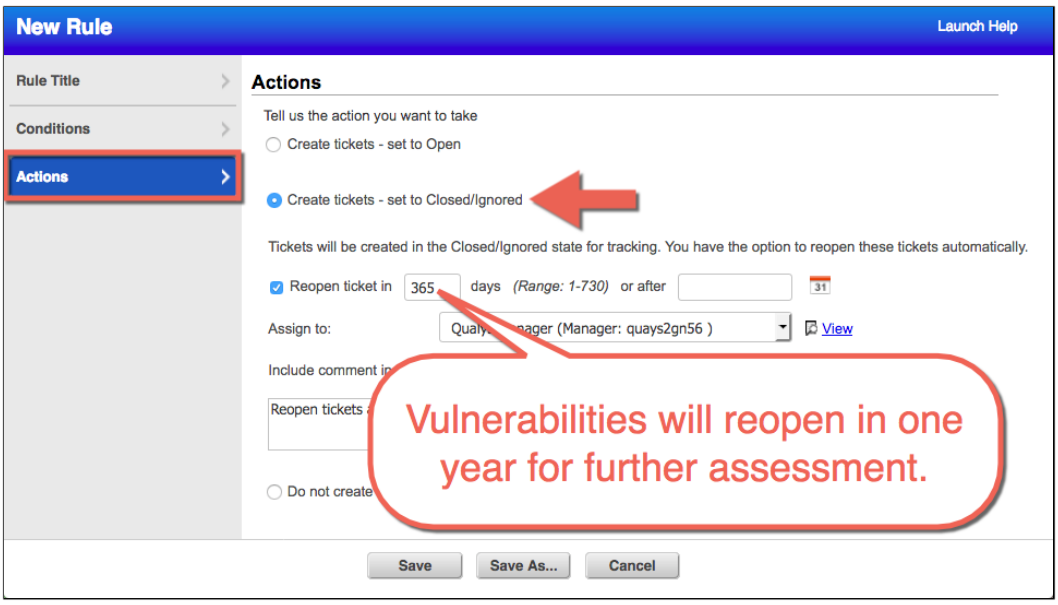
1. **From the "Remediation" section, click the "Policies" tab and create a new Remediation Rule titled "Ignore Low Risk Vulnerabilities".**



2. **Click "Conditions" in the navigation pane (left) and replace "All" with "AG: San Jose" as the host asset target for this policy.**

3. **Click the** Add Lists **button, just to the right of the "Vulnerability" dialog box.**

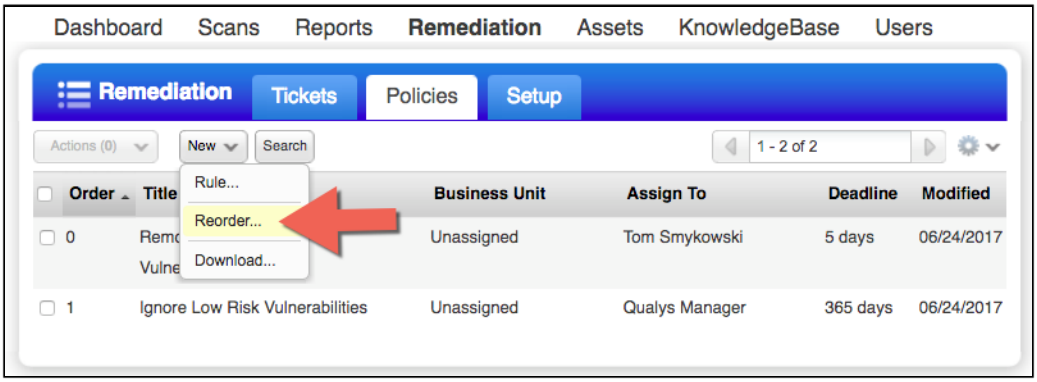
4. **Scroll down, select the "Low Severity Vulns (Sev. 1 and 2) no patch" check box and click the "OK" button.**



5. **Click "Actions" in the navigation pane (left), and select the "Create Tickets – set to Closed/Ignored" radio button (the dialog box will change).**
6. **Configure the option to reopen vulnerabilities in 365 days (one year).**

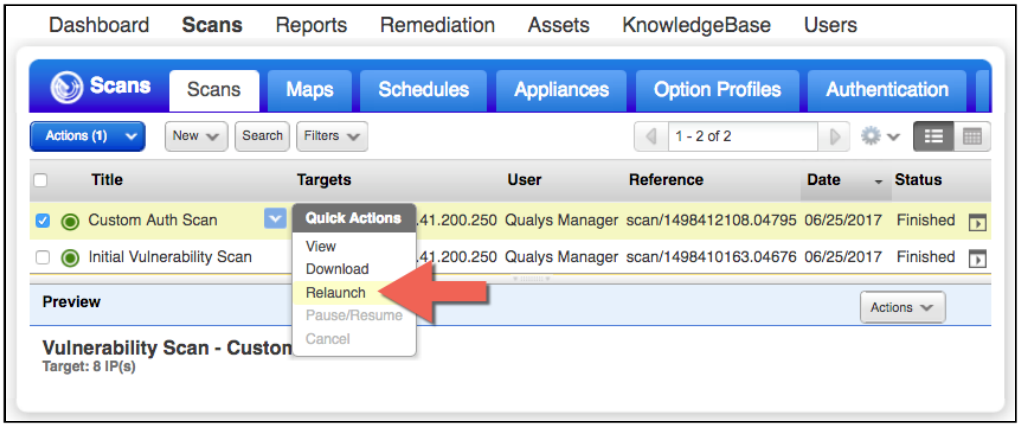
   This option is convenient for those who wish to re-assess the risk of ignored vulnerabilities at regular intervals.
7. **Assign "ignored" vulnerabilities to the "Manager" account, when they are reopened.**
8. **Click the "Save" button.**

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



9. **From the "Policies" tab, click the "New" button and experiment with the "Reorder" option.**

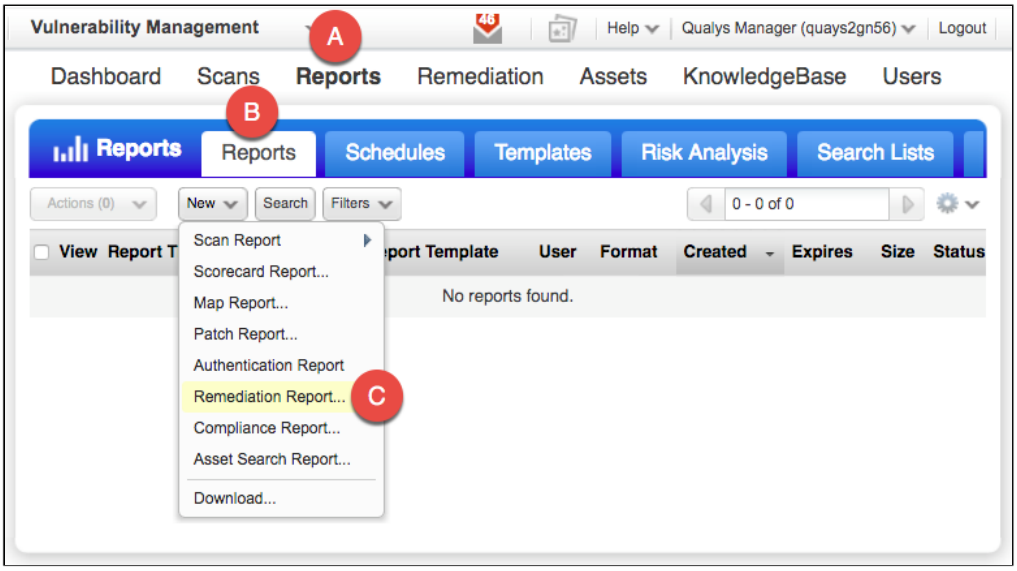
An additional vulnerability scan will be required here, to see the results of the Remediation Policies just created.



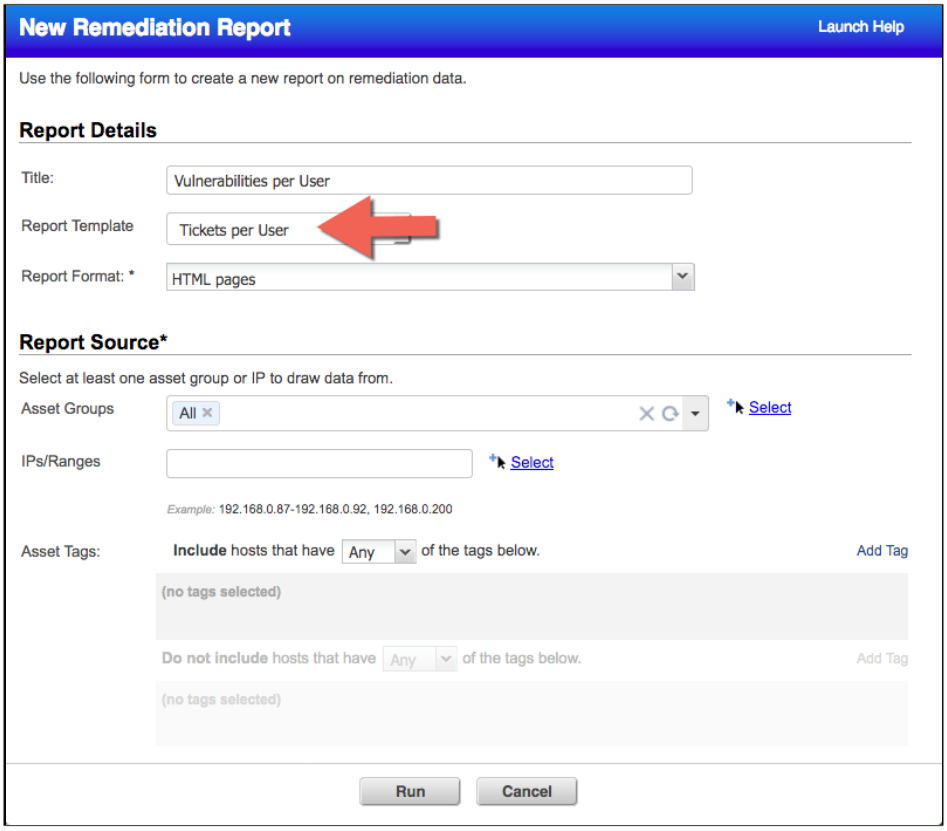
10. **Navigate to the "Scans" section and the "Scans" tab.**
11. **Use the "Quick Actions" menu to "Relaunch" the "Custom Auth Scan."**

Create Remediation Report

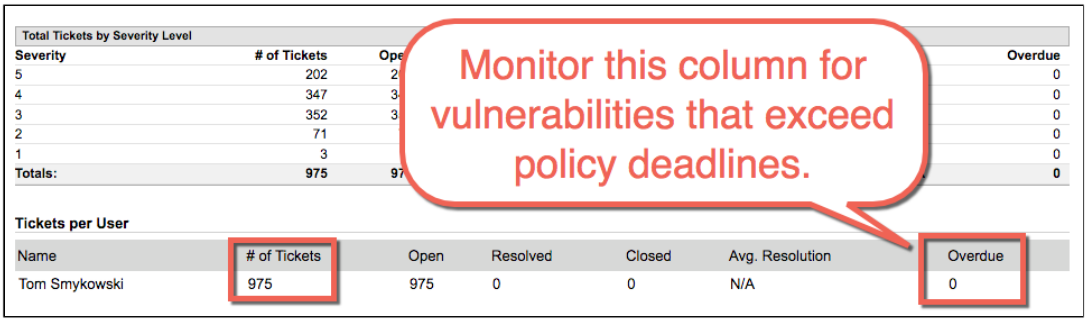
With the creation of at least one remediation policy, you can build reports reflecting the progress of your patching and mitigation activities.



1. **Navigate to A) the "Reports" section, followed by B) the "Reports" tab.**
2. **Click the "New" button and select C) the "Remediation Report…" option.**



3. **Type "Vulnerabilities per User" in the "Title" field.**
4. **In the "Report Template" field select the "Tickets per User" option.**
5. **Use the "HTML pages" report format.**
6. **Leave the "Report Source" and all other setting at their default values.**
7. **Click the "Run" button.**



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

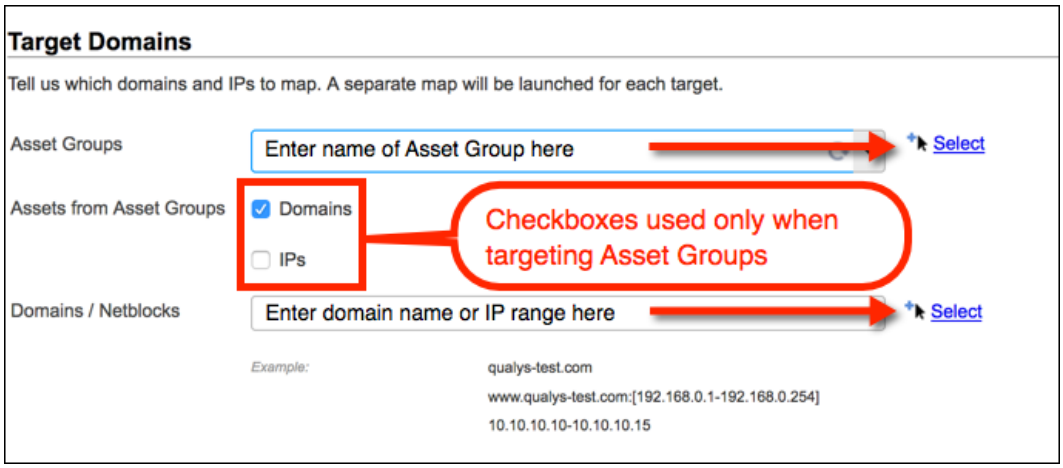
Map reports are very useful tools when managing all host assets within your company or enterprise architecture. Only mapping provides "discovery" data that will allow you to distinguish between authorized and unauthorized hosts. When used properly, mapping can help you add a new host to your Vulnerability 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

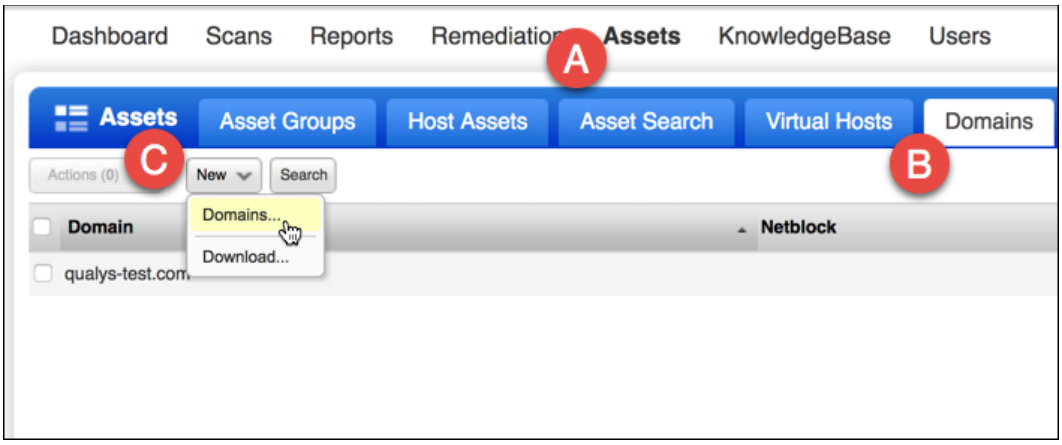
Another target option for mapping involves using a domain name. A domain name must be added to the "Domains" tab, before it can be used as a target for mapping. Basic DNS reconnaissance is used to collect information from a domain target. Additionally, TCP, UDP, and ICMP probes are used to validate the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

Netblock

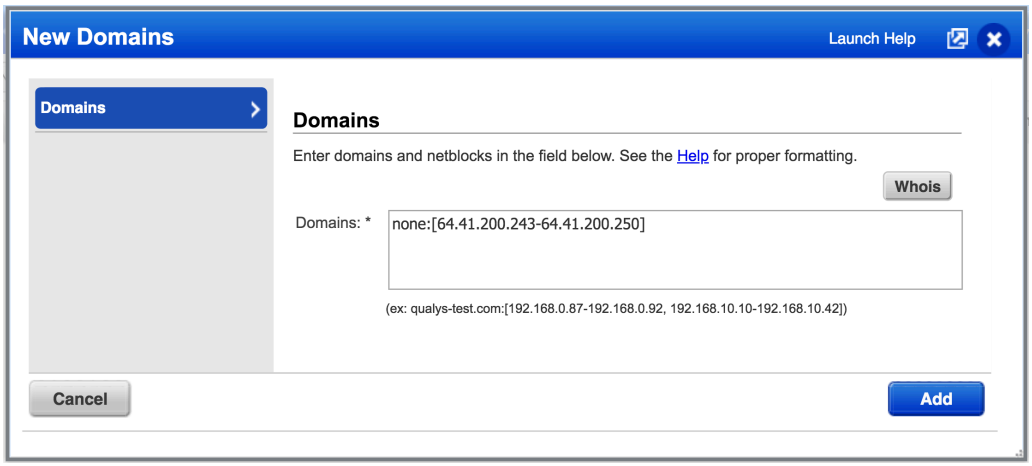
A netblock must also be added to the “Domains” tab, before it can be used as a mapping target. The “none” Domain is a special domain, used to add netblocks to the “Domains” tab. Various probes such as TCP, UDP, and ICMP are used to locate LIVE hosts within the targeted netblock.

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]`

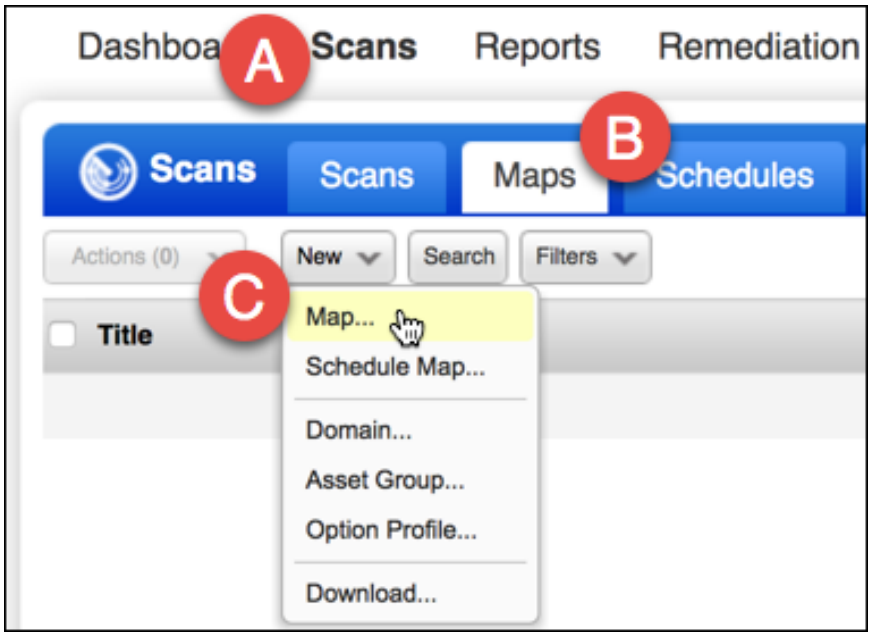
   DO NOT USE COPY AND PASTE (there is no blank space in the “none” domain).

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.

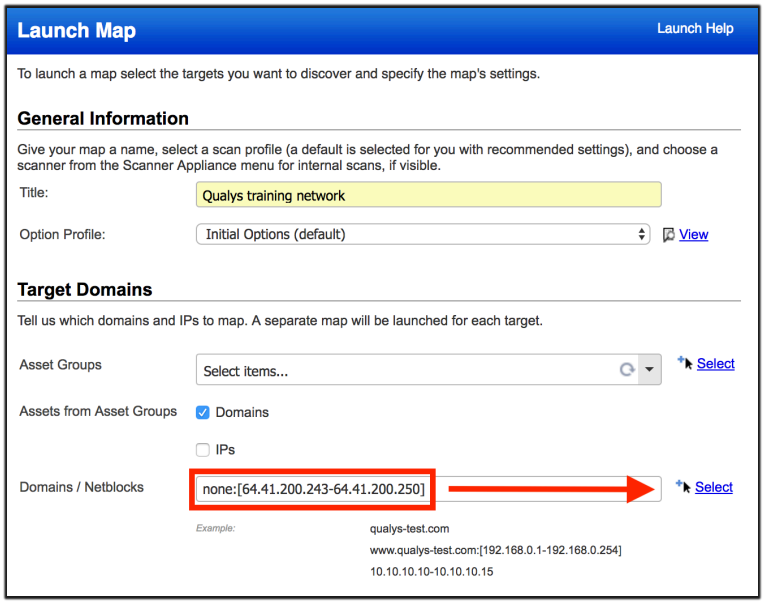
3. **Click the “OK” button to acknowledge your scanning permission.**

Launch Map

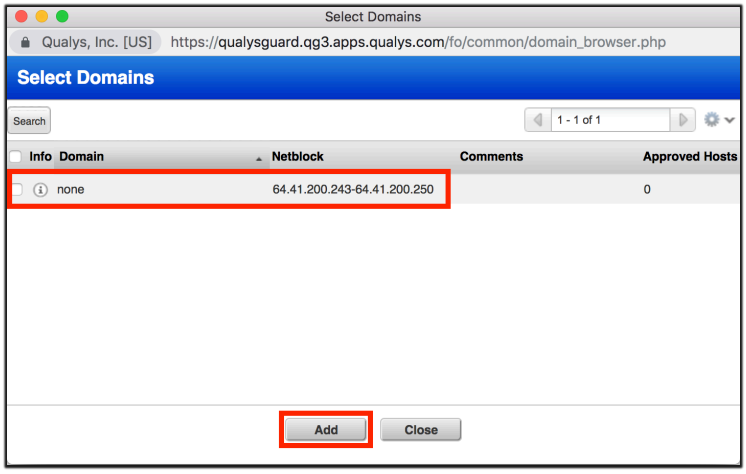
In the next few exercise steps, you will use the "none" domain target to create a Map Report of the hosts within the Qualys Training Network.



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.**



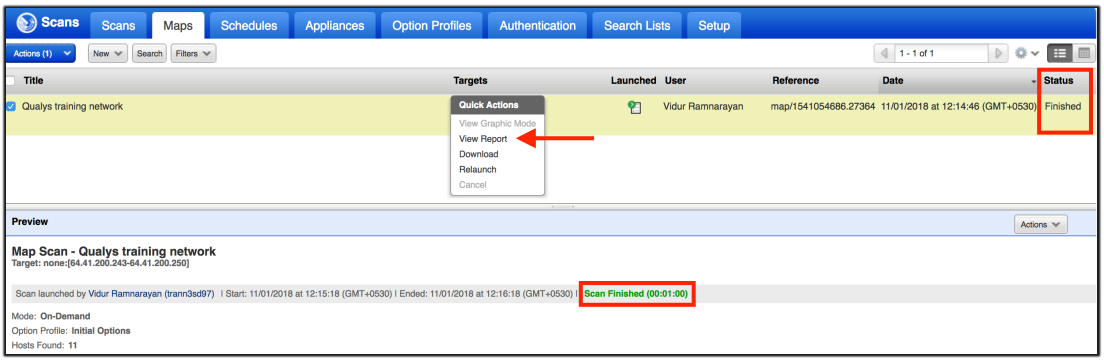
2. **In the "Title" field type: "Qualys Training Network".**
3. **Leave the Option Profile set to: Initial Options (default).**
4. **Under "Target Domains" click the "Select" link just to the right of the "Domains/Netblocks" field.**



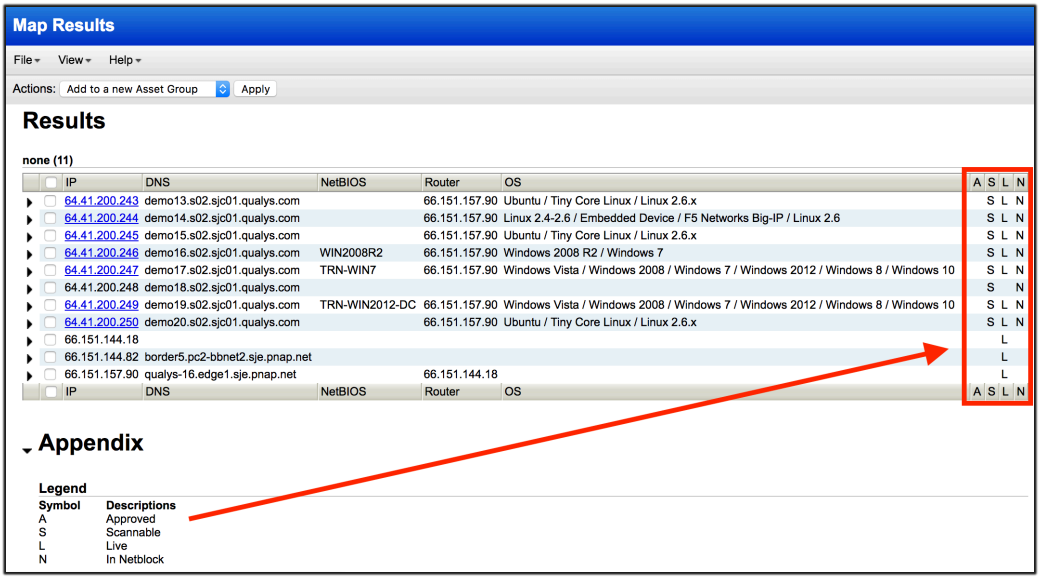
5. **Check the "none" Domain and click the "Add" button.**
6. **Click the "Launch" button to begin mapping. It is normal for your map task to display the "Queued" status, before changing to the "Running" status.**

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.



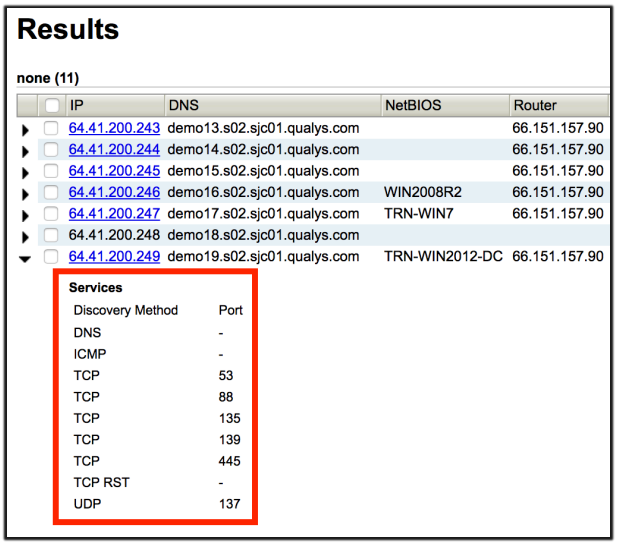
1. **To view your finished map results, open the Quick Action menu and select the "View Report" option.**



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.

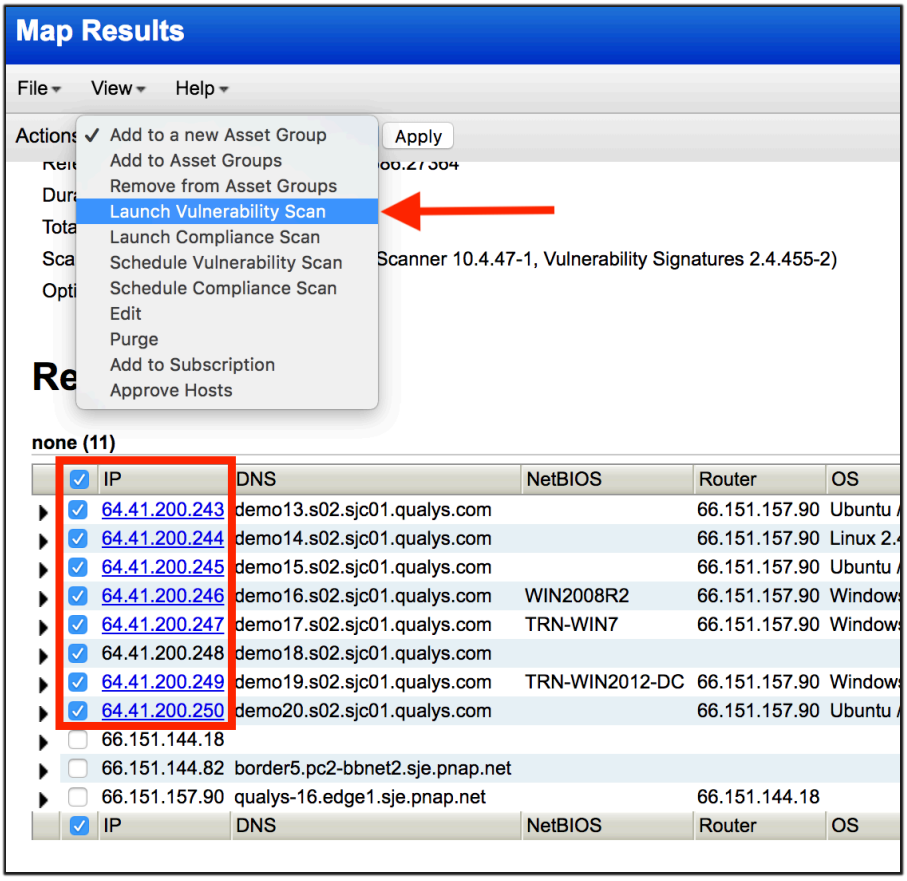


3. Click the arrow icon ▶ to the left of a host to view its discovery method.

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.

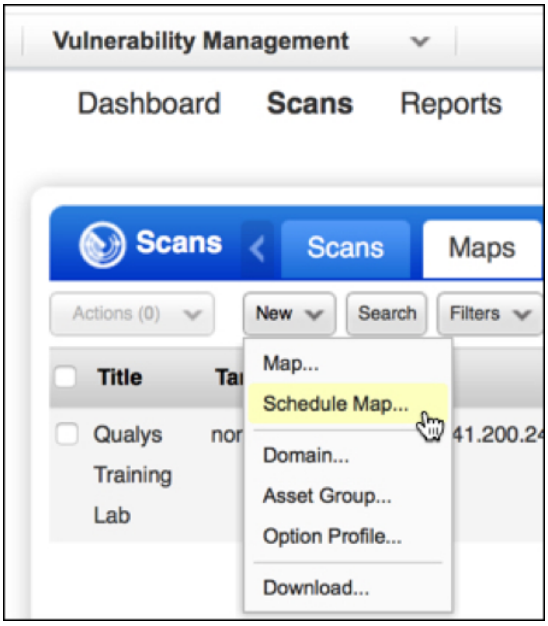


1. **Close the Map Results (File > Close).**

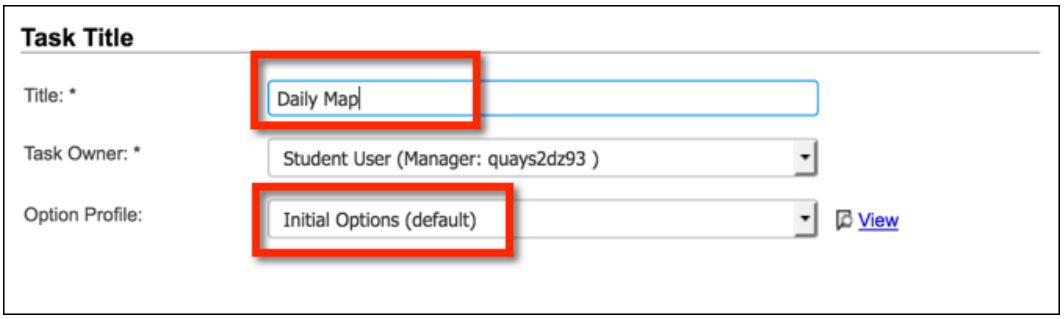
Scheduled Maps

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.

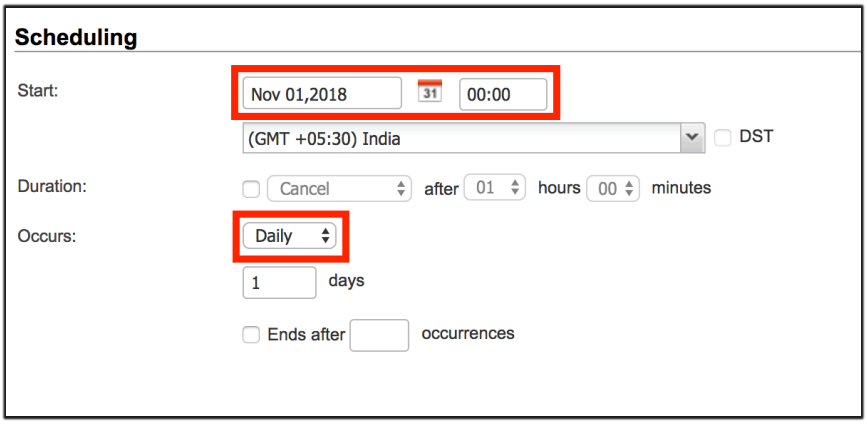
Reporting like this relies on having regular snapshots of the network from which to make a comparison. The next lab steps are designed to schedule a Map Report to run every day.



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]**



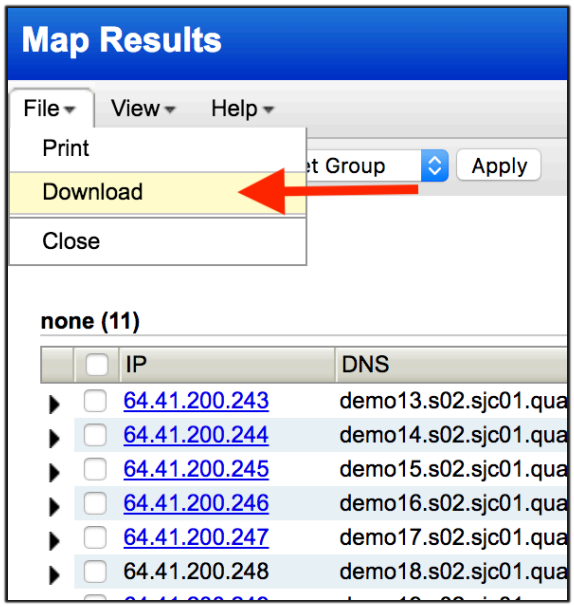
- **Scheduling: Start the scheduled task at a future date and time (time zone is required)**
- **Occurs: Daily**

3. **Click "Save".**

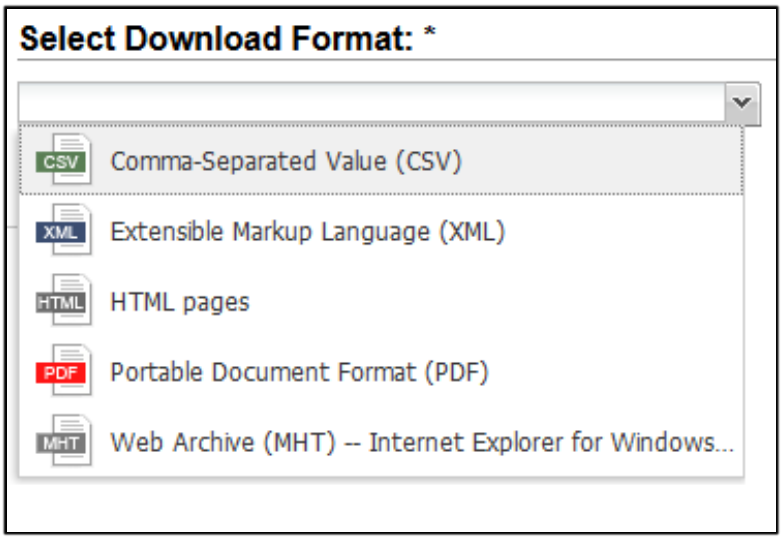
Export and View Map Results

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

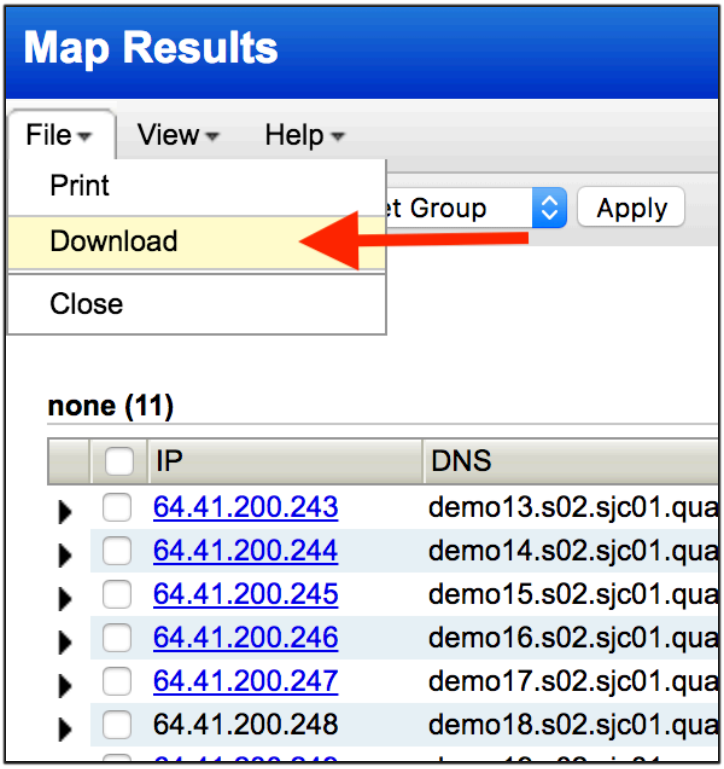
1. **Navigate to the "Maps" tab within the "Scans" section.**
2. **Use the Quick Actions menu to open up and view a Map that you have already created.**



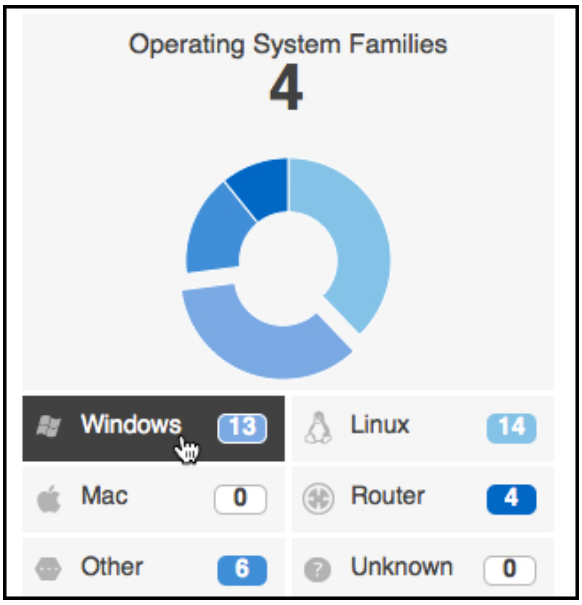
3. **While viewing the map results, click the "File" menu and select the "Download" option.**



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.**

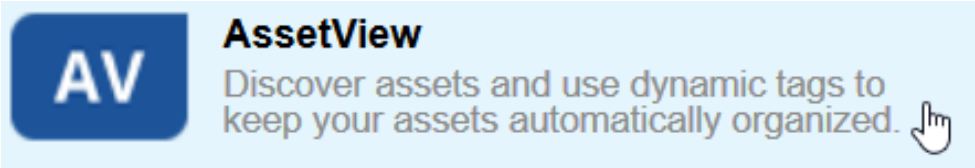


5. **Use the filters on the left to locate the Windows assets in the map results (right). Experiment with different OS options.**
6. **Click the icon over any host to view its information in the preview pane.**

   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: Asset Tag Examples

Provided here are some additional Asset Tagging examples, using different Asset Tag Rule Engines. The first three Asset Tag examples, will be created using AssetView.

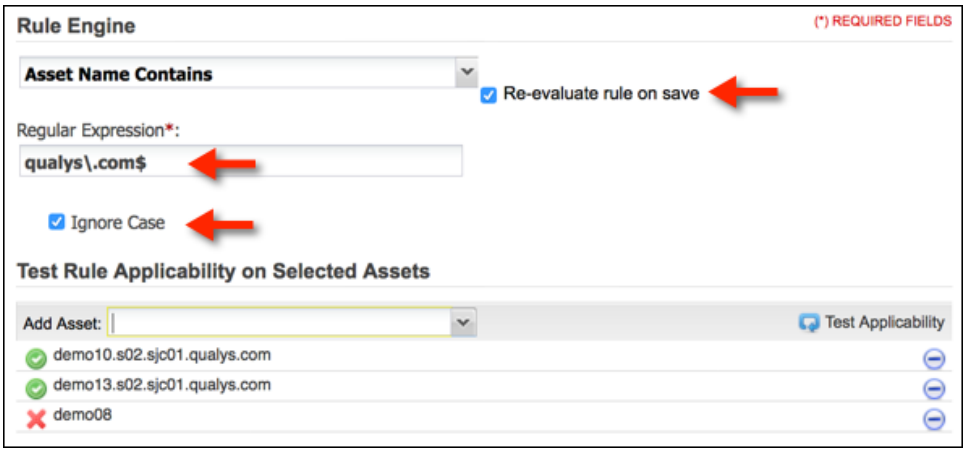


1. **Open the AssetView application.**
2. **Navigate to the "Assets" section, followed by the "Tags" tab.**

Asset Name Contains Rule Engine

If your host asset names contain useful pieces of information (e.g., device type, function, owner, location, etc…), the "Asset Name Contains" Rule Engine can help you create tags by parsing through host asset names.

1. **From the "Tags" tab, click the "New Tag" button.**
2. **Type "Qualys" in the "Name" field, and click the "Continue" button.**



3. **Select "Asset Name Contains" from the "Rule Engine" drop-down menu.**
4. **Type** `"qualys\.com$"` **(omit quotes) in the "Regular Expression" field.**
5. **Select the "Ignore Case" check box, and the "Re-evaluate rule on save" check box.**
6. **Use the "Test Rule Applicability on Selected Assets" section to validate your regex against various host assets.**

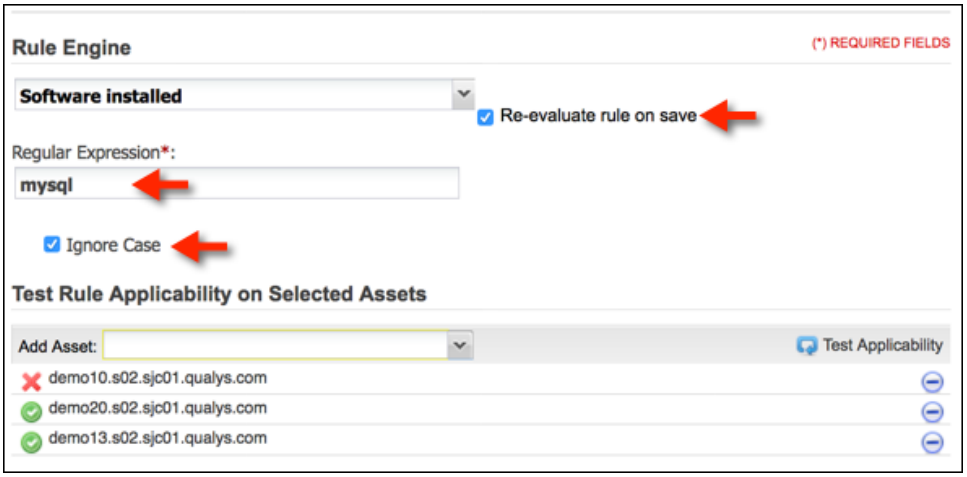
   A properly constructed regex will place tags on hosts that have an asset name that ends with 'qualys.com'.

7. **Click "Continue" and "Finish".**

Software Installed Rule Engine

The “Software Installed” Rule Engine can help you tag assets that are hosting targeted software applications.

1. **From the “Tags” tab, click the “New Tag” button.**
2. **Type “MySQL” in the “Name” field, and click the “Continue” button.**



3. **Select “Software Installed” from the “Rule Engine” drop-down menu.**
4. **Type** `“mysql”` **(omit quotes) in the “Regular Expression” field.**
5. **Select the “Ignore Case” check box, and the “Re-evaluate rule on save” check box.**
6. **Use the “Test Rule Applicability on Selected Assets” section to validate your regex against various host assets.**

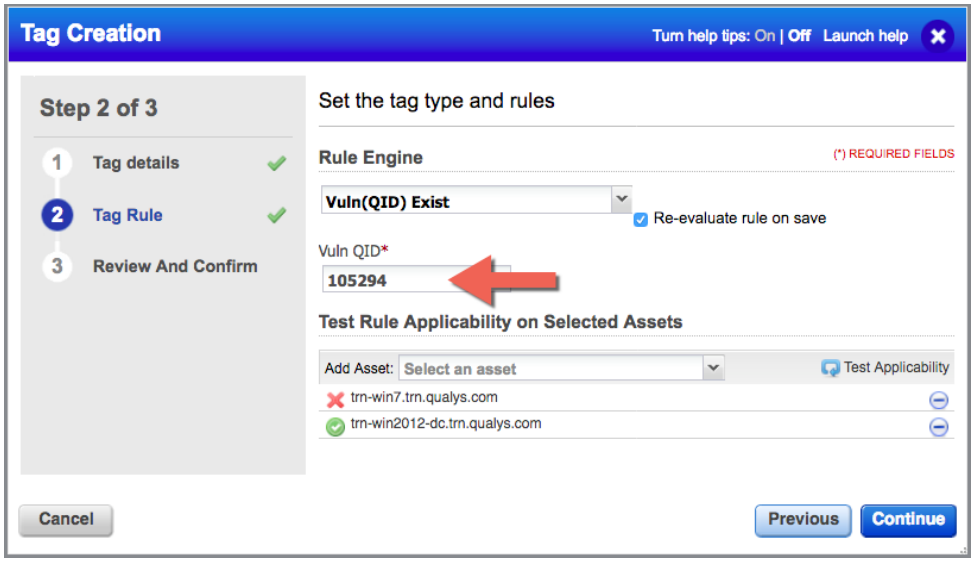
   A properly constructed regex will place tags on hosts that have the MySQL database application installed.

7. **Click “Continue” and “Finish”.**

Vuln (QID) Exists Rule Engine

Asset Tags can be assigned to host assets using any QID in the Qualys KnowledgeBase using the "Vuln (QID) Exists" Rule Engine.

1. **From the "Tags" tab., click the "New" button.**
2. **Type "Antivirus NOT Detected" in the "Name" field, and click the "Continue" button.**



3. **Select "Vuln (QID) Exist" from the "Rule Engine" drop-down menu.**
4. **Type "105294" in the "Vuln QID" field (the Title for this QID is "Antivirus Product Not Detected on the Windows Host").**
5. **Select the "Re-evaluate rule on save" check box.**
6. **Use the "Test Rule Applicability on Selected Assets" section to validate your regex against various Windows host assets.**

   A properly constructed regex will place tags on hosts that do NOT have an antivirus application installed.

7. **Click "Continue" and "Finish".**
8. **Using the example above as a guide, create another tag to identify host assets that are Windows Domain Controllers (QID 90036).**

Stale Host Tag

A retired host can add unwanted vulnerability findings to operational reports, such as a Qualys Patch Report. Asset Tags can help you identify stale or retired hosts, so their vulnerability data can be excluded from your day-to-day operational reports.

10. **Use the application drop-down menu to open the Vulnerability Management application.**
11. **Click the "Assets" section followed by the "Asset Search" tab.**
12. **In the Asset Groups section, type the word "All".**
13. **At the bottom of the Asset Search, next to "Last Scan Date", select "not within" and type "30" for the amount of day.**
14. **Click the "Create Tag" button.**
15. **Give it a name of "Stale Hosts".**

You've created a tag that will tag hosts that have not been scanned in 30 days. You can use this as a way to exclude hosts from your operational reports.

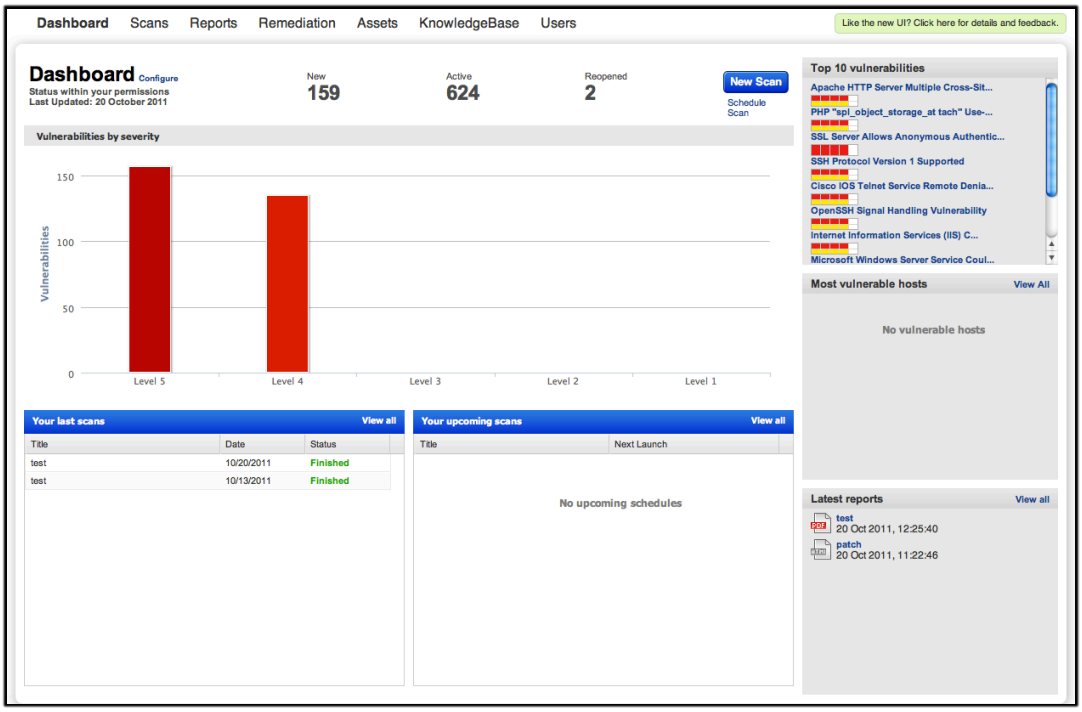
Appendix C: Account Configuration

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.**

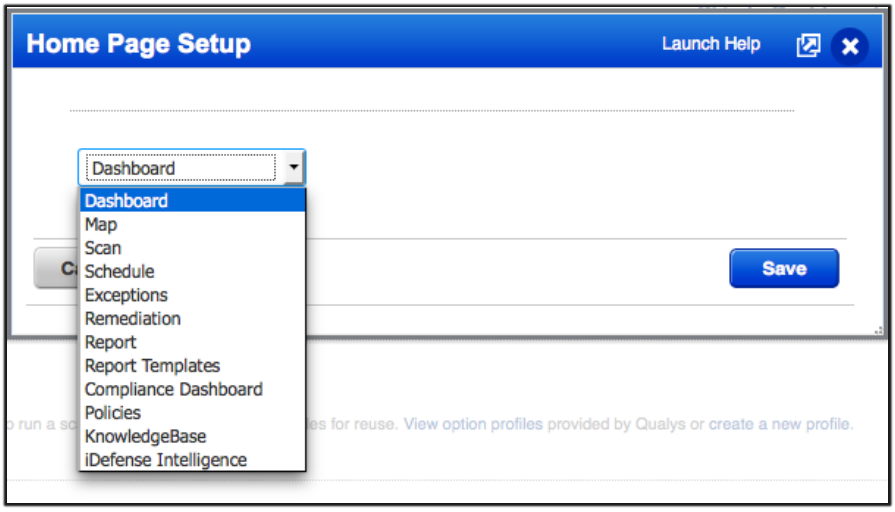


2. **Customize some items on the Dashboard by clicking on the "Configure" link.**

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.

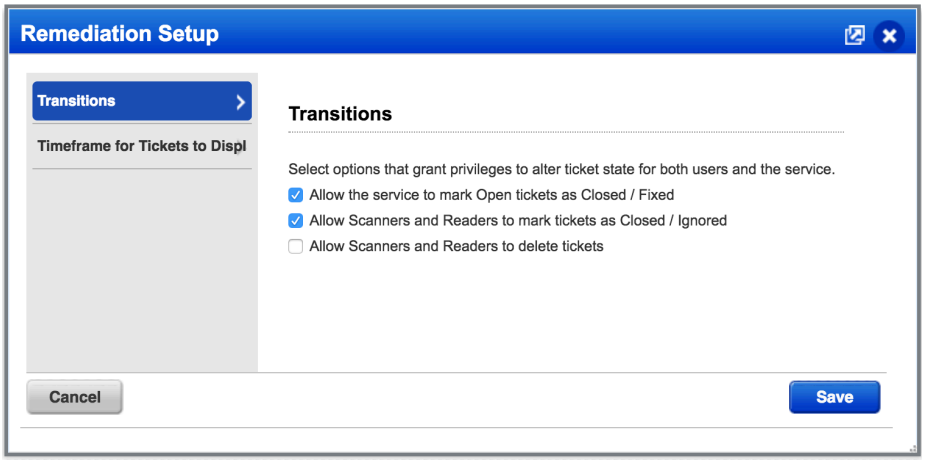
1. **Navigate to the "Setup" tab in the "Scans" section, and click on Excluded Hosts section.**
2. **A new screen will appear.**
3. **Click the "Edit" button.**
4. **Add the IP 64.41.200.243 to the list. Click "Add".**
5. **Add a comment (the Comment field is required).**
6. **Click "Close".**

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.**

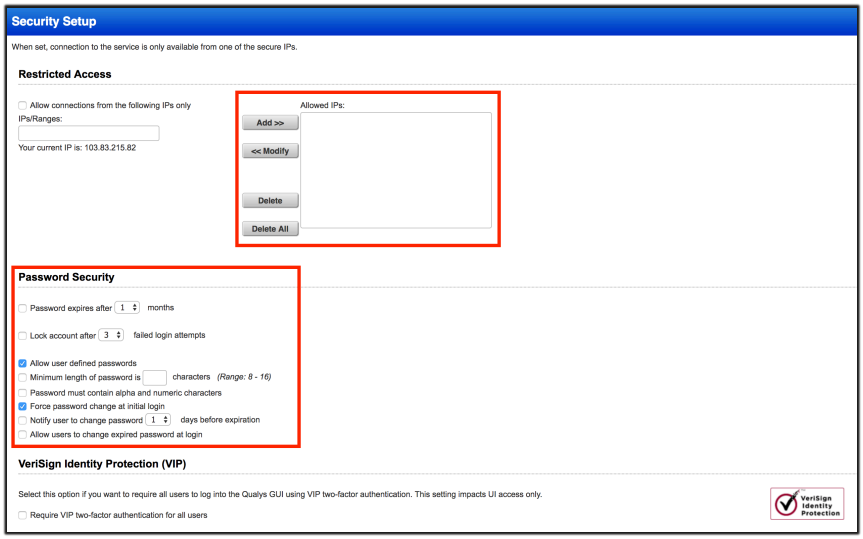
Keep in mind, once you exclude a host, it's a global setting for your subscription, the IPs will be excluded from ALL activity, even though it's still listed in your subscription.

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:

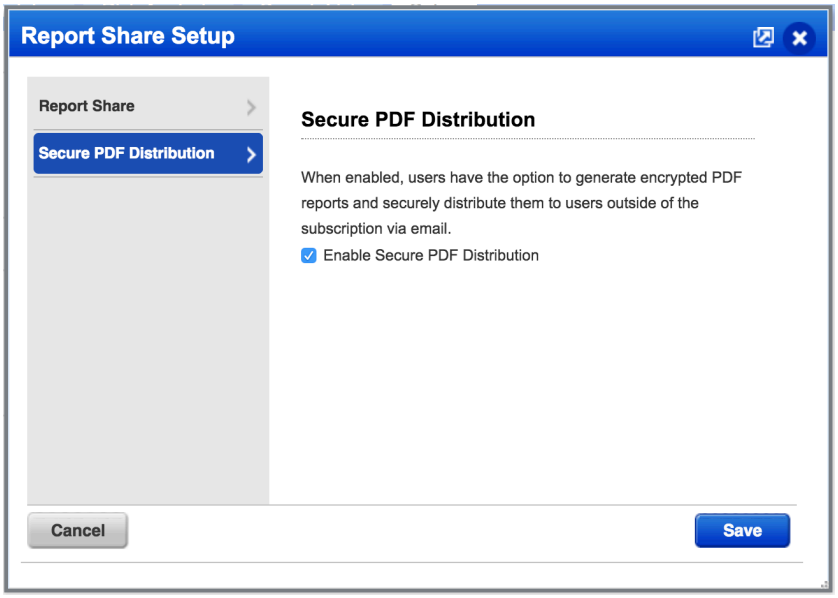


You may want to restrict which IPs have the ability to connect to your QG UI. For this reason, you can restrict access. You can also set password security, even allowing users to set their own passwords.

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".**

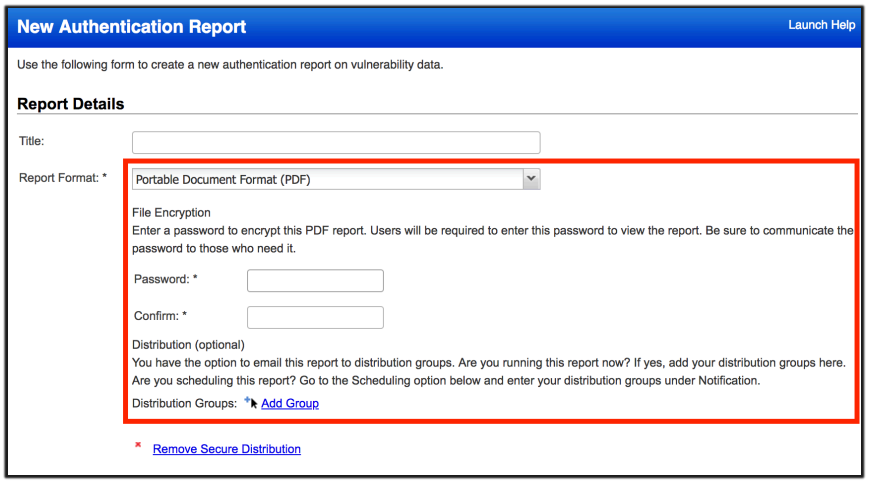
9. **Choose to "Enable Secure PDF Distribution".**



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.**

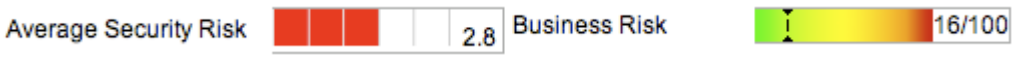


13. **Run the Report.**

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.

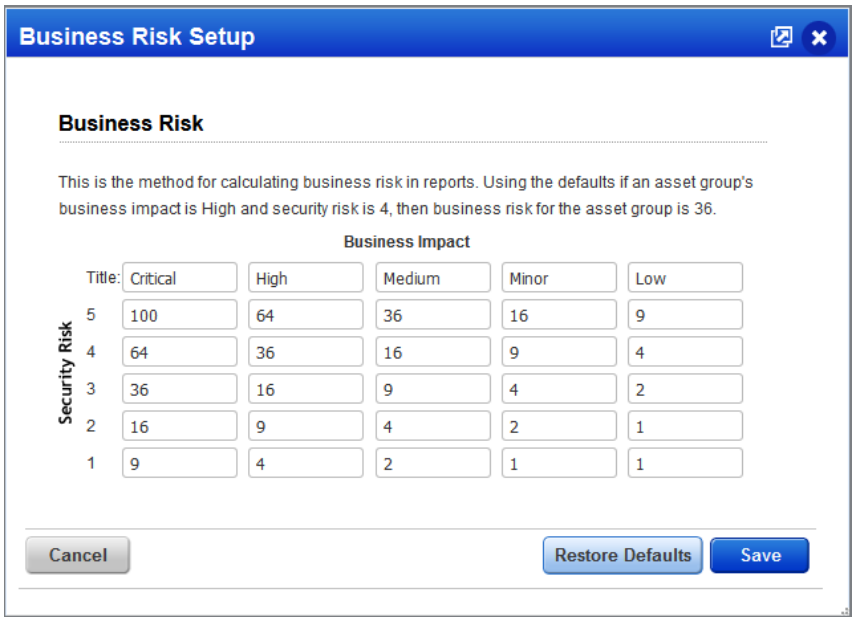
Configuring Business Risk

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.



Security Risk	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

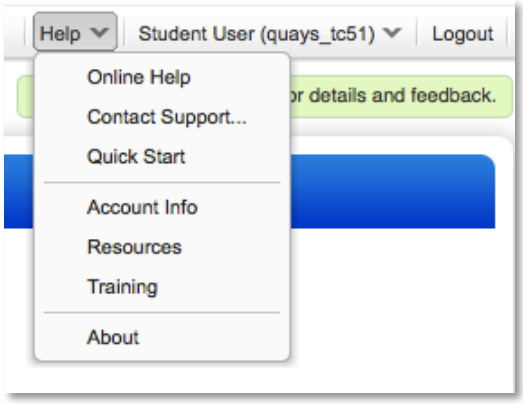
These are the default values for Business Risk. As you can see, a level 5 vulnerability on a host whose Asset Group is of “Critical” importance is weighted 100 times greater than that of a level 1 vulnerability on a host whose asset group is of “Low” importance.

Appendix D: Contacting Support

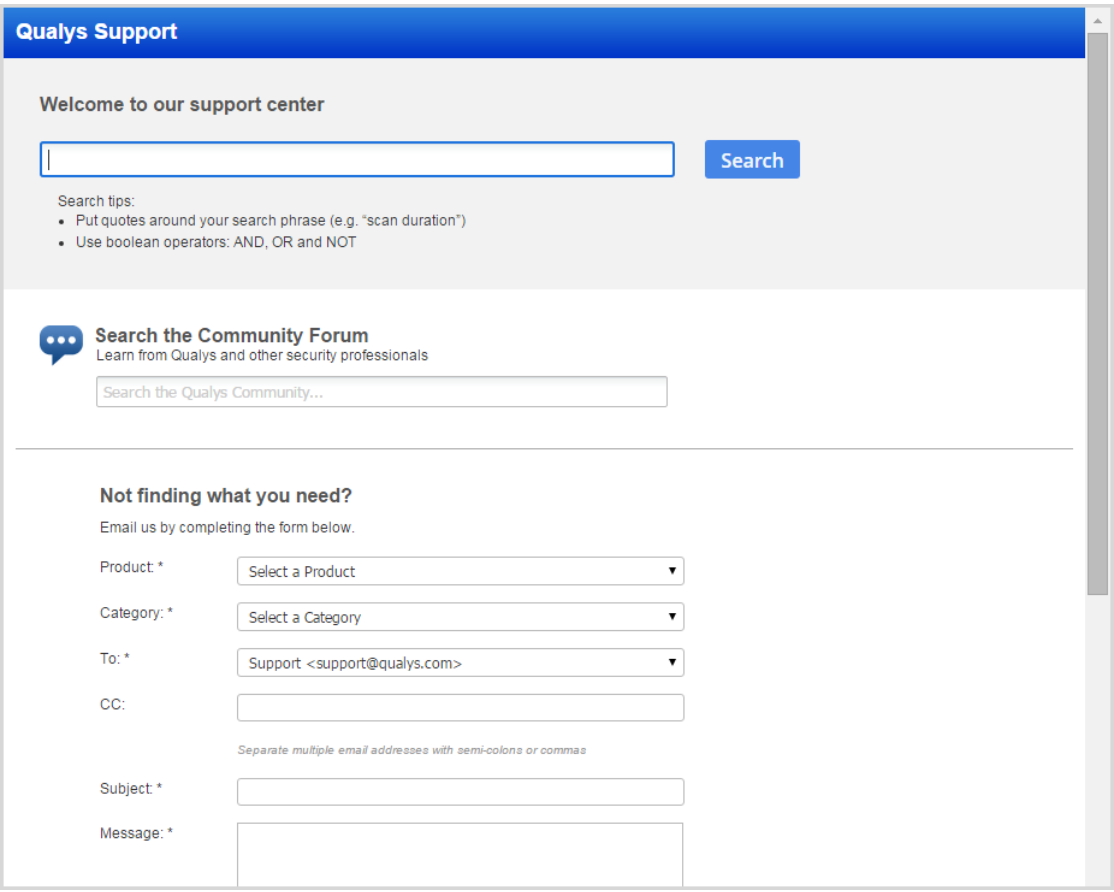
Overview

Try as we may, inevitably you will need to contact support and we support you 24x7.

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.
  - O*n 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.

Appendix E: Qualys Cloud Agent Installation

Qualys Cloud Agent (CA) provides data collection and security services to host assets running supported operating systems.

Because this is a training/learning activity, Qualys recommends performing the CA installation on a "nonessential" lab host used for testing purposes.

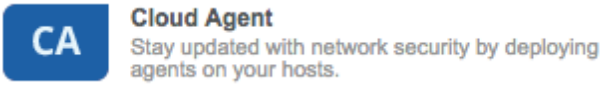
If you elect to install CA on your "everyday" laptop or desktop computer, be sure to uninstall the agent before your student trial account expires.

You must have administrative or root access to your target host to successfully perform the Cloud Agent installation. The target host must have Internet access, and a clear path to the Qualys Cloud Platform.

*** IMPORTANT: Please create or acquire your installation/target host prior to the start of class. Lab time is not provided for this task.*

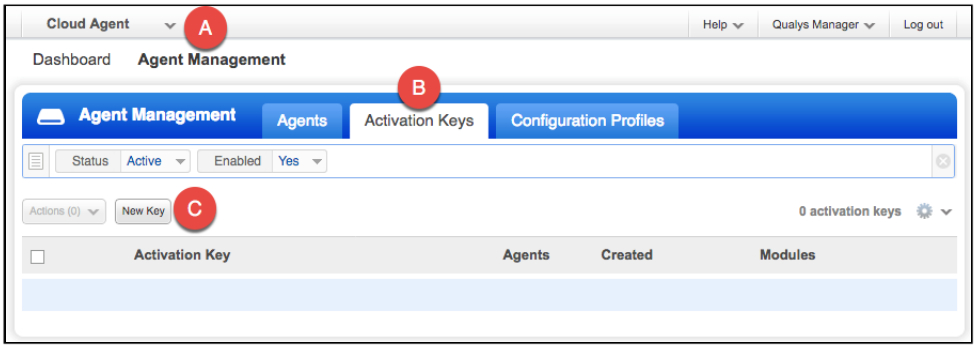
Create Cloud Agent Activation Key

Before you can install Cloud Agent on a target host, you must first generate an activation key. Activation Keys allow you to manage and control the distribution of agents throughout your organization.



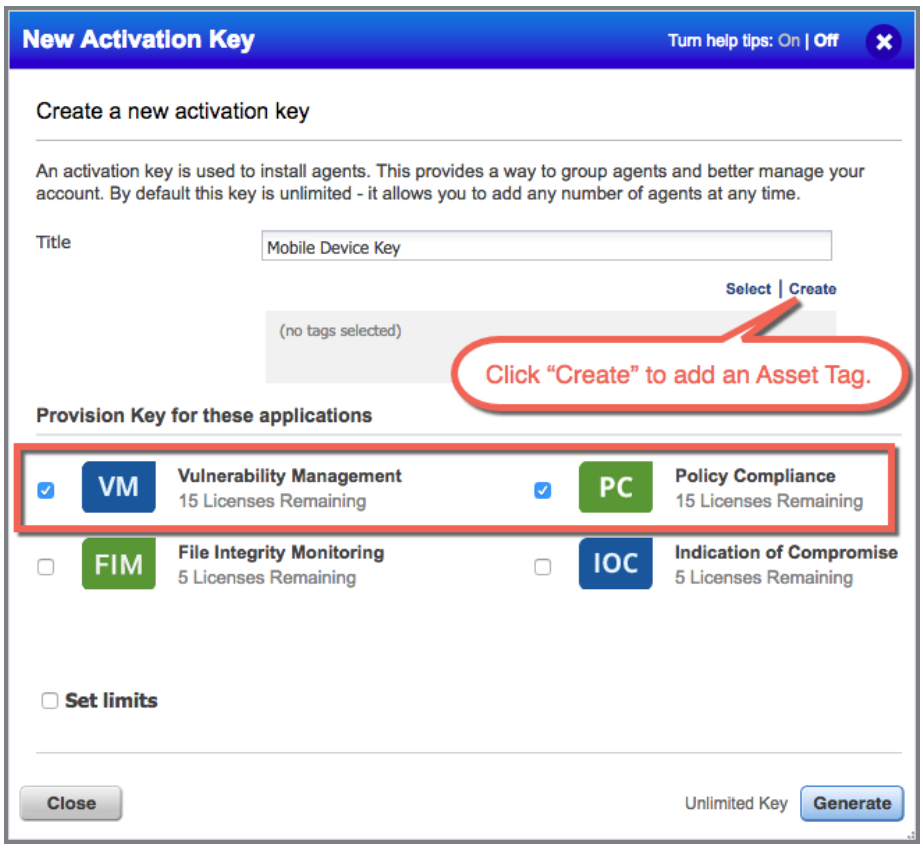
1. **Use the Application drop-down menu to open the Cloud Agent application.**

   The Cloud Agent application is your command and control center for deploying and managing agents.



2. **Click A) the "Agent Management" menu, followed by B) the "Activation Keys" tab, and then click C) the "New Key" button.**

Each activation key will specify: the Qualys application modules supported, Asset Tags assigned to agent hosts, or any activation key limitations.



3. **Give this key the title of "Mobile Device Key".**
4. **Select the check boxes for the VM and PC applications.**

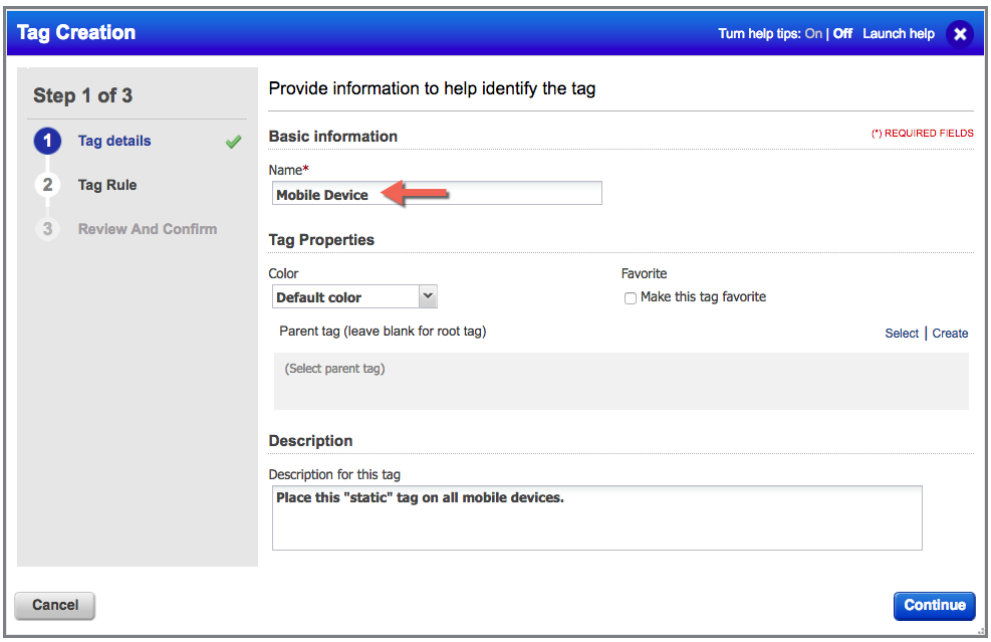
   The FIM and IOC modules will be activated in a later lab exercise.
5. **Do not set any limits on this activation key.**

   Potential limits include:

   - *Maximum number of agents installed (using this key)*
   - *Key expiration date*

   If both limits are selected, the key will expire when the first limit is reached.
6. **Click the "Create" link (just below the Title) to add an Asset Tag to this key.**

The "Tag Creation" wizard will walk you through the steps to create an Asset Tag. Adding an Asset Tag will make it easier to identify agents installed with this key.

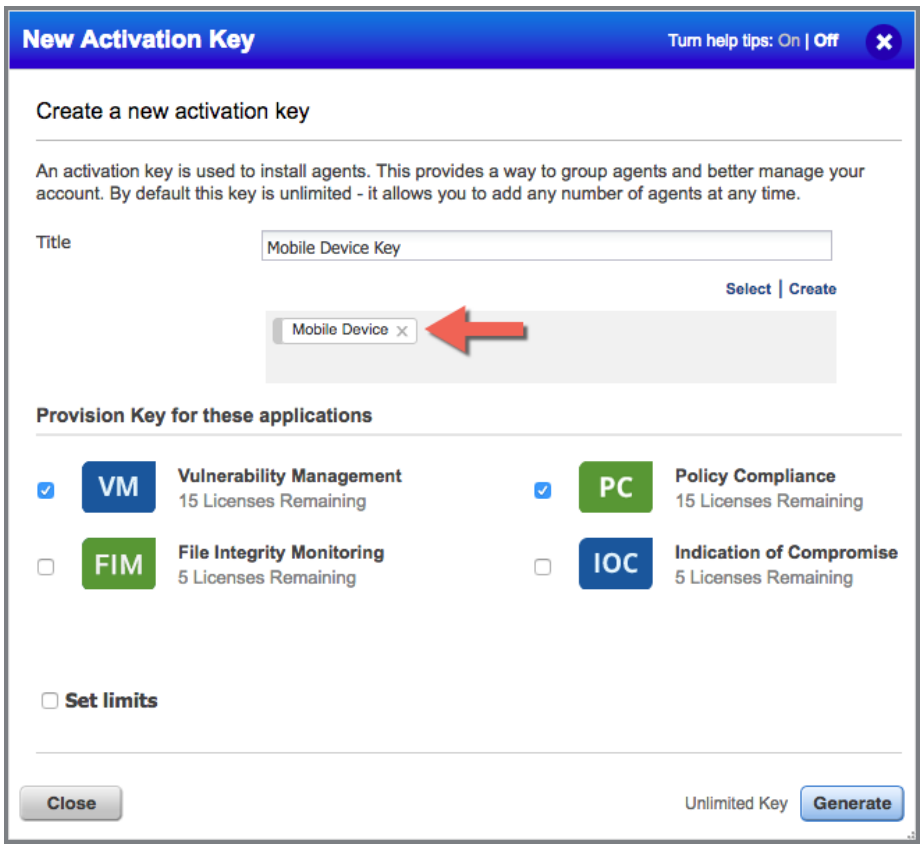


7. **Type "Mobile Device" in the "Name" field and click the "Continue" button.**

8. **Leave the Rule Engine set to the "No Dynamic Rule" option and click the "Continue" button, followed by the "Finish" button.**

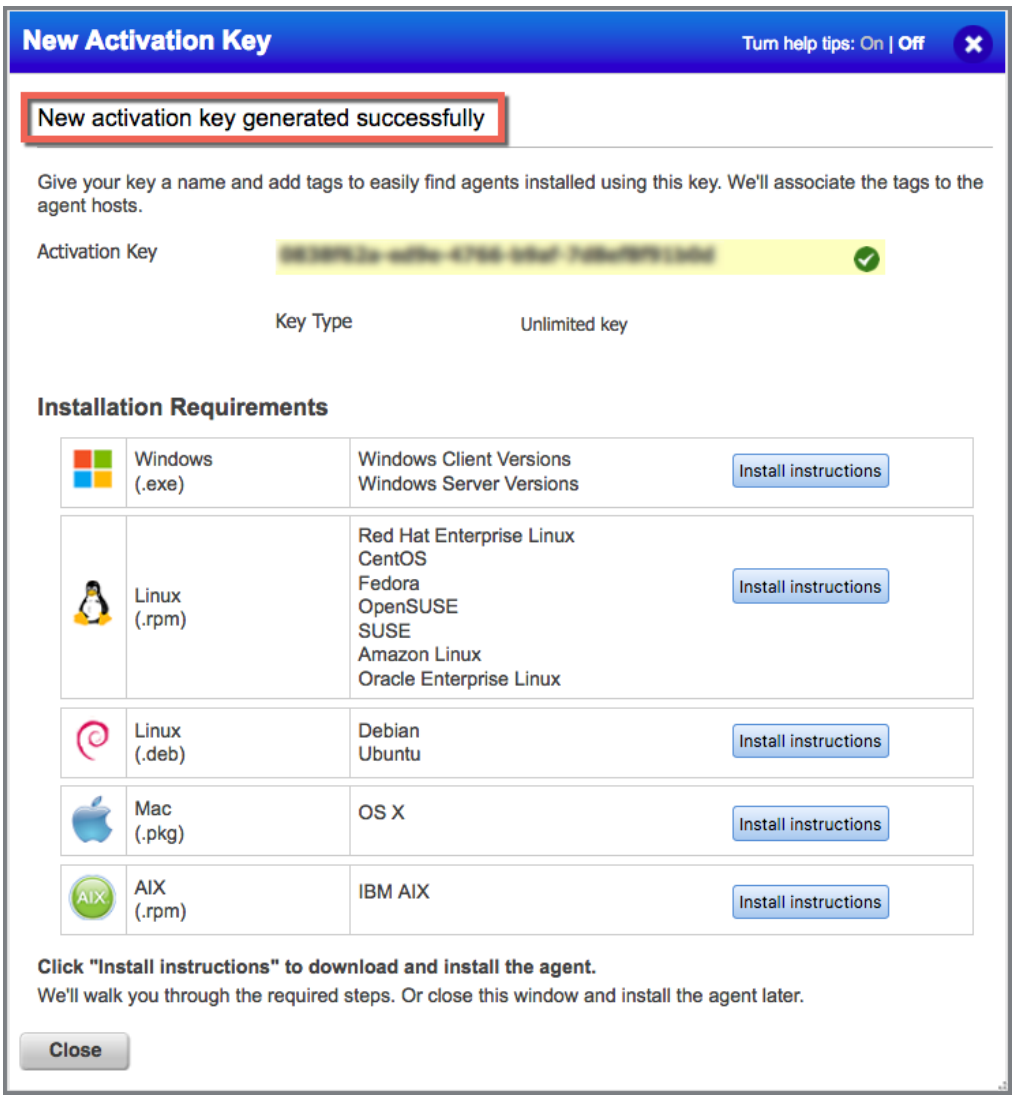
   The "No Dynamic Rule" is used here, because it allows you to control the placement of this Asset Tag (i.e. no random or dynamic behavior).

The "Mobile Device" tag will now be placed on all agent hosts created with this key. You will use this same tag later, to assign agent hosts to their appropriate Configuration Profile.



9. **With the "Mobile Device" tag added to this key, click the "Generate" button.**

Once your activation key is successfully generated, it can be used with any of the supported operating systems.



You can download the agent installation programs or acquire the installation commands anytime; just click the "Install Instructions" button that matches your targeted OS.

10. **For now, click the "Close" button.**

    The exercise steps that follow, provide instructions for a Windows, Mac, or Unix agent installation. A single installation will suffice for this lab (i.e., you do not need to perform more than one installation).

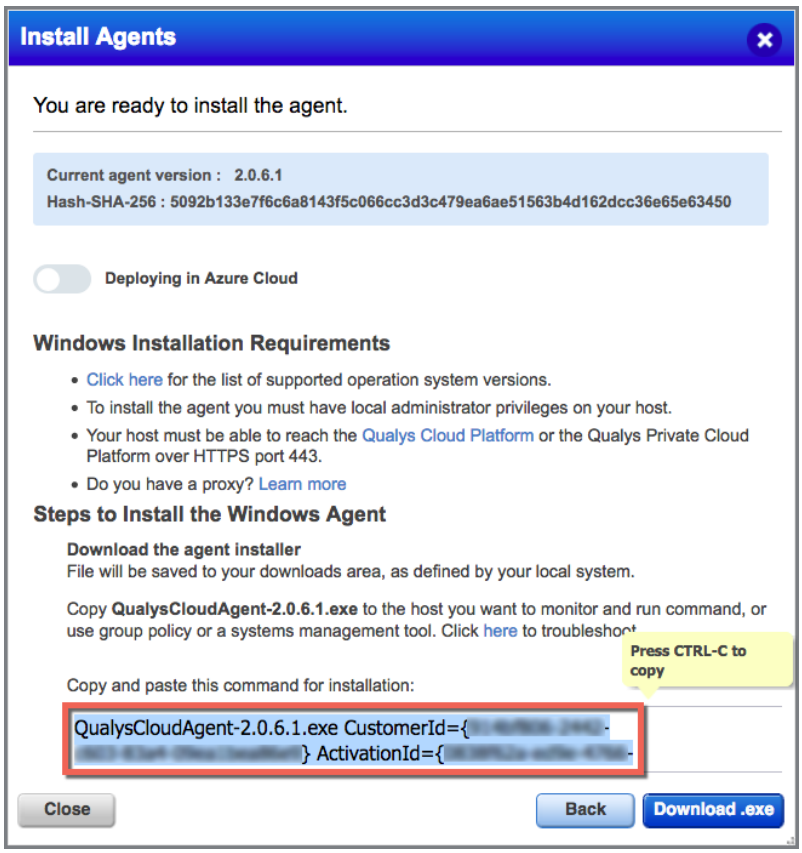
Windows Agent Installation

The installation steps that follow support Windows XP SP3 or greater. If your target host is running a Mac or Unix-based OS, you may skip these steps and proceed to the next "OS Installation" section.

*** IMPORTANT: You must have administrative access to the target Windows host, to successfully perform the Cloud Agent installation steps that follow.*

1. **Open a Web browser (e.g. Edge, IE, Chrome, Firefox, etc...) on the target Windows host and login to your student trial account (`https://qualysguard.qg3.apps.qualys.com/`).**

   If you are installing to a Windows Server, you will typically need to launch "Server Manager" and disable the "IE Enhanced Security Configuration" option for the Local Server.
2. **Open the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**
3. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**
4. **Click the "Install instructions" button for the "Windows (.exe)" option.**



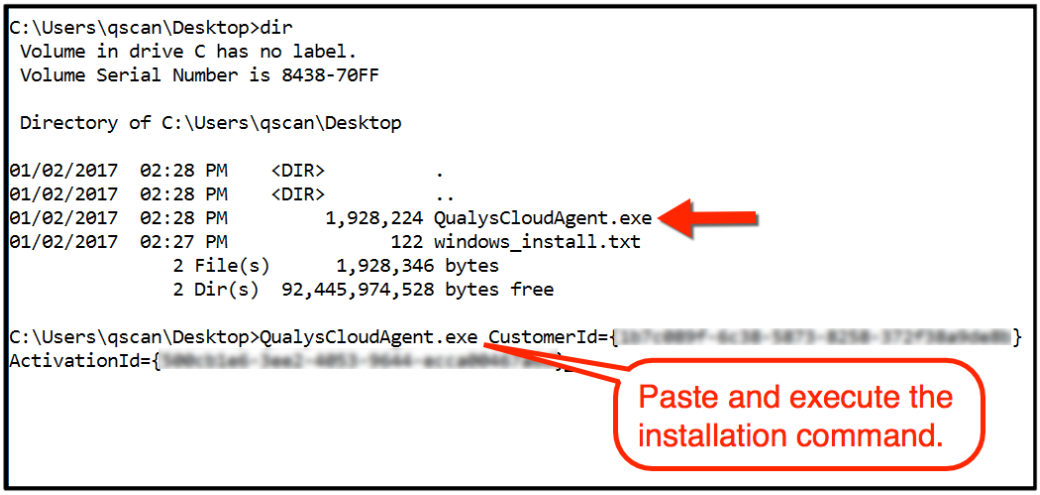
5. **Copy and paste the installation command into a plain text document and save the document as 'windows_install.txt' to the Desktop of your target Windows host.**
6. **Click the "Download .exe file" button and save the Cloud Agent installation file (.exe) to the Desktop of your target Windows host.**
7. **After the download is complete, click the "Close" button.**

   The Desktop of your target Windows host should now contain both files: 1) windows_install.txt and 2) "QualysCloudAgent" installation file (.exe).

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployments.

1. **Open a "Command Prompt" window on the target Windows host.**



2. **Navigate to the Desktop, or the directory that contains the Cloud Agent installation program (QualysCloudAgent.exe).**

3. **Use the "dir" command to verify the existence of the installation program file.**

   If you do not see the "QualysCloudAgent" installation file (.exe) navigate to its correct location before executing the installation command.

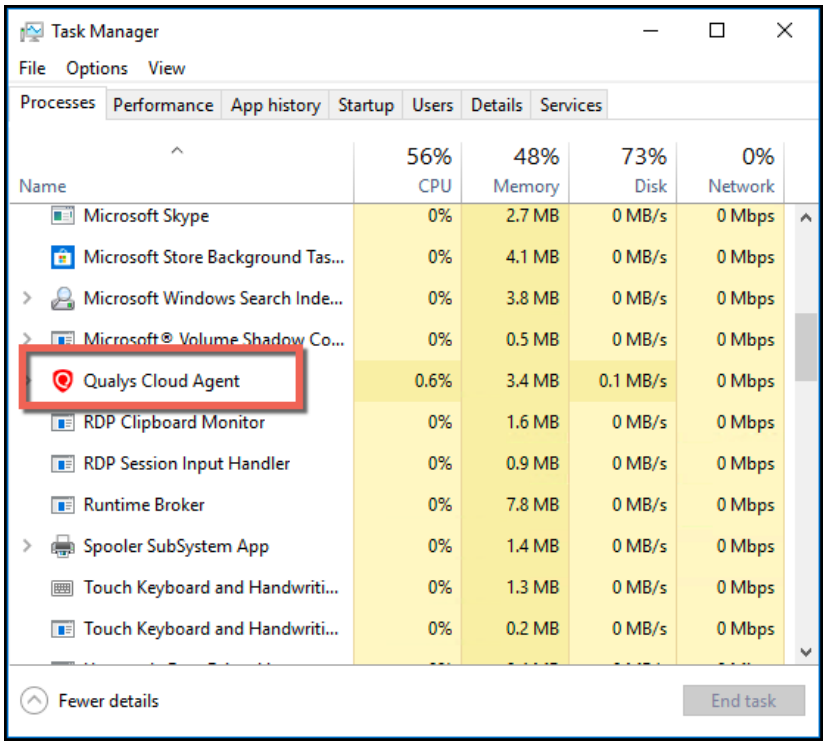
4. **Open the text file that contains your Cloud Agent installation command (i.e., windows_install.txt).**

5. **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.

Validate CA Installation

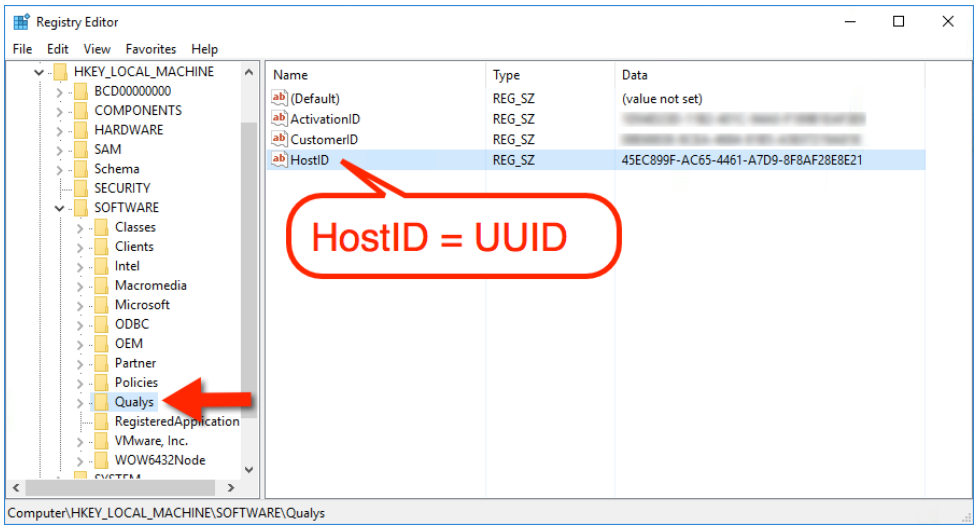
To verify the success of your installation, look for the Cloud Agent process within Windows Task Manager.



1. **Open the Windows Task Manager and verify Qualys Cloud Agent is running (***Ensure you are viewing processes from all users).*
2. **Close the Windows Task Manager.**

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Windows host, this Host ID can be found in the Windows Registry.



3. **From a "Command Prompt" window, open the Windows Registry Editor (i.e., regedit.exe) and navigate to HKLM\SOFTWARE\Qualys.**

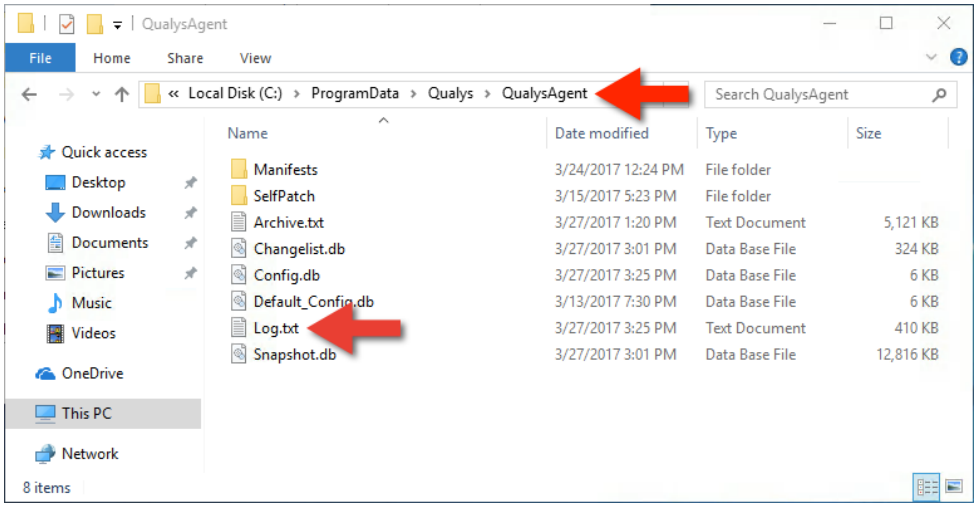
   The value in the "HostID" field will be used to track the vulnerability findings history for this host.

   If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

4. **Close the Windows Registry Editor.**

View CA Log File (Log.txt)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Windows host in the ProgramData (hidden) folder.



5. **Use Windows Explorer or a Command Prompt window to navigate to the following directory path:**

   `C:\ProgramData\Qualys\QualysAgent`

   A Windows host may deny access to the QualysAgent folder. In this event, simply copy of the QualysAgent folder to your Desktop and use the copy to complete the next step.

6. **Use any text editor, such as Notepad, to open and view file Log.txt.**

   **Note: a Windows XP host uses a different directory path for its agent log file:*

   `C:\Documents and Settings\All Users\Application Data\Qualys\QualysAgent`

7. **Once your Cloud Agent installation is complete and successfully validated, return to your original host (and Web browser) to complete the remaining lab exercises.**

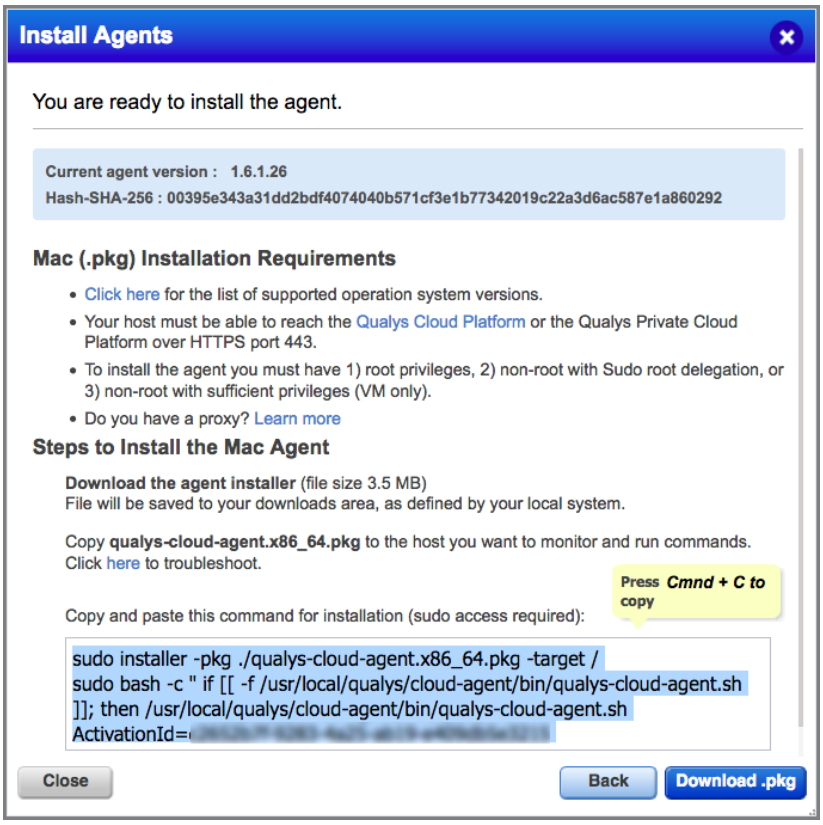
Mac OS Agent Installation

If you have already completed a Windows agent installation, or your target host is running a Unix-based OS, you may skip these steps and proceed to the next section.

The installation steps that follow support Mac OS 10.12 or higher.

*** IMPORTANT: You must have root or root-equivalent access to the target Mac host, to successfully perform the Cloud Agent installation steps that follow.*

1. **Open a Web browser (e.g. Chrome, Firefox, or Safari) on the target Mac host and login to your student trial account (`https://qualysguard.qg3.apps.qualys.com/`).**
2. **Open the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**
3. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**
4. **Click the "Install instructions" button next to the "Mac (.pkg)" option.**



5. **Copy and paste the installation commands into a plain text document and save the document as 'mac_install.txt' to the Desktop of the target Mac host.**

   There are two (2) commands. Each command begins with 'sudo'.

6. **Click the "Download .pkg" button and save the Cloud Agent installation file (.pkg) to the Desktop of your target Mac host.**
7. **After the download is complete, click the "Close" button.**

   The Desktop of your target Mac host should now contain both files: 1) mac_install.txt and 2) "qualys-cloud-agent" installation file(.pkg).

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

The Mac Agent installation file (.pkg) must be installed from a "Terminal" window. Do NOT attempt to install this file using typical Mac GUI techniques.

1. **Open a "Terminal" window on the target Mac host.**
2. **Navigate to the Desktop, or the directory that contains the Cloud Agent installation file (.pkg).**

```
Air:desktop$ ls -la
total 8352
drwx------+   8      256 Aug  6 15:21 .
drwxr-xr-x+  34     1088 May 10 14:32 ..
-rw-r--r--@   1      487 Aug  6 15:11 mac_install.txt
-rw-r--r--@   1  3241714 Aug  6 15:12 qualys-cloud-agent.x86_64.pkg
```

3. **Use the "ls" command to verify the existence of the installation package.**

   If you do not see the "qualys-cloud-agent" installation file (.pkg) navigate to its correct location before executing the installation command.

4. **Open the text file that contains your Cloud Agent installation commands (i.e., mac_install.txt).**
5. **Copy and paste only the first "sudo" command of this file into the "Terminal" window and press the "Enter" key.**

   This first command unpacks and installs the Cloud Agent package.

6. **When the first command has completed, copy and paste the remainder of the mac_install.txt file (i.e., the second "sudo" command) into the "Terminal" window, and press the "Enter" key.**

   This second command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

1. **Use the "ps –e" command, to verify 'qualys-cloud-agent' is running.**

```
ps -e | grep qualys
```

```
macBook:desktop$ ps -e | grep qualys
 1237 ??         /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent
 1259 ttys000  0 grep qualys
```

Locate Host ID

All agent host assets are automatically assigned a Qualys Host ID (UUID). For a Mac host, this Host ID can be found at /etc/qualys/hostid.

2. **From a Terminal window, execute the following command:**

```
sudo cat /etc/qualys/hostid
```

If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Mac host in the /var/log/qualys directory.

3. **From a Terminal window, execute the following command:**

   ```
   sudo cat /var/log/qualys/qualys-cloud-agent.log
   ```

4. Once your Cloud Agent installation is complete and successfully validated, return to your original host (and Web browser) to complete the remaining lab exercises.

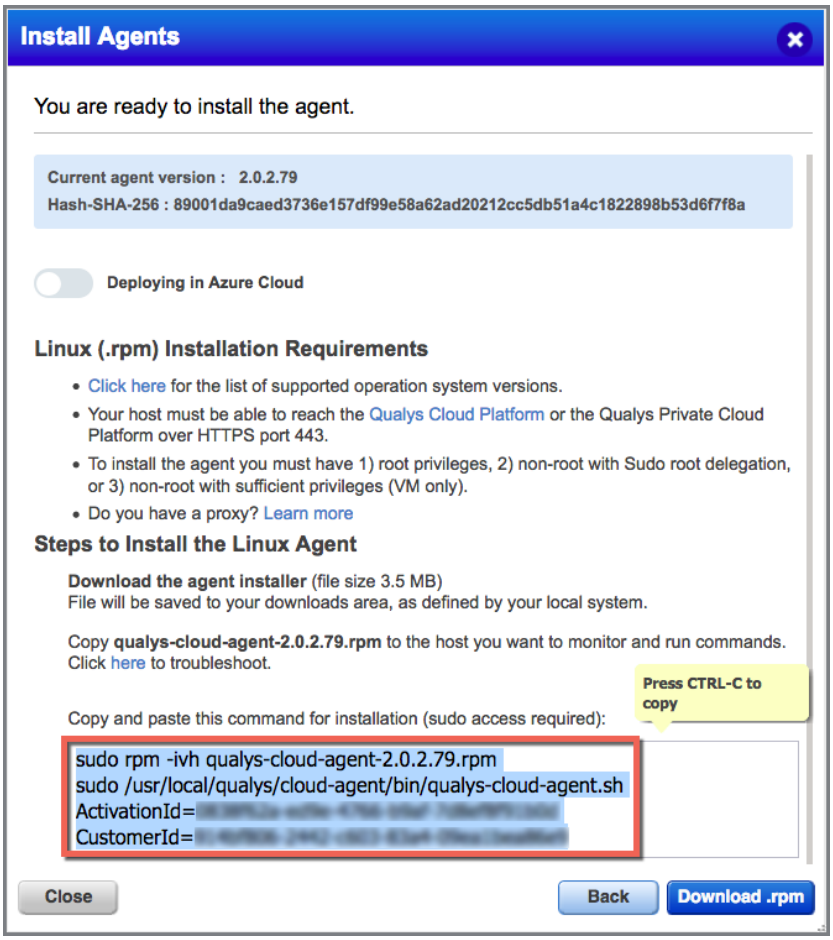
RPM-Based Agent Installation

If you have already completed a Windows or Mac OS agent installation, or your target host is running Debian or Ubuntu OS, you may skip these steps and proceed to the next section.

RPM-based Linux operating systems include: Red Hat Enterprise Linux, CentOS, Fedora, OpenSuSE, SuSE, Amazon Linux, and Oracle Enterprise Linux.

*** IMPORTANT: You must have root or root-equivalent access to the target host, to successfully perform the Cloud Agent installation steps that follow.*

1. **Open a Web browser (e.g. Chrome or Firefox) on the target UNIX host and login to your student trial account (`https://qualysguard.qg3.apps.qualys.com/`).**
2. **Open the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**
3. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**
4. **Click the "Install instructions" button next to the "Linux (.rpm)" option.**



5. **Copy and paste the installation commands into a plain text document and save the document as 'unix_install.txt' to the Desktop of the target Unix host.**

   There are two (2) commands. Each command begins with 'sudo'.

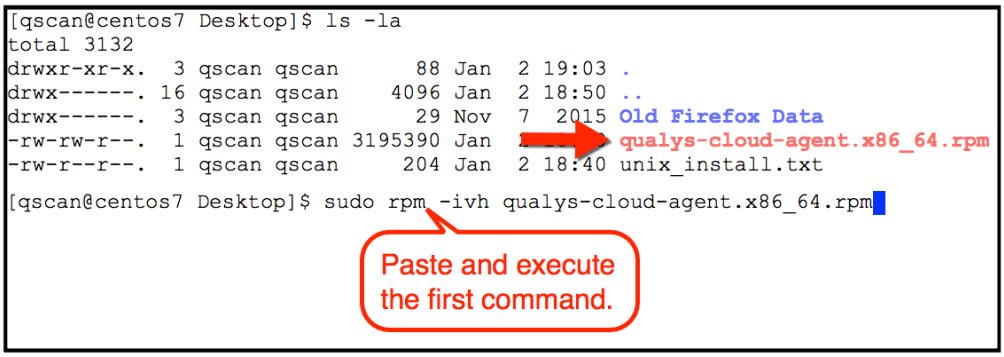
6. **Click the "Download. rpm file" button and save the Cloud Agent installation file (.rpm) to the Desktop of your target Unix host.**
7. **After the download is complete, click the "Close" button.**

   The Desktop of your target Unix host should now contain both files: 1) unix_install.txt and 2) "qualys-cloud-agent" installation file (.rpm).

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

7. **Open a "Terminal" window on the target Unix host.**
8. **Navigate to the Desktop, or the directory that contains the Cloud Agent installation file (.rpm).**



9. **Use the "ls" command to verify the existence of the installation file.**

   If you do not see the "qualys-cloud-agent" installation file (.rpm) navigate to its correct location before executing the installation command.

10. **Open the text file that contains your Cloud Agent installation commands (i.e., unix_install.txt).**
11. **Copy and paste only the first command line of this file into the "Terminal" window and press the "Enter" key.**

    This first command unpacks and installs the Cloud Agent package.

12. **When the first command has completed, copy and paste the remainder of the unix_install.txt file (i.e., the second command) into the "Terminal" window, and press the "Enter" key.**

    This second command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

```
 6972 tty7     00:00:00 Xorg
 6984 ?
 6985 ?
 6987 ?
 6988 pts/1    00:00:00 bash
 8404 pts/2    00:00:00 qualys-cloud-ag
 8420 pts/1    00:00:00 ps
24375 ?        00:00:14 java
26814 ?        00:00:00 httpd
```

Type "ps -e" from the command line.

5. **Use the "ps –e" command, to verify 'qualys-cloud-ag' is running.**

```
ps -e | grep qualys
```

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Unix host, this Host ID can be found at /etc/qualys/hostid.

6. **From a Terminal window, execute the following command:**

```
sudo cat /etc/qualys/hostid
```

If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Unix host in the /var/log/qualys directory.

7. **From a Terminal window, execute the following command:**

```
sudo cat /var/log/qualys/qualys-cloud-agent.log
```

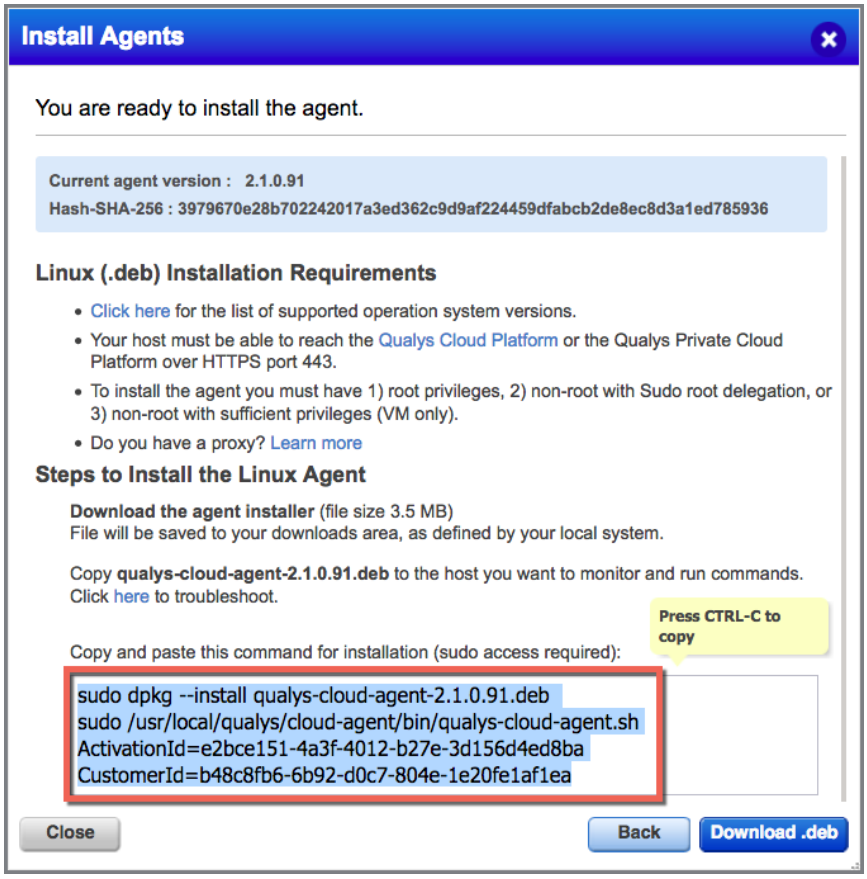
8. **Once your Cloud Agent installation is complete and successfully validated, return to your original host (and Web browser) to complete the remaining lab exercises.**

Debian or Ubuntu Agent Installation

If you have already completed a Windows, Mac OS, or RPM-Based Linux agent installation, you do not need to perform these installation steps and may proceed to the next section.

*** IMPORTANT: You must have root or root-equivalent access to the target host, to successfully perform the Cloud Agent installation steps that follow.*

1. **Open a Web browser (e.g. Chrome or Firefox) on the target UNIX host and login to your student trial account (`https://qualysguard.qg3.apps.qualys.com/`).**
2. **Open the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**
3. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**
4. **Click the "Install instructions" button next to the "Linux (.deb)" option.**



5. **Copy and paste the installation commands into a plain text document and save the document as 'unix_install.txt' to the Desktop of the target Unix host.**

   There are two (2) commands. Each command begins with 'sudo'.

6. **Click the "Download. deb file" button and save the Cloud Agent installation file (.deb) to the Desktop of your target Unix host.**
7. **After the download is complete, click the "Close" button.**

   The Desktop of your target Unix host should now contain both files: 1) unix_install.txt and 2) "qualys-cloud-agent" installation file (.deb).

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

13. **Open a "Terminal" window on the target Unix host.**
14. **Navigate to the Desktop, or the directory that contains the Cloud Agent installation file (.deb).**

```
ubuntu@ec2-ubu1604:~$ ls -la
total 4000
drwxr-xr-x 4 ubuntu ubuntu    4096 Aug 29 15:12 .
drwxr-xr-x 5 root   root      4096 Aug  9 14:40 ..
-rw------- 1 ubuntu ubuntu    2801 Aug 29 15:17 .bash_history
-rw-r--r-- 1 ubuntu ubuntu     220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu    3771 Aug 31  2015 .bashrc
drwx------ 2 ubuntu ubuntu    4096 Aug  7 21:39 .cache
-rw-r--r-- 1 ubuntu ubuntu     655 May 16  2017 .profile
-rw-r--r-- 1 ubuntu ubuntu 4058210 Aug  7 [illegible] qualys-cloud-agent-2.0.2.79.deb
drwx------ 2 ubuntu ubuntu    4096 Aug  7 21:28 .ssh
-rw-r--r-- 1 ubuntu ubuntu       0 Aug  7 21:41 .sudo_as_admin_successful
-rw------- 1 root   root      2935 Aug 29 15:12 .viminfo
ubuntu@ec2-ubu1604:~$
```

15. **Use the "ls" command to verify the existence of the installation file.**

    If you do not see the "qualys-cloud-agent" installation file (.deb) navigate to its correct location before executing the installation command.

16. **Open the text file that contains your Cloud Agent installation commands (i.e., unix_install.txt).**
17. **Copy and paste only the first command line of this file into the "Terminal" window and press the "Enter" key.**

    This first command unpacks and installs the Cloud Agent package.

18. **When the first command has completed, copy and paste the remainder of the unix_install.txt file (i.e., the second command) into the "Terminal" window, and press the "Enter" key.**

    This second command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

```
 6972 tty7     00:00:00 Xorg
 6984 ?
 6985 ?
 6987 ?
 6988 pts/1    00:00:00 bash
 8404 pts/2    00:00:00 qualys-cloud-ag
 8420 pts/1    00:00:00 ps
24375 ?        00:00:14 java
26814 ?        00:00:00 httpd
```

Type "ps -e" from the command line.

9. **Use the "ps –e" command, to verify 'qualys-cloud-ag' is running.**

```
ps -e | grep qualys
```

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Unix host, this Host ID can be found at /etc/qualys/hostid.

10. **From a Terminal window, execute the following command:**

    ```
    sudo cat /etc/qualys/hostid
    ```

    If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Unix host in the /var/log/qualys directory.

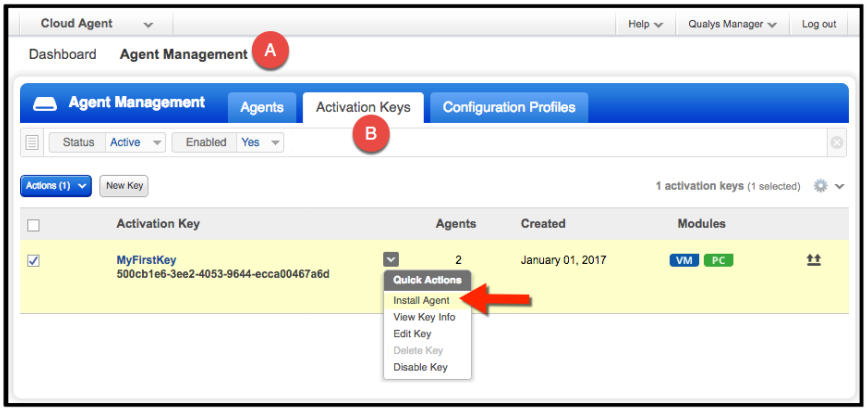
11. **From a Terminal window, execute the following command:**

    ```
    sudo cat /var/log/qualys/qualys-cloud-agent.log
    ```

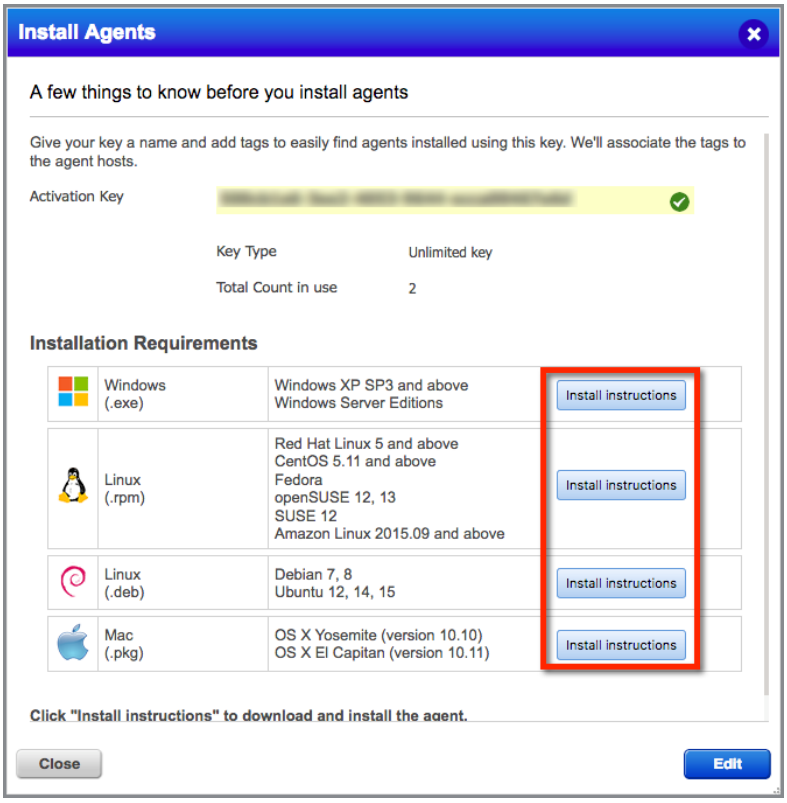
12. **Once your Cloud Agent installation is complete and successfully validated, return to your original host (and Web browser) to complete the remaining lab exercises.**

CA Install Programs and Scripts

You can always return to the “Activation Keys” tab, to retrieve CA installation programs and scripts.



1. **From the Cloud Agent application, navigate to A) the “Agent Management” section, and click B) the “Activation Keys” tab.**
2. **Use the “Quick Actions” menu for any activation key and select the “Install Agents” option.**

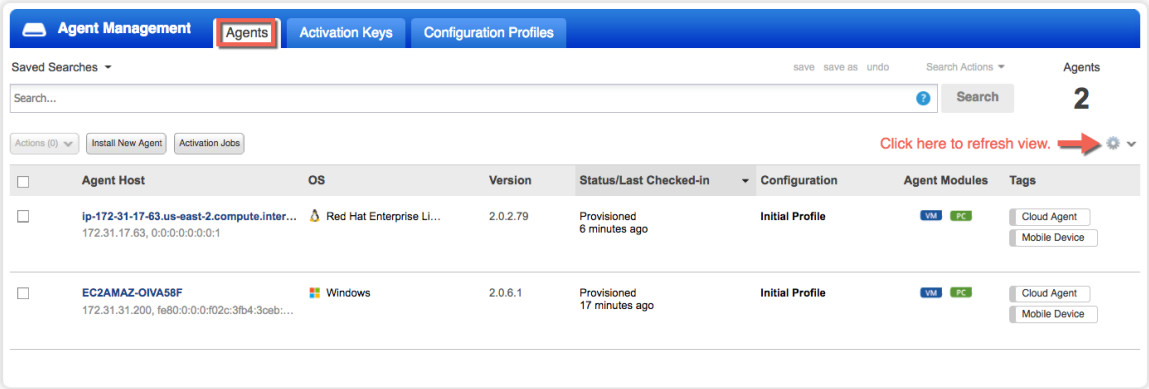


3. **Click any “Install instructions” button to reproduce an installation script or download an installation program, and then click the “Close” button.**

Cloud Agent Inventory

At this point, you may return to your original host (and Web browser), if you installed Cloud agent on a separate host.

It typically takes a few minutes for a new Agent Host to appear under the “Agents” tab.



1. **Click the “Widget” icon in the upper-right corner to refresh your view.**

   In addition to the “Mobile Device” tag created by your Activation Key, a “Cloud Agent” Asset Tag is automatically placed on your agent host.

   Additional objects and indicators will be added, as your newly installed agent continues to work through its initial manifest.