Qualys Cloud Platform

Evaluator's Guide

December 26, 2022

Copyright 2011-2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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

Table of Contents

Getting Started 4

Key Features of the UI 4
Account Setup 6
Installing Your Scanner Appliance 6
Creating Network Domains 6
Adding Hosts for Scanning 6
Controlling Access to Assets 7
User Management 8
Controlling User Access to Apps 13
You're Now Ready 14

Mapping Your Network 15

Running a Map 15
Map Results 16
Scheduling Maps 18
Map Targets 19
Mapping Summary 19

Scanning for Vulnerabilities 20

Starting a Scan 21
Scan Status 23
Scan Results 24
Scheduling Scans 27
Scanner Parallelization 28
Selective Scanning using Search Lists 28
PCI Scans and Compliance 29
Vulnerability KnowledgeBase 32
Scanning Summary 33

Search, View, Prioritize 34

View Your Dashboard 34
View Asset and Vulnerability Details 36
Run a Prioritization Report 38

Reporting and Remediation 39

Launching Reports 39
Accessing Reports 40
Sharing Reports 41
Scheduling Reports 41
Trend Analysis and Differential Reporting 44
Scorecard Reports 49

Patch Reports 51
Reporting Summary 52
Remediation Summary 52

Wait, there's more! 53

Policy Compliance 53
Add Cloud Agents 54
Get Real-Time Security Alerts 55
Scan Your Web Apps and APIs for Vulnerabilities 56

Support and Training 57

Contact Support 57
Free Training and Certification 57
Our Online Community 57
Looking for user guides? 57
New Feature Announcements and Platform Status 57

Dear Evaluator,

First, thank you for taking the time to evaluate Qualys Cloud Platform, an integrated suite of security and compliance applications. Today you must do everything to protect your network from the myriad of new threats, discovered almost every day, and meet compliance. Although you need to fully evaluate a solution for your enterprise time is not on your side. You need a solution now and your risk increases every day you wait. We have produced this *Evaluator's Guide* to help you use your time more efficiently.

Toward that end, we had several objectives for this document. One was for it to be reasonably concise. In addition, it had to be structured to enable you to apply the primary functions – mapping, scanning, reporting, remediation, and policy compliance – while offering you the option to explore deeper into sub-functions.

The *Evaluator's Guide* helps you test the product highlights without limiting your options. We urge you to apply Qualys to a network of your choice. That is the only way to get a true sense of its capabilities. For demonstration purposes, Qualys has an Internet facing network with a handful of IP addresses that you may want to scan first before scanning your chosen network. Please feel free to do that. We will be happy to provide you with the current IP addresses.

At various steps in the *Evaluator's Guide*, you will see procedures and screen shots designed to simplify every aspect from authentication to remediation. Also there will be references to sections in the online help, which is available from every location in the user interface, for more details.

One of the biggest hurdles in using an enterprise information security management solution is the installation and deployment. With Qualys, this is eliminated. You interact with the solution using a Web browser that allows you to log onto Qualys to start the mapping, scanning, reporting, remediation, and policy compliance processes.

Should you have any questions during this process please contact your Qualys representative or Qualys Support at www.qualys.com/support/.

Again, thank you for evaluating the Qualys Cloud Platform.

Sincerely,

Qualys, Inc.

Getting Started

All of your interactions with the Qualys solution will be through the Secure Internet Interface. After registration for the trial, you will receive an email with a secure link to a user name and password and login URL. This is a one-time-only link. Once you have connected to the Web page, neither you nor anyone else can do so a second time. This protects you in the event someone intercepts your email. Your login is fixed and assigned by Qualys. Your password is a randomly generated "strong" password to begin and you may change it at any time.

To log in to the Qualys user interface, go to your account registration email and click the login URL link.

Key Features of the UI

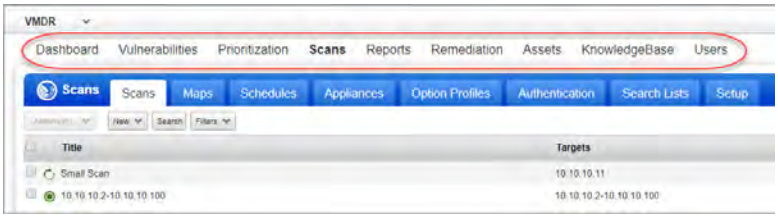
Let's take a quick look at the Qualys user interface and some of its key features.

Security and Compliance Suite

Our integrated suite of solutions is presented in a single view. Simply choose the solution you're interested in from the module picker and get started right away. See an example of the picker to the right.

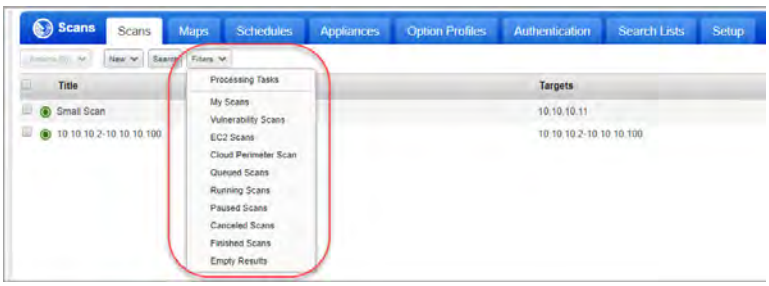
Easy Navigation

Once you've selected the application you want, you'll see menu options across the top of the screen representing the main sections of the application. Each section provides workflows specific to the application.



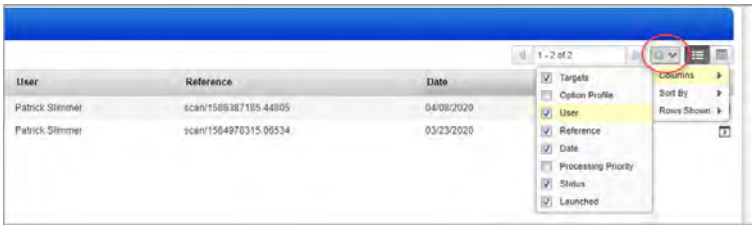
Interactive Filters with Visual Feedback

Use filters to change your data list view.



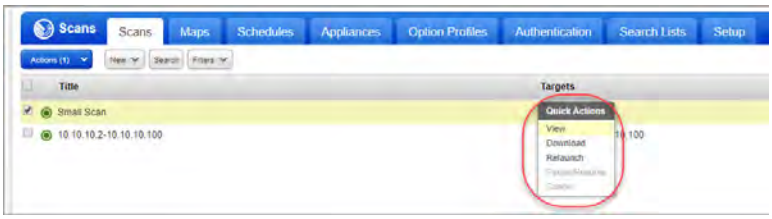
Customize Your View

You can hide columns, change the sorting criteria and specify the number of rows to appear in each list. To do so, use the Tools menu above the list, on the right side.



Actionable Menus

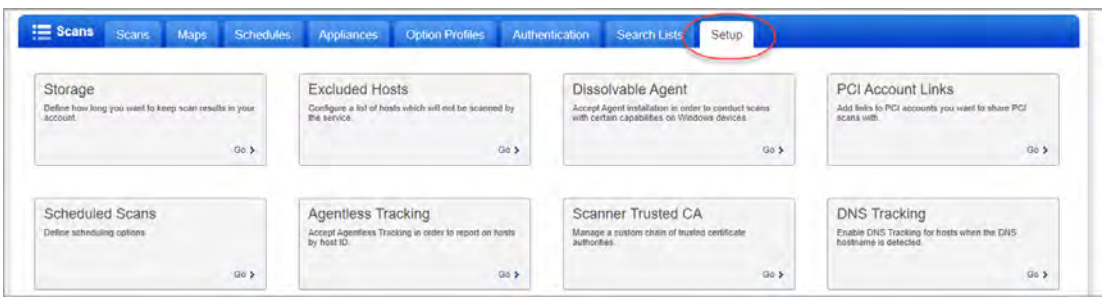
Take actions on a single item using the Quick Actions menu. Place your mouse cursor over the data list row to see the drop-down arrow. Then click the arrow to see the possible actions you can take. For example, view or download scan results for a finished scan.



Take actions on multiple items in a data list. Select the check box for each item in the data list your action applies to and then select an action from the Actions menu above the list. You'll notice that the Actions button displays the number of items that you've selected.

Contextual Setup

Setup options are available where you need them. For example, setup options affecting scans and scan results appear on the Setup tab in the Scans section. This means you don't have to leave the Scans section to setup your configurations or set global scan options. The setup options available to you depend on your service level and subscription settings. The ability to edit setup options is determined by your role and permissions.



Account Setup

Now that you're familiar with the user interface, let's perform a few key tasks to setup your account. You'll need to install your scanner appliance, add domains for mapping, and add hosts (IP addresses) for scanning. We'll also look at how you can organize your assets and users.

Installing Your Scanner Appliance

By installing a scanner appliance within your network, you will have the ability to do vulnerability assessments for your entire network. We offer both physical appliances and virtual appliances for ease of integration with your network environment. The scanner appliance features a hardened OS kernel, is highly secure, and stores no data. It's recommended best practice that you create dedicated user accounts for installing scanner appliances, so that changes in account status do not affect scanner appliance availability. For the purpose of this review, you will simply install your scanner appliance using the same login and password you are currently using. Go to VM/VMDR > Scans > Appliances to set up a 14 day trial of Qualys Virtual Scanner.

Creating Network Domains

Qualys uses a domains concept for its network mapping process. "Domain" in this context is our name for a DNS entry, for a netblock, or for a combination.

To create such a domain, you select "Assets" on the top menu and then select the "Domains" tab. Go to New > Domains. Here you will specify a domain or a netblock of IPs. Once you have typed them into the New Domains pop-up, click "Add". A notice will appear reminding you that you must have permission to discover (map) the specified domains and netblocks. Click "OK". You will be returned to the domains list, and the added domains will now be shown.

When specifying domains, you may add existing registered domain names recognizable by DNS servers on your network, such as "mycompany.com". Also you have the option to add a domain called "none" with netblocks (one or more IP addresses and IP ranges).

Qualys provides a demo domain called "qualys-test.com" for network mapping. This domain may already be in your account. If not you can add it yourself. Note that the devices in the demo domain reside in Qualys Security Operations Centers, so the Qualys Internet scanners can be used for mapping this domain.

Adding Hosts for Scanning

The service supports network scanning and compliance scanning. Host assets are the IP addresses in your account that may be used as scan targets.

In preparation for network scanning, you need to tell us which IP addresses and/or ranges you wish to scan. Select "Assets" on the top menu and then select the "Host Assets" tab. Go to New > IP Tracked Hosts.

The New Hosts page will appear. In the section titled "Host IPs" enter the IPs for which you have permission to scan. You'll see the check box "Add to Policy Compliance Module" if the compliance module is enabled for your subscription. Select this check box if you want the new IPs to also be available for compliance scanning. At the bottom of the page, click the "Add" button. A notice appears asking you to verify that you are authorized to scan the IP addresses being added. Select "OK." The host assets list will now return to your display, and the newly added hosts will be added to the list.

How can I discover hosts?

You can discover the devices on your network starting from a domain or netblock. Then add the IPs to your account using the workflow from the Map Results report.

Tell me about tracking hosts by DNS and NetBIOS.

You'll notice that you have the option to add hosts tracked by DNS and NetBIOS hostname, which allows for reporting host scan results in dynamic networking environments. For example, you may want to use DNS or NetBIOS hostname tracking if the hosts on your network are assigned IP addresses dynamically through DHCP.

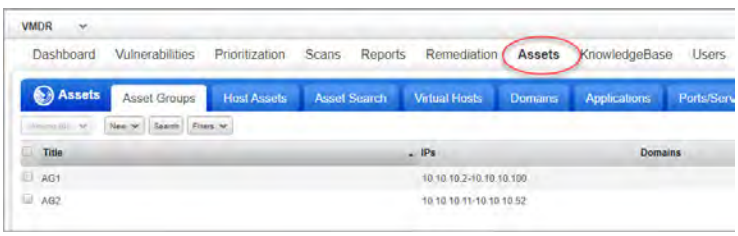
Tell me about support for virtual hosts.

A virtual host is a single machine that acts like multiple systems, hosting more than one domain. For example, an ISP could use one server with IP address 194.55.109.1 to host two Web sites on the same port: www.merchantA.com and www.merchantB.com. To ensure that the scanning service analyzes all domains when the host is scanned, set up a virtual host configuration for this IP address and specify the port and fully-qualified domain names. Select the "Virtual Hosts" tab under "Assets". Then go to New > Virtual Host to create a new virtual host configuration.

Controlling Access to Assets

You can control user access to assets (scanner appliances, domains and hosts) by organizing them into user-defined asset groups and then assigning these groups to users. This is how you limit users to certain assets in the subscription.

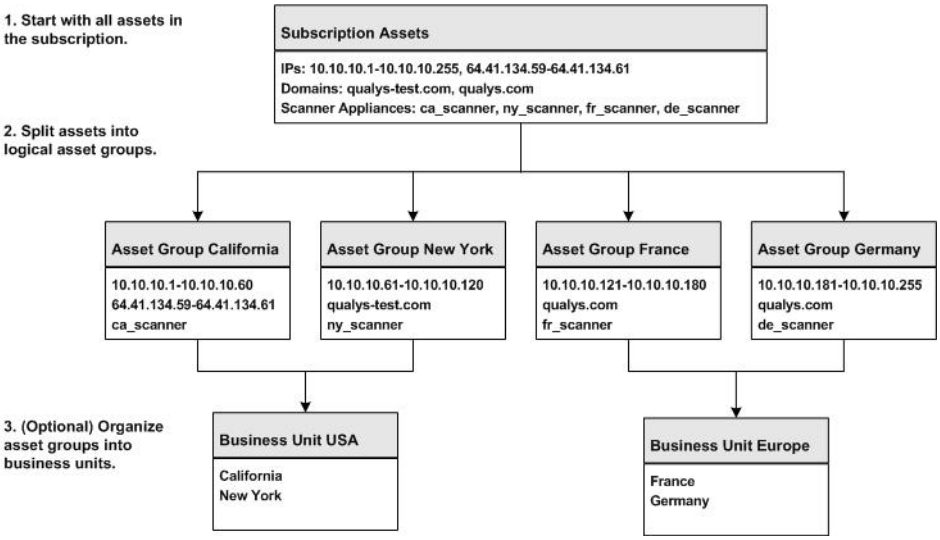
Select "Asset Groups" under "Assets" to view your asset groups. Go to New > Asset Group to add a new asset group. Asset grouping offers great flexibility, allowing you to assign assets to multiple asset groups.



To view information associated with an asset group, click anywhere in the data list row for the group you're interested in, then click the down arrow that appears in the row to see the Quick Actions menu. Select "Info" from the Quick Actions menu.

You may wish to go one step further and organize asset groups into business units. This allows you to grant management responsibilities to dedicated Unit Managers. Unit Managers are tasked with overseeing assets and users within their respective business units. Business Units are managed in the “Users” section.

Following is a typical example of how an enterprise might segregate their assets into user-defined business units:



User Management

User management capabilities allow you to add multiple users with varying roles and privileges. Each user is assigned a pre-defined user role which determines what actions the user can take. The most privileged users are Managers - they have full privileges and access to all assets in the subscription.

Managers and Unit Managers have the ability to manage assets and users. Managers have management authority for the subscription, while Unit Managers have management authority on an assigned business unit only.

Scanners and Readers have limited rights on their assigned assets. Scanners can launch scans and run reports. Readers can run reports.

Auditors have compliance management privileges. Auditors cannot run compliance scans, however they can define policies and run compliance reports. Auditors only have visibility into compliance data (not vulnerability data). This role is available when PC is enabled for the subscription.

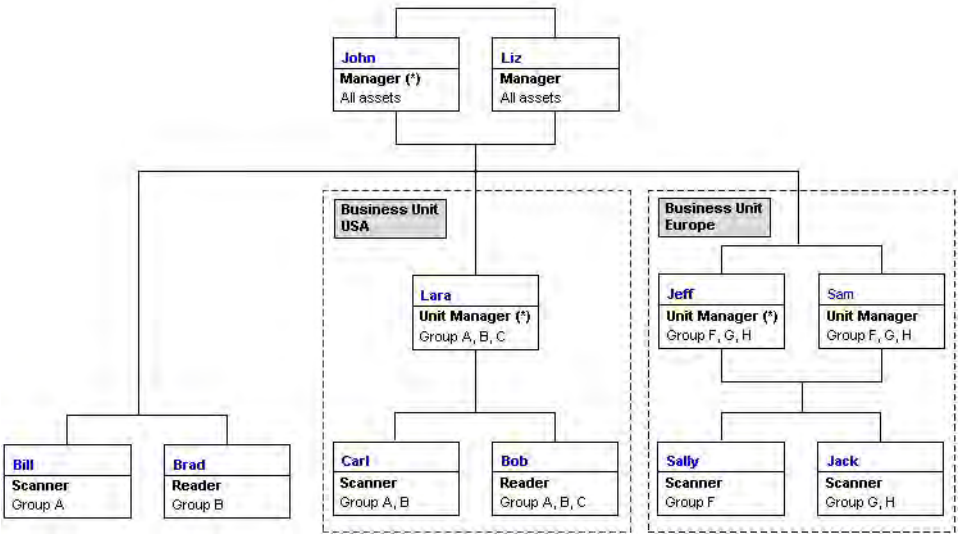
A Remediation User has limited access to the UI and can access only remediation tickets and the vulnerability knowledgebase. Remediation users do not have any scanning or reporting privileges. A Manager can assign Business Unit and Asset Groups and also tickets generated by policy rules for assets (asset groups) to the Remediation User.

A KnowledgeBase Only user has limited access to the UI. They can send and receive vulnerability notifications and view vulnerabilities in the KnowledgeBase. (This role is only available when this feature is enabled for your subscription. Only a Manager can assign this role.)

A User Administrator user will only have access to users, assets groups, business units and distribution groups. Users with this role can create and edit all types of users, except other User Administrators. They can edit and delete Manager users as long as there is at least one Manager account remaining in the subscription. That means the User Administrator cannot delete the last Manager account and cannot change the role for the last Manager account. The User Administrator does not have permission to delete business units, distribution groups, or asset groups.

Contacts have one permission only - to receive scan email notifications.

A typical deployment will have multiple users with multiple business units as depicted in the following chart:

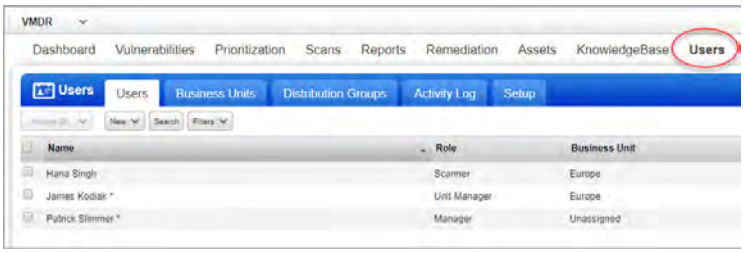


The Qualys solution provides great flexibility in defining users, asset groups, and business units to reflect the organizational structure and business requirements for the enterprise.

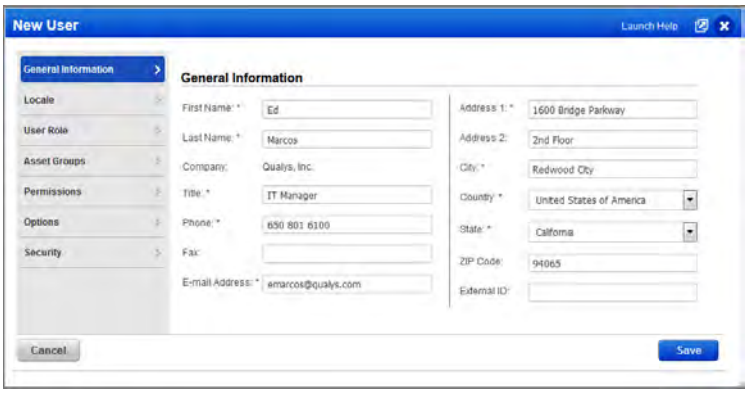
Note: For Express Lite accounts, you can add a total of 3 Manager users (no other user roles are available), and Business Units are not available.

Adding Users

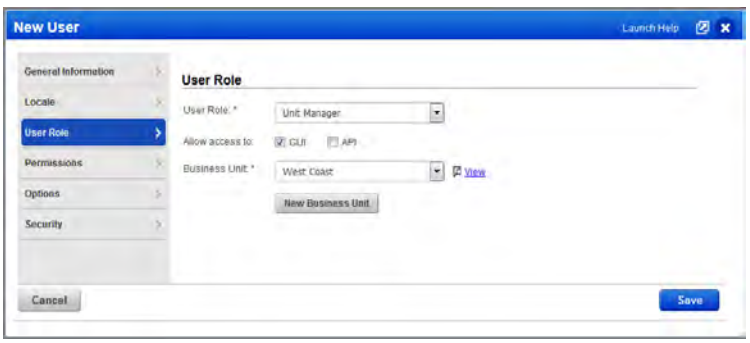
On the top menu, select “Users”. Then go to New > User. You can add users to your account, assign them roles, and associate them with business units.



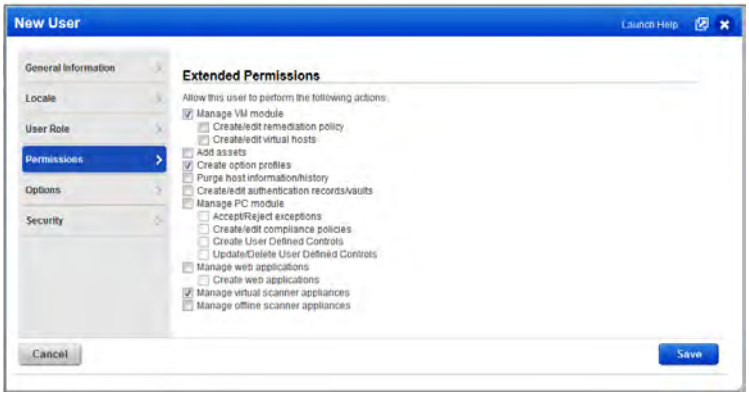
In the “General Information” section the account creator provides general user information like the user’s name, business title, and contact information.



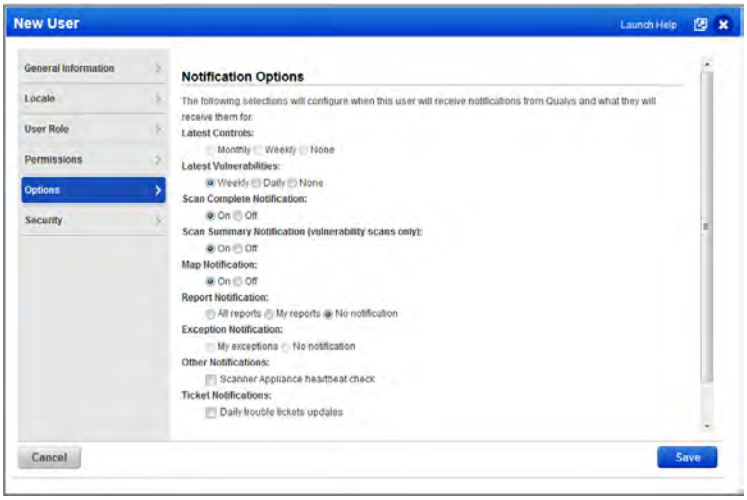
Go to “User Role” to assign a user role, access permissions and business unit.



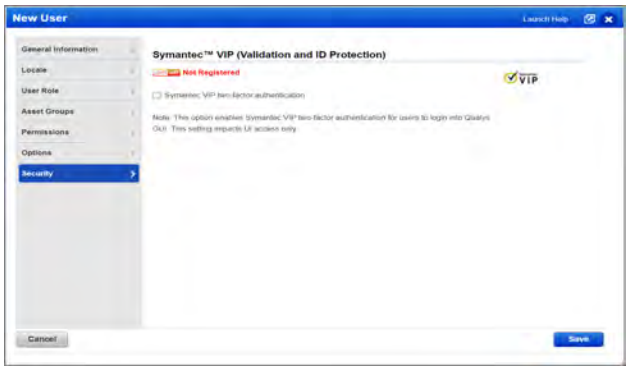
Go to “Permissions” to assign permissions to the user. Different permissions appear for different user roles. The example below is for a Unit Manager role.



Select “Options” and you’ll see several email notifications you can enable for the user.



Now go to “Security” and you can select Symantec VIP two-factor authentication for the user, or enable SAML SSO for the user (when this option is enabled for your subscription). If both options are turned on, Symantec VIP will be ignored and SAML SSO will be used. (Tip: Managers can require Symantec VIP or SAML SSO for all users by going to Users > Setup. For Symantec VIP, select Security. For SAML SSO, select SAML SSO Setup.)



About SAML SSO

When SAML SSO is activated for a user account, the user will no longer log in to the service using their service credentials. Instead, users will click a link to enter a username and password to authenticate to their identity provider (IdP). Upon successful authentication, the IdP redirects to the service's Assertion Consumer Service URL, the service validates the contents of the response, resolves the usernames and starts the user's session.

The account must have these settings:

1) SAML SSO must be enabled for your subscription by support or your account manager.

2) The New Data Security Model must be accepted for the subscription. A Manager can opt in by going to Users > Setup > Security.

How to enable SAML SSO for all new users

Managers can go to Users > Setup > SAML SSO Setup and select the option "Enable SAML SSO for new users".

How to enable SAML SSO for select users

Go to Users > Users and edit the user's account. You'll see the SAML SSO option in the Security section.

About Symantec VIP Support

When Symantec VIP is enabled for a user, the user completes a two-part process to log in to our user interface. The user will enter login credentials (login name and password) followed by Symantec VIP credentials (Symantec VIP credential ID and one-time security code).

Note - Symantec VIP two factor authentication impacts UI access only (not API access).

How to enable Symantec VIP authentication for all new users

Managers can go to Users > Setup > Security and select the option "Require Symantec VIP two-factor authentication for all users".

How to enable Symantec VIP authentication for select users

If not enabled globally, a Manager can enable Symantec VIP authentication individually for specific users. Go to Users > User Accounts and edit the account you're interested in. Then select the option "Symantec VIP two-factor authentication" under Security.

How to enable Symantec VIP authentication for yourself

All users with login privileges can opt in for Symantec VIP authentication by registering their own Symantec VIP credential with our security service. Edit your own user account, go to the Security section and register your credential.

I don't have a Symantec VIP credential. How do I get one?

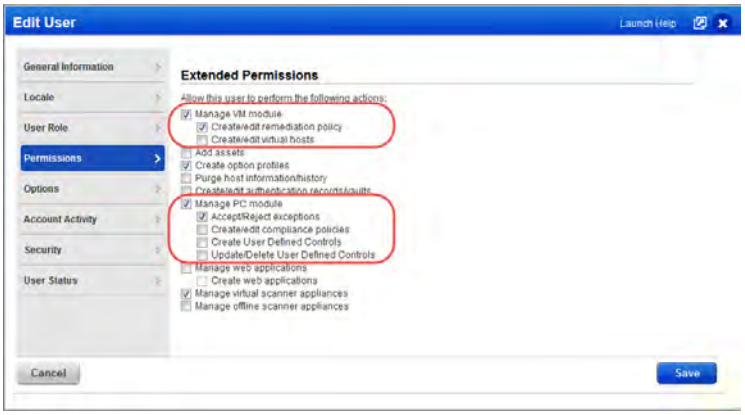
You can get a credential from the Symantec Center at: https://idprotect.vip.symantec.com or https://vip.symantec.com. Each Symantec VIP credential bears a credential ID and allows the user to generate one-time security codes as needed.

Controlling User Access to Apps

You can grant a user's account access to various apps on our Cloud Security Platform.

Grant access to VM, PC, SCA

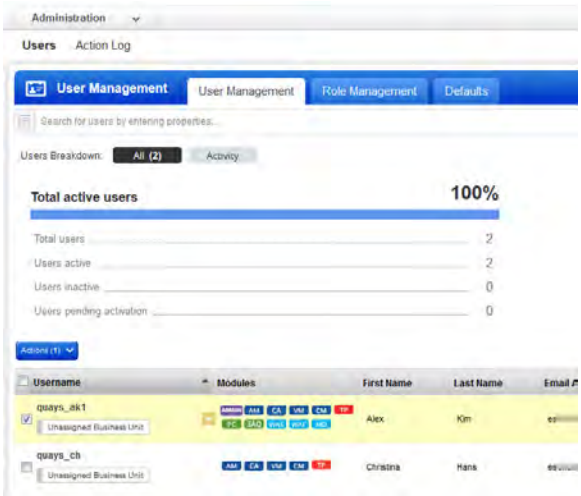
(Managers) Edit a sub-user's account to grant access to these apps: VM, PC, SCA. Select "Manage VM module" to grant access to VM, "Manage PC module" to grant access to PC or "Manage SCA module" to grant access to SCA. Only apps enabled in your subscription are available. Clear any of these options to take away access.



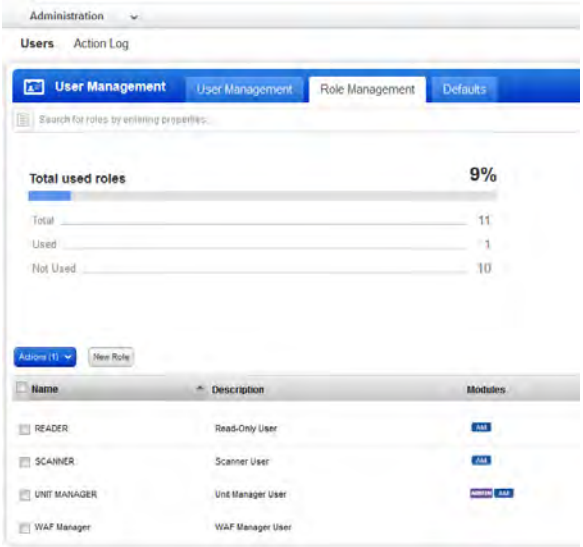
Note - Depending on the user's role you may see additional permissions for each app.

Grant access to other apps on our Cloud Security Platform

(Managers) Use the Administration utility (last option in the app picker) to view and manage users and grant access to applications like WAS, WAF, CA, CM, SAQ, etc. On the User Management tab you'll see the apps each user has access to. Access is role based.



Go to Users > Role Management to view, create, edit roles with various permissions and access.



You're Now Ready

At this point, you should have successfully obtained authorization, logged in, created domains for mapping, added hosts for scanning, and are ready to begin mapping and scanning. If any of the preceding steps failed to provide results similar to those in this setup section, please email or call Qualys Support before continuing. The sections to follow walk you through the primary functions of the Qualys solution, including mapping, scanning, reporting and remediation.

Mapping Your Network

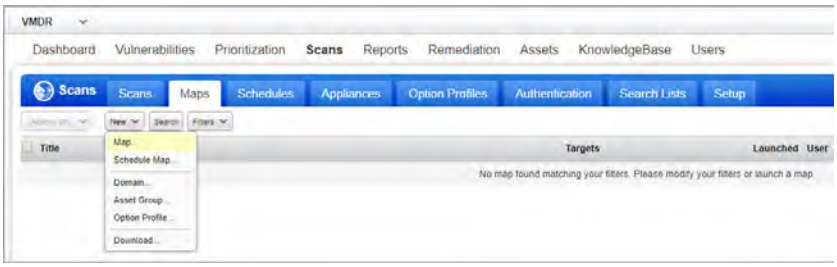
Before you can map a portion of your network, you have to tell us how you would like it to perform that mapping. This is called a "Network Map Profile."

Under Scans, select the "Option Profiles" tab, and then go to New > Option Profile. A New Option Profile page will open. Give the new profile a title, such as "Network A Map".

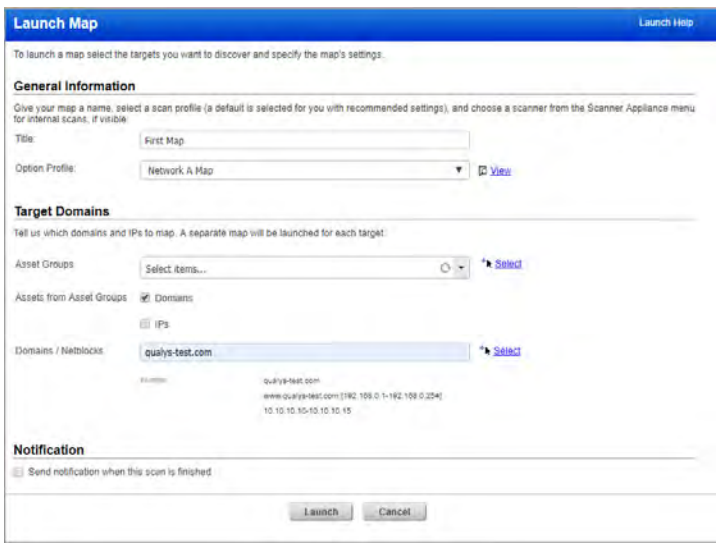
Go to the "Map" section of the option profile. Scroll down to the Options section and make sure the "Perform Live Host Sweep" option is selected. This option will allow you to map a domain and identify hosts in the netblock. If you're mapping an internal domain or internal IPs, then scroll up and select the option "Netblock Hosts only" for basic information gathering. Feel free later to try different selections for your map profile, but for now, select the "Save" button to save the option profile.

Running a Map

Now you're ready to run your first map. Select the "Maps" tab in the "Scans" section. The maps list appears. Go to New > Map.



The Launch Map pop-up appears, as shown below.

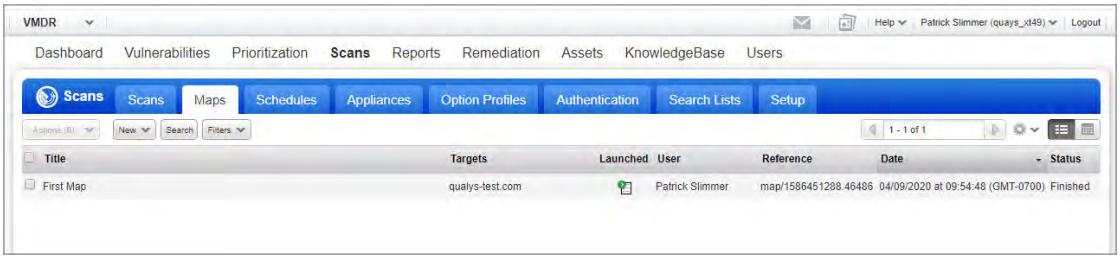


Enter the name "First Map" in the "Title" field and select your new map profile (e.g. "Network A Map") from the "Option Profile" menu.

The "Scanner Appliance" menu appears when your account includes a scanner appliance. When present, select the name of your scanner (required for mapping private use internal IPs) or External for external scanners.

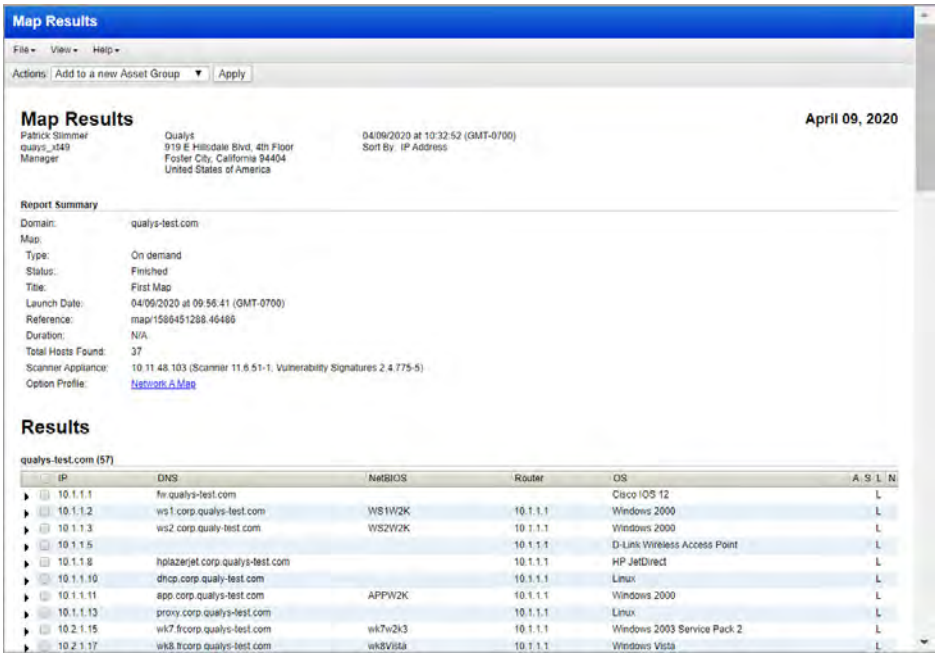
In the “Domains/Netblocks” field, enter the domain you already added or click the “Select” link to choose a domain from a list of domains in your account. In the example shown, the domain “qualys-test.com” is selected. (You can also map IP addresses and asset groups. See Map Targets to learn more.) Select “Launch” to start the map.

The maps list is refreshed and your new map is shown with the status “Running”. When the mapping is complete, the status changes to “Finished.” Also, the Qualys service will send you a map summary email to the address with which you registered when the map summary notification option is enabled in your account.



Map Results

On the maps list, click the data list row for your finished map and select the down arrow ▾ that appears in the row. Then select “View Report” from the Quick Actions menu. Your Map Results will appear online in an HTML report. The sample map below was generated for the “qualys-test” domain. At the top of the page is a Report Summary. Take a look at yours and note the information completeness.



Now scroll down the page to see the list of hosts discovered along with legend information that indicates "Approved," "Scannable," "Live," and "Netblock." This map was generated on the qualys-test domain for demonstration purposes. The discovered hosts were all live at the time of the scan but are not in the approved hosts list for the domain or in the domain's associated netblock. Hosts are scannable when they are already in the user's account and available for scanning. Your map will have results specific to the domain that you mapped.

Click the arrow (▶) next to any host to view a list of open services on the host. The discovery method used to detect each service is listed along with the port the service was found to be running on (if available).

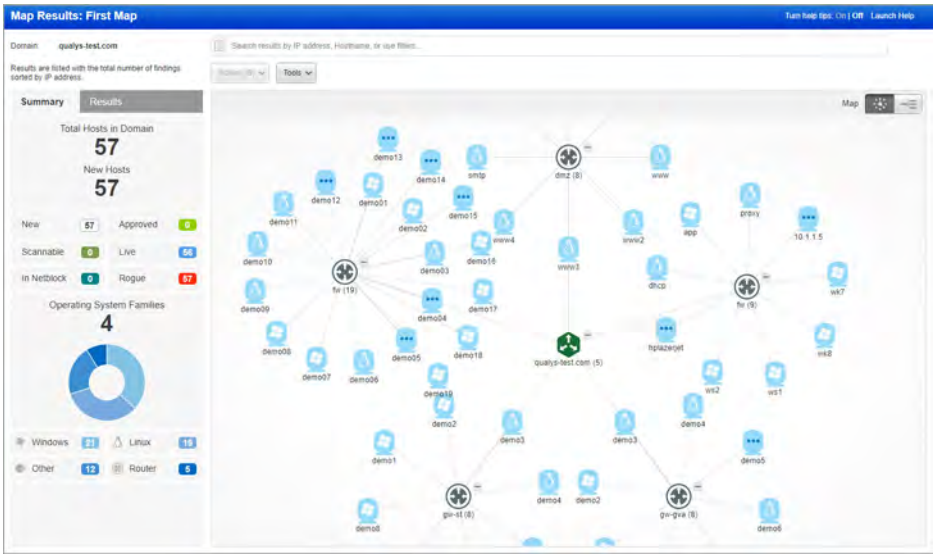
The top of your report includes an Actions drop-down menu with powerful workflow options that allow you to select hosts in the results and do any of the following: add hosts to the subscription, add hosts to groups, remove hosts from groups, launch and schedule scans on hosts, edit hosts, purge host details, and approve hosts for the domain.

Let's add hosts from the map results to a new asset group for scanning. Hosts with the "S" indicator on the right-side legend are scannable, meaning that they already exist in your account. Select the check box next to each scannable host you want to add to the group. Then go to the Actions menu at the top of your report and select "Add to a new Asset Group" from the drop-down menu, and click "Apply". On the New Asset Group page give your asset group a title, such as "First Asset Group." You'll notice that the selected hosts are already assigned in the IPs section. The Business Info section is where you specify an impact level used to calculate business risk in scan status reports (automatic). The impact level "High" is assigned by default. Select "Save." The new asset group is saved to your asset groups list and is available for mapping, scanning and reporting. We'll reference this group in the next chapter when scanning for vulnerabilities.

Viewing Map Results in Graphic Mode

Now go to View > Graphic Mode from the menu at the top of your report.

We will prepare a graphical representation of the map in a separate window. Following is an example.



Click on any host in the map to see details in the Preview pane, as shown below. You'll see basic information on the discovered host, its OS, and how it was identified:

Looking for certain hosts? Easily search the results by IP address, hostname, or certain host attributes. Make selections in the Search field at the top or in the Summary pane on the left.

Scheduling Maps

In the previous instance, you ran a map on demand. You can also schedule maps, periodically, that require no human intervention. To schedule a map, select the "Schedules" tab under "Scans". Then go to New > Schedule Map. Give the scheduling task a title, such as "First Map Schedule". Your name should appear in the Task Owner field and the default option profile will appear in the Option Profile field. In the Target Domains section, specify your map target. Then go to the Scheduling section to pick the start date and time, duration, and any other options. Select "Launch Help" in the top right-hand corner for assistance with available settings. When finished, select "Save."

Now Qualys will repeat that map as scheduled, and each time it completes the map, it will send you a summary email with a secure link to the Map Results report. As you will see later, repeated mapping coupled with reporting on prior map results, a Manager can quickly see any changes to the domain due to any new or rogue devices.

Map Targets

Each time you launch or schedule a map, you specify one or more map targets in the Target Domains section. You may specify any combination of registered domains, IP addresses/ranges, and asset groups. When you select an asset group for the map target, you have the option to map the domains and/or the IPs defined in the asset group.

When multiple map targets are submitted in a single map request, the service automatically produces multiple map reports. The service produces a separate map report for each registered domain and for each group of IPs. For example, if you enter 2 registered domains, then the service produces 2 map reports. If you enter 2 registered domains plus a range of IPs, then the service produces 3 map reports. All of the maps produced from a single request will share the same user-provided map title. The Targets column in your Maps list identifies the registered domain name or the IP addresses/ranges included in each map report.

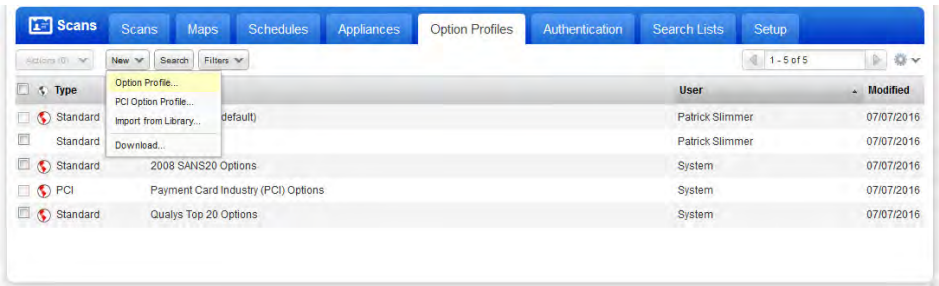
Mapping Summary

Qualys supports both on demand and scheduled mapping. Mapping profiles allow you to tailor the discovery based on your selection of mapping criteria. All mappings initiate emails with result summaries and links to the saved Map Results information.

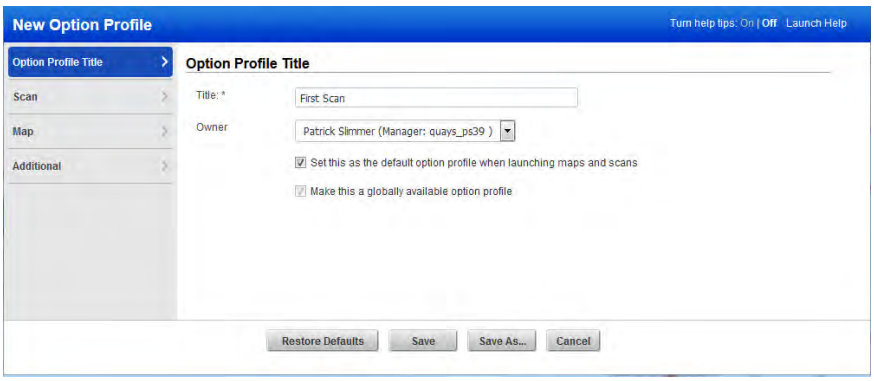
Scanning for Vulnerabilities

As with mapping, scanning requires an option profile. You can create your own option profile, use the default profile, or select one from the library. The Qualys Library provides pre-configured option profiles designed specifically for vulnerability scanning. You can import these option profiles into your account and use as-is or edit them as required.

Let's create a new option profile. Go to "Scans" on the top menu and select the "Option Profiles" tab. Then go to New > Option Profile.



The New Option Profile page appears. As you did with mapping, give the profile a name, such as "First Scan" and then select the "Set this as the default…scans" check box.



Now go to the "Scans" section on the left to see available scan options. Keep all of the default scan options as is except scroll down to the "Authentication" section and select the "Windows" check box to enable Windows authentication. Select "Save" to save the new option profile. You will now be returned to the option profiles list, and the new default profile called "First Scan" will appear.

The Windows Authentication feature enables Windows trusted scanning. Qualys supports trusted scanning for Windows, Unix, Oracle, Oracle Listener, SNMP, Cisco IOS, IBM DB2, VMware, MySQL and many more technologies. Refer to the online help and search for "authentication" to find all supported technologies. When authentication is enabled for your scans, we have the ability to gather more system intelligence on target hosts.

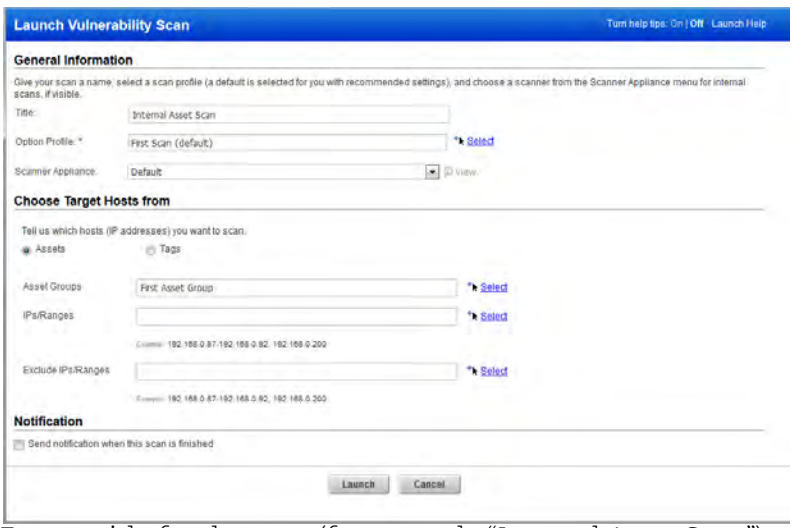
Trusted scanning references user-defined authentication records in your account. Each record identifies authentication credentials to be used for authentication to certain hosts. For Windows authentication you may select local or domain authentication. For domain authentication Qualys provides methods for IP-based authentication and domain-based authentication. Trusted relationships are supported using both of these methods.

If domain authentication will be used, please review our documentation for information on domain account requirements before you begin. Refer to the online help or download the document "Windows Trusted Scanning" from the Resources section (Help > Resources > Tips and Techniques).

To add a Windows authentication record, select the "Authentication" tab under "Scans". Then go to New > Windows Record. On the New Windows Record page, give the record a title. Under Login Credentials, select local or domain authentication. For domain authentication it's recommended you select "NetBIOS, User-Selected IPs" for IP-based authentication and then enter the target domain name. For basic authentication, enter the user name and password for the Windows user account to be used. (Optionally, select "Authentication Vault" if the password for the Windows user account is stored in a third party authentication vault. You must already have a vault record defined in your account to use this option.) In the IPs section, under Available IPs, select the IPs/ranges to be scanned and click "Add". Lastly, select "Save". The authentication records list will appear and your new record will be listed.

Starting a Scan

Now you are ready to run your first scan. Go to the "Scans" tab and then go to New > Scan. The Launch Vulnerability Scan pop-up appears.



Enter a title for the scan (for example "Internal Asset Scan") and make sure that the "Option Profile" field shows your new scan profile (for example "First Scan"). Note the service provides a variety of pre-configured option profiles to assist you with vulnerability scanning. You can import an option profile from the Library and apply it to the scan (and the imported profile will be saved in your account for future use).

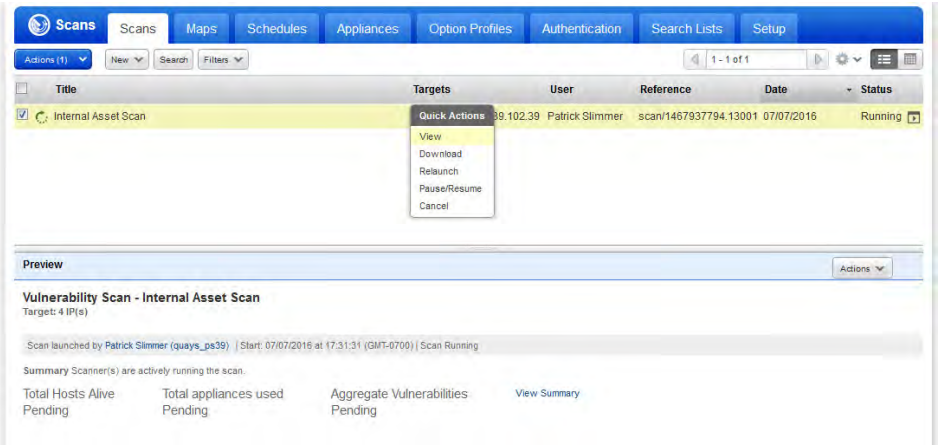
Specify a target asset group (for example, “First Asset Group” created previously from your map results). You can also enter IPs or IP ranges in he “IPs/Ranges” field.

You can also pick one or more scanner appliances for running the scan in the “Scanner Appliance” field, or let the system use the default scanner associated with the asset group that you are scanning. (Note: If you are scanning the demo IPs, you must select External in this field.)

Now, click “Launch”.

Once the scan begins, you will see the Scan Status window which is updated every 60 seconds with scan status information. You can move this window out of your way or close it. You can re-open the scan status at any time from the scans list.

During the scan, you can view the scans list in the main window and see the scan task status. To take actions on a scan, click anywhere in the data list row and then click the down arrow that appears in the row to show the Quick Actions menu.



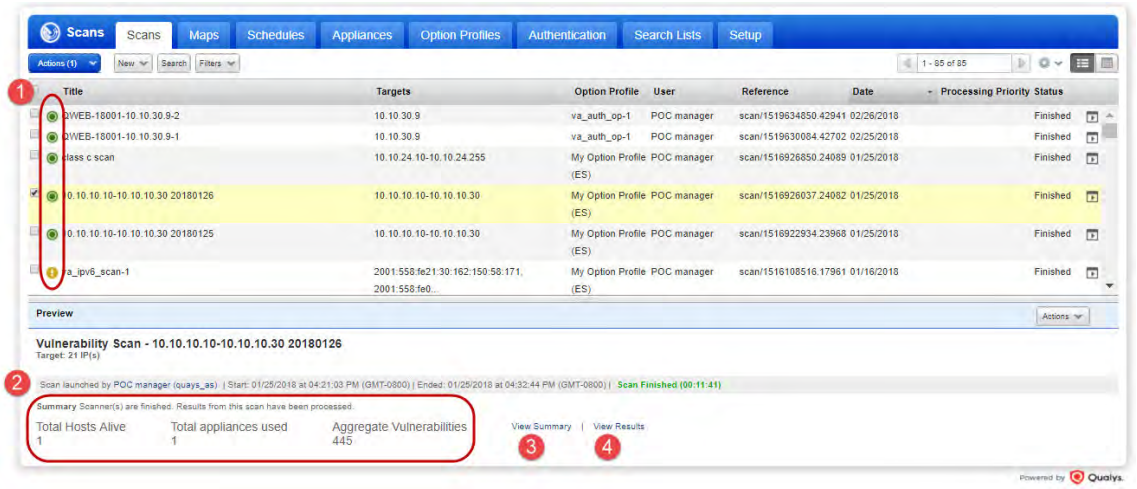
For a scan in progress you can cancel it to stop the scan job, and you can pause it to stop the scan job and resume it later. When you later resume a paused scan, the scan task will pick up where it left off. Select “View” to re-open the Scan Status window (see sample below).

The “Relaunch” option allows you to re-start a previous scan using the previous scan’s settings. The service makes a best effort to recall the previous scan’s settings and prefill values as a convenience; the current date is appended to the previous scan’s title.

A scan segment is the time when scanner(s) are actively scanning a scan job, or a part of it in the case of a paused scan. Only the time when the scanner(s) are performing a scan job is counted in the scan duration.

Scan Status

You can easily track a scan and its status by going to the scans list. The solid icon tells you all scan results have been processed and these results are available for reporting. The next time you create a scan report (based on automatic data) the scan results from the scan will be included. Also you'll see the scan results throughout the application.

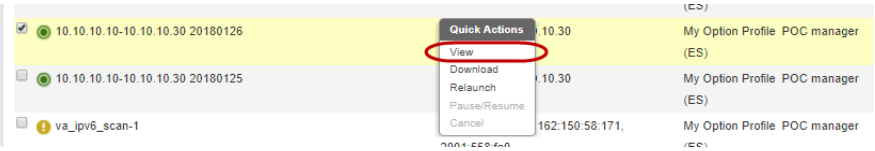


1) Scan Status Icons. A solid icon (filled-in) means all results available for the scan have been processed, meaning the host scan data has been updated throughout your subscription, and the results are available for reporting. When a scan is finished and the results have been processed, you'll see . When results processing is in progress, you'll see . You can always mouse over an icon to see the scan status.

2) Summary in the Preview Pane. The summary includes the number of hosts scanned and the number of appliances used and the number of vulnerabilities detected. A summary statement gives you the status of the scan and whether the results have been processed. Also, if your scan was interrupted or if there was a scan error, such as the scanner appliance was unavailable, then you'll see the error returned.

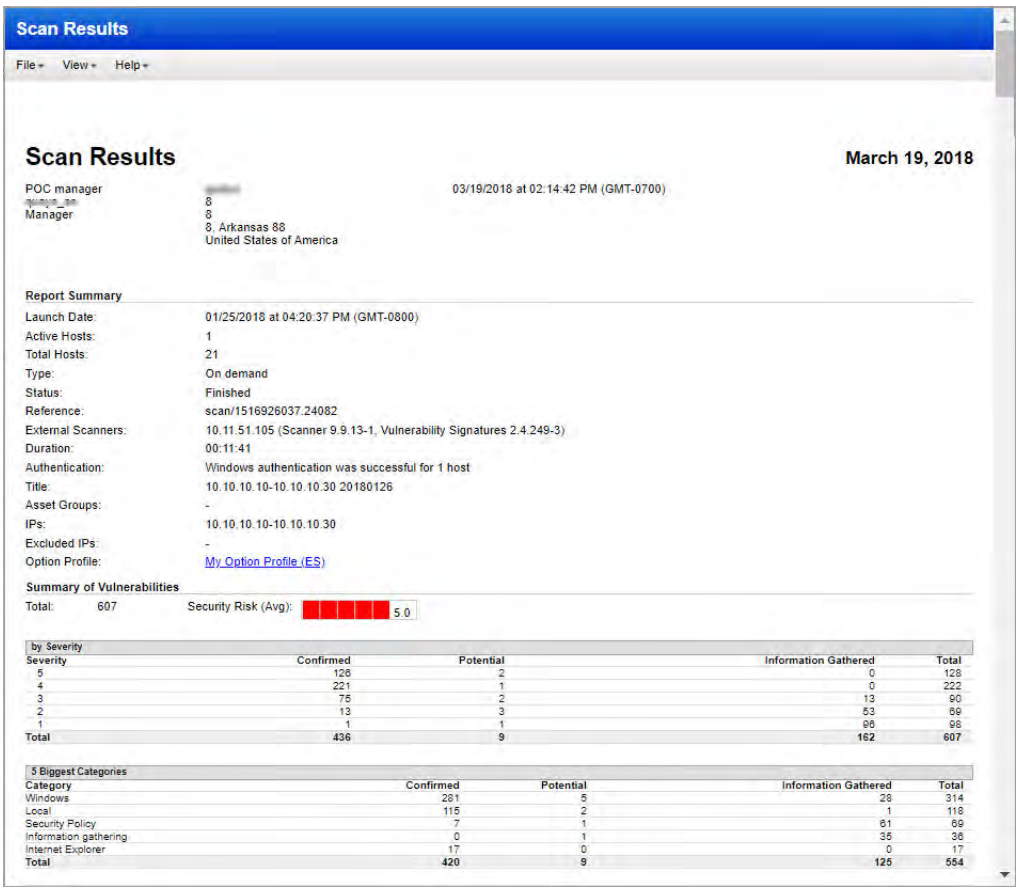
3) View Summary. Click the link in the preview section to see the current status of the scan and details about scanner usage, including which scanners were used to scan target hosts. Click on the Scanners section and expand details for a scan segment to see which scanners (external scanners and/or scanner appliances) were used to scan hosts. (Note the Scanners section is only visible in accounts with New Scanner Services enabled.)

4) View Results. Click the link in the preview section (or choose View from the Quick Actions menu).



Scan Results

Scan results for completed scans are always available from the scans list. The top of the report shows a Report Summary with information about the scan task like the scan date, number of active hosts, the option profile used. Following the Report Summary is the Summary of Vulnerabilities.



Scan Results

File ▾ View ▾ Help ▾

Scan Results March 19, 2018

POC manager
Manager

8
8
8, Arkansas 88
United States of America

03/19/2018 at 02:14:42 PM (GMT-0700)

Report Summary

Launch Date:	01/25/2018 at 04:20:37 PM (GMT-0800)
Active Hosts:	1
Total Hosts:	21
Type:	On demand
Status:	Finished
Reference:	scan/1516926037.24082
External Scanners:	10.11.51.105 (Scanner 9.9.13-1, Vulnerability Signatures 2.4.249-3)
Duration:	00:11:41
Authentication:	Windows authentication was successful for 1 host
Title:	10.10.10.10-10.10.10.30 20180126
Asset Groups:	-
IPs:	10.10.10.10-10.10.10.30
Excluded IPs:	-
Option Profile:	My Option Profile (ES)

Summary of Vulnerabilities

Total: 607 Security Risk (Avg): 5.0

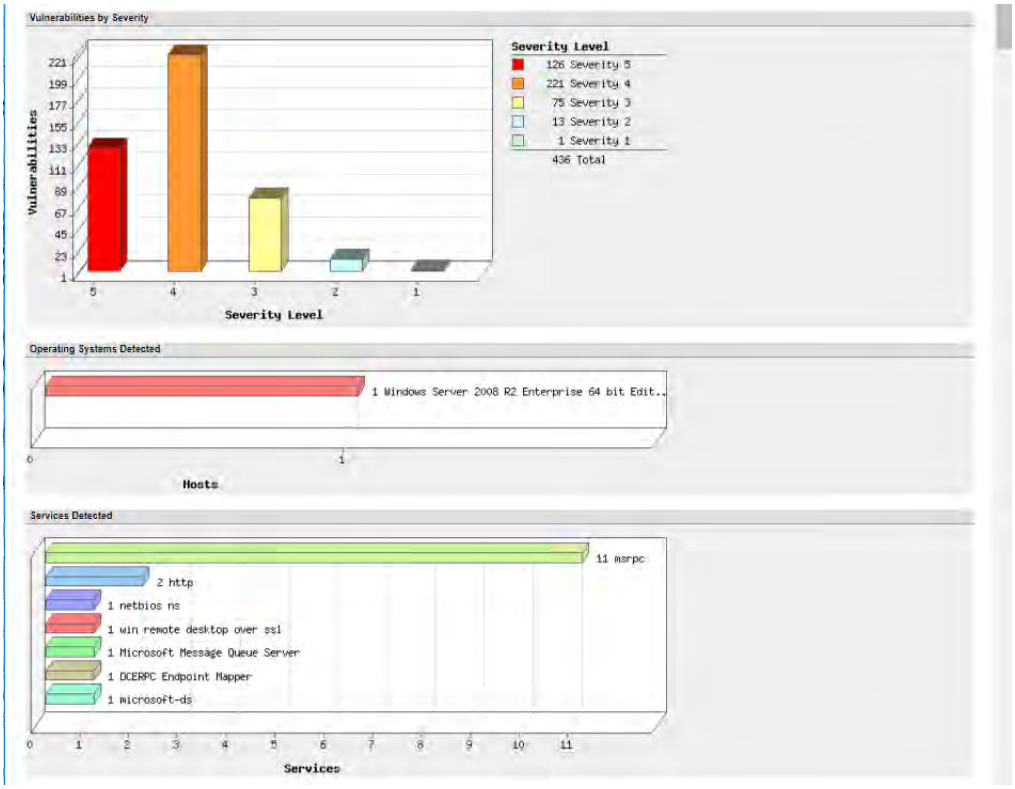
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	126	2	0	128
4	221	1	0	222
3	75	2	13	90
2	13	3	53	69
1	1	1	96	98
Total	436	9	162	607

5 Biggest Categories

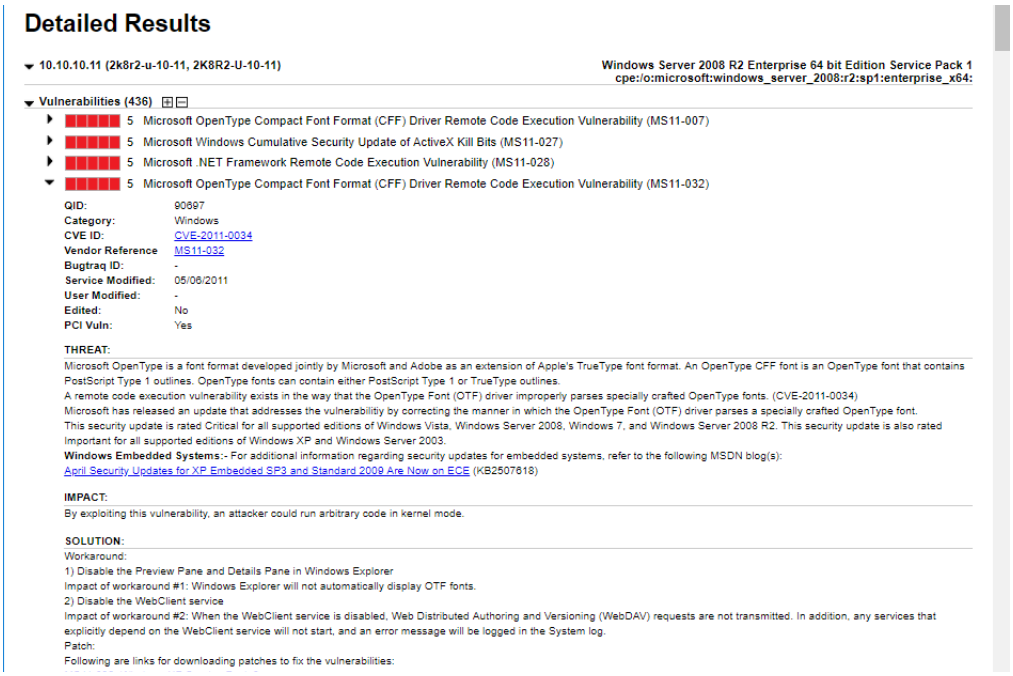
Category	Confirmed	Potential	Information Gathered	Total
Windows	281	5	28	314
Local	115	2	1	118
Security Policy	7	1	61	69
Information gathering	0	1	35	36
Internet Explorer	17	0	0	17
Total	420	9	125	554

Scrolling down, you will see graphs displaying the total number of vulnerabilities by severity, the operating systems detected and the services detected.



Then what follows are detailed results sorted by host and characterized by operating system. Detailed results for your internal hosts will be shown in this section of the report. The sample detailed results section below shows there were 436 confirmed vulnerabilities for IP address 10.10.10.11 running Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1.

If you click on the title of a vulnerability, you'll see a comprehensive description of the vulnerability, including threat, impact, verified solution .



Detailed Results

10.10.10.11 (2k8r2-u-10-11, 2K8R2-U-10-11) — **Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1**
cpe:/o:microsoft:windows_server_2008:r2:sp1:enterprise_x64:

Vulnerabilities (436)

- 5 Microsoft OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (MS11-007)
- 5 Microsoft Windows Cumulative Security Update of ActiveX Kill Bits (MS11-027)
- 5 Microsoft .NET Framework Remote Code Execution Vulnerability (MS11-028)
- 5 Microsoft OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (MS11-032)

QID: 90697
Category: Windows
CVE ID: CVE-2011-0034
Vendor Reference MS11-032
Bugtraq ID: -
Service Modified: 05/06/2011
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:
Microsoft OpenType is a font format developed jointly by Microsoft and Adobe as an extension of Apple's TrueType font format. An OpenType CFF font is an OpenType font that contains PostScript Type 1 outlines. OpenType fonts can contain either PostScript Type 1 or TrueType outlines.
A remote code execution vulnerability exists in the way that the OpenType Font (OTF) driver improperly parses specially crafted OpenType fonts. (CVE-2011-0034)
Microsoft has released an update that addresses the vulnerability by correcting the manner in which the OpenType Font (OTF) driver parses a specially crafted OpenType font.
This security update is rated Critical for all supported editions of Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. This security update is also rated Important for all supported editions of Windows XP and Windows Server 2003.
Windows Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog(s):
April Security Updates for XP Embedded SP3 and Standard 2009 Are Now on ECE (KB2507618)

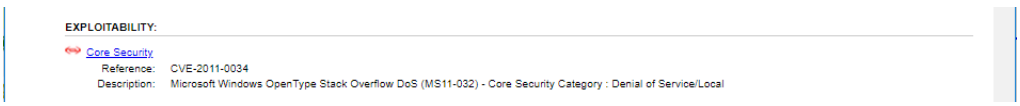
IMPACT:
By exploiting this vulnerability, an attacker could run arbitrary code in kernel mode.

SOLUTION:
Workaround:
1) Disable the Preview Pane and Details Pane in Windows Explorer
Impact of workaround #1: Windows Explorer will not automatically display OTF fonts.
2) Disable the WebClient service
Impact of workaround #2: When the WebClient service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted. In addition, any services that explicitly depend on the WebClient service will not start, and an error message will be logged in the System log.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Qualys correlates exploitability information from third party vendors and/or publicly available sources to provide up to date references to exploits and related security sources. Exploitability information enables users to perform risk-oriented analysis of vulnerabilities and to further prioritize their remediation plans.

Qualys correlates malware information with Qualys-detected vulnerabilities when malware threats for vulnerabilities are published in the Trend Micro Threat Encyclopedia. This correlation allows users to prioritize and filter vulnerabilities so that they can get actionable information to administrators for remediation of vulnerabilities that can lead to malware infections.

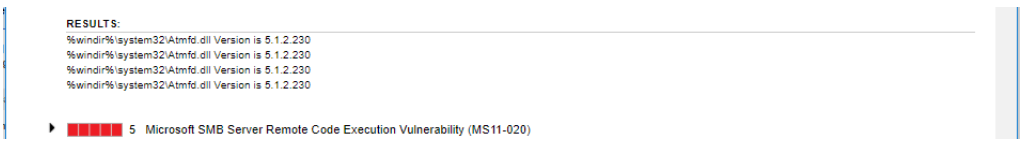
Sample exploitability information is below.



EXPLOITABILITY:

Core Security
Reference: CVE-2011-0034
Description: Microsoft Windows OpenType Stack Overflow DoS (MS11-032) - Core Security Category : Denial of Service/Local

Some vulnerability detections return scan test results. Sample scan test results is below.



RESULTS:
%windir%\system32\Atmfd.dll Version is 5.1.2.230
%windir%\system32\Atmfd.dll Version is 5.1.2.230
%windir%\system32\Atmfd.dll Version is 5.1.2.230
%windir%\system32\Atmfd.dll Version is 5.1.2.230

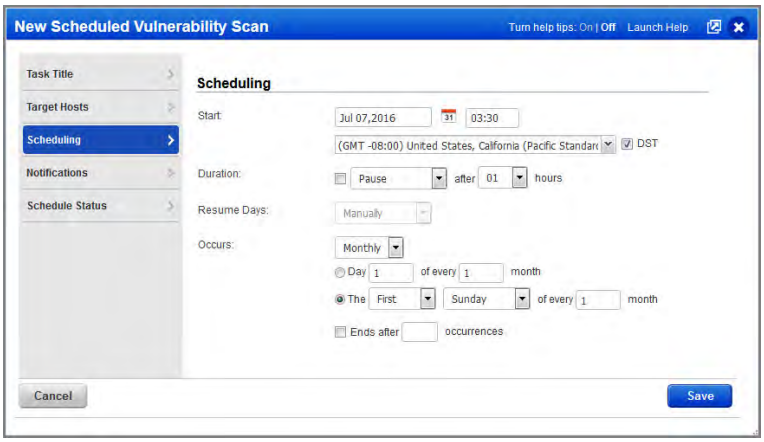
- 5 Microsoft SMB Server Remote Code Execution Vulnerability (MS11-020)

Scheduling Scans

As you saw with mapping, scanning can also be scheduled. Select the “Schedules” tab under “Scans” and then go to New > Vulnerability Schedule Scan. The New Scheduled Vulnerability Scan page appears. You give the schedule a title, select scan targets, and then choose a start time, duration and occurrence frequency.

By scheduling scans in conjunction with reports that combine historical data, managers can see vulnerability trends over time. This provides a good executive-level view of current state of vulnerabilities, and progress being made in remediation – a key element for regulatory compliance reporting.

You can configure the scheduled scan to run daily, weekly, monthly or one time one. This scan task runs monthly, the first Sunday of every month, starting at 3:30 AM Pacific Time (GMT-0800). You have the option of observing Daylight Saving Time (DST). You can also configure the scheduled scan to automatically stop after a set number of hours.



The Manager primary contact has the option to allow users to configure a scheduled scan to relaunch once a scan instance finishes, when New Scanner Services is enabled for the subscription. This gives users the ability to perform continuous scanning by launching a new scan as soon as the previous one finishes. This option is set by going to Scans > Setup > Scheduled Scans. Once configured, users have the option to start continuous scanning by configuring a schedule and selecting “Relaunch on Finish” from the Occurs menu.

Please note:

1) The schedule will be deactivated the first time a scan error is reported unless you choose to deactivate it after two or more scans have errors.

2) Be aware that each active scan counts towards the concurrent scans limit set for your subscription. Also any scan may have impact to your network and the same impact could occur repeatedly, until the schedule is deactivated, canceled or paused.

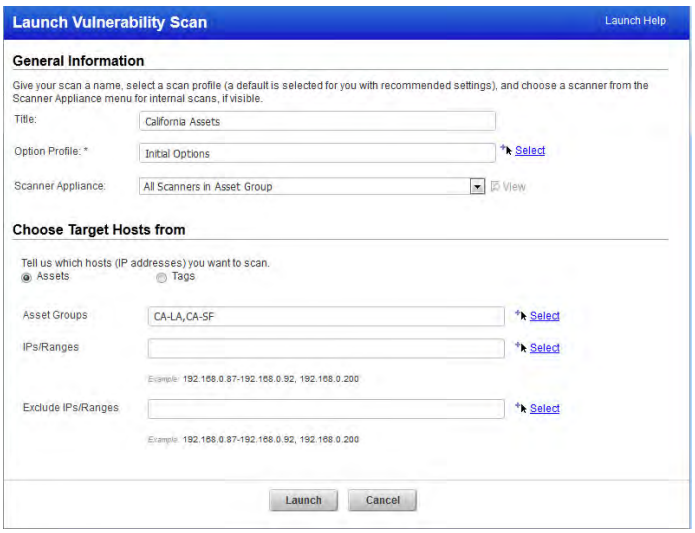
The Manager primary contact has the option to prevent the service form starting a new scheduled scan when there's an instance of it running. In this case the service skips launching the second scan, sets the next launch date to the future, and counts the skipped scan as an occurrence. This option is set by going to Scans > Setup > Scheduled Scans.

Scanner Parallelization

The scanner parallelization feature increases scan speed, making a scan up to 4 times faster, depending on the size of your network, while maintaining scan accuracy. It allows you to distribute a scan task to multiple scanner appliances when the scan target includes asset groups.

When enabled for a scan task at scan time, the task is distributed to multiple scanner appliances in parallel for each target asset group. The scanners in each asset group are used to scan the asset group's IP addresses. Upon completion, results are combined into a single Scan Results report.

To use the scanner parallelization feature, select the option "All Scanners in Asset Group" from the "Scanner Appliance" menu when launching or scheduling a scan.



View the scanner appliances list to see information about scanner appliances in your account. Select the "Appliances" tab under "Scans". Columns show whether an appliance status is online (blank) or offline (yellow warning icon) based on the latest heartbeat check (every 4 hours), whether the appliance is busy running maps and/or scans, and whether its software is up to date. Select "Info" from the Quick Actions menu to view more information for any appliance.

Selective Scanning using Search Lists

To perform a scan on individual vulnerabilities, you can tune the option profile for the scanner to only scan for selective vulnerabilities. This can be done by adding search lists to the "Vulnerability Detection" section of the scan profile. Select the "Custom" option and then click the "Add Lists" button to add one or more saved search lists to the option profile. The search lists define which vulnerabilities you want to scan for. When the option profile is applied to a scan task, the QIDs in the search list are scanned.

There are 2 types of vulnerability search lists: Static and Dynamic. A *Static* search list includes a specific list of vulnerabilities (QIDs) that you define. A *Dynamic* search list consists of a set of vulnerability search criteria (severity level, category, CVSS score, patch availability, etc). When a dynamic search list is used, the service queries the KnowledgeBase to find all QIDs that currently match the search criteria and then includes those QIDs in the action. Dynamic search lists are updated automatically by the service as new QIDs are added to the KnowledgeBase and new patch information becomes available.

To create and manage the search lists in your account, select the "Search Lists" tab from any of these sections of the UI: Scans, Reports or KnowledgeBase.

Note that vulnerability search lists may also be used in other business objects, including scan report templates (for selective vulnerability reporting) and remediation policy rules (for ticket creation). You can find complete information and instructions for managing and using search lists in the online help.

PCI Scans and Compliance

Qualys is certified to help merchants and their consultants evaluate the security of credit card payment systems that process, transmit and store cardholder data, and achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS). To learn how to validate compliance with the PCI Data Security Standard, go here.

The Payment Card Industry (PCI) Compliance module is available in your account only when the PCI module is enabled for your subscription.

PCI Data Security Standard

The PCI Security Standards Council requires banks, online merchants and Member Service Providers (MSPs) to protect cardholder information by adhering to a set of data security requirements outlined in the PCI Data Security Standard. Founding members of the PCI Security Standards Council are American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The PCI Data Security Standard (DSS) represents a common set of industry tools and measurements for ensuring the safe handling of sensitive information. It details technical requirements for the secure storage, processing and transmission of cardholder data.

Quarterly PCI External Scans Workflow

Per PCI DSS v3.0 requirement 11.2.2, the PCI Council requires merchants to perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the PCI Security Standards Council (PCI SSC). Qualys is a certified ASV. Every part of cardholder data system components needs to be scanned.

Follow these simple steps to achieve the PCI DSS requirements for quarterly external scans.

Step 1: Run a PCI External Scan

Go to VM/VMDR > Scans. To launch an on demand scan, select New > Scan. To schedule a scan, select New > Schedule Scan. For the scan settings, select the option profile "Payment Card Industry Options". This profile is provided by the service and it is required in order to meet PCI compliance for external scans. It includes configuration settings required for PCI external scans, according to the PCI Data Security Standard (PCI DSS). For the scan target, select your cardholder data system components.

Step 2: Fix Vulnerabilities and Re-Scan

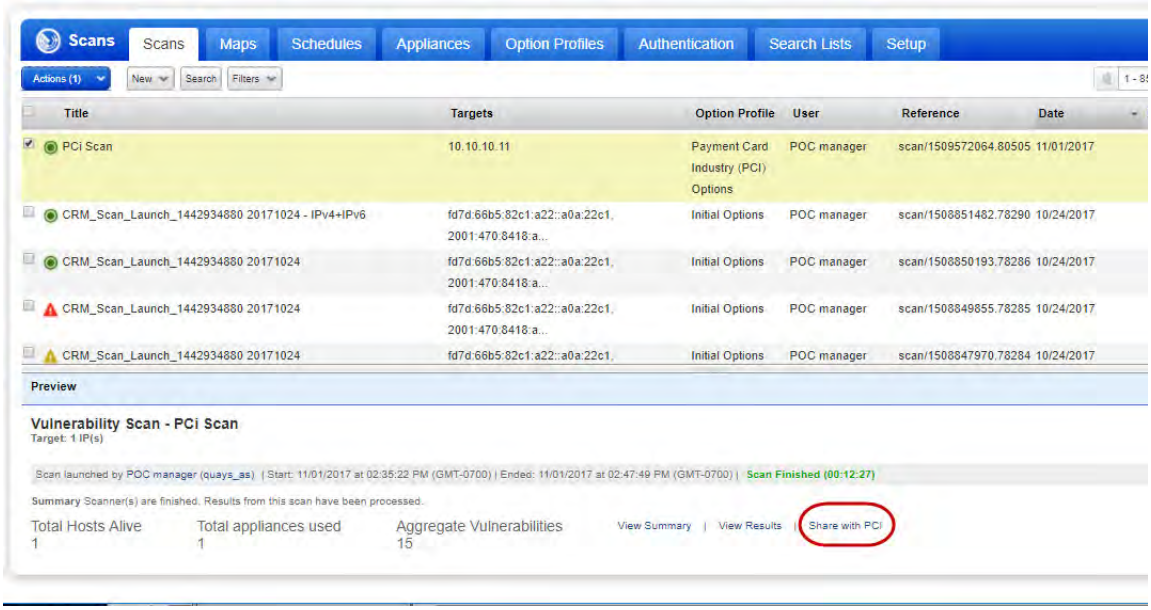
Run the PCI Technical Report to see whether your scan is compliant. Go to Reports > Templates, hover over the "Payment Card Industry (PCI) Technical Report" and then select Run from the Quick Actions menu.

Looking at your report you'll see the PCI compliance status (PASS or FAIL) for the overall report, for each host and each vulnerability detected. Vulnerabilities with the FAIL status must be fixed to pass the PCI compliance requirements. (Vulnerabilities with no PCI status are not required for compliance, however we do recommend you fix them in severity order.)

After fixing vulnerabilities, be sure to re-scan to verify that all PCI vulnerabilities are fixed and the overall status is PASS.

Step 3: Create Your Certification Report

1. Select PCI from the application picker. Then add a link to a PCI Merchant account (new or existing). You'll use this account for creating your certification report.
2. Select VM/VMDR from the application picker. Go to Scans, select your external PCI scan from the list, click Share with PCI (in the preview pane), and select the PCI account you've linked to.



3 Select PCI from the application picker. Log in to your PCI account.

4 Now you're ready to create your certification report within PCI. Go to Compliance > Compliance Status, click Generate (under Compliance Status > Actions) and use the report wizard to create your report and submit it to your acquiring banks.

Quarterly PCI Internal Scans Workflow

Per PCI DSS v3.0 requirement 11.2.1 and 11.2.3, the PCI Security Standards Council (PCI SSC) requires merchants to perform quarterly internal vulnerability scans and obtain a passing scan. Every part of cardholder data system components needs to be scanned. Per requirement 6.1, the PCI Council requires merchants to establish a process to identify and assign risk rankings for newly discovered security vulnerabilities, and to ensure all High ranking vulnerabilities are fixed.

How it works: The service uses the PCI risk rankings High, Medium and Low. By default these are set to the same CVSS scores as required for ASV external scans. By customizing the risk ranking scale within a PCI scan template, you have the ability to create different reports on different sub-nets using a different risk ranking scale for each.

Follow these simple steps to meet the PCI DSS requirements for quarterly internal scans.

Step 1: Create Asset Groups based on PCI Risk Ranking

Go to Assets > Asset Groups and create groups that organize your IPs according to your custom PCI risk ranking. Each group will correspond to a risk ranking. Later, after you scan your IPs, you'll create scan reports to verify compliance against your risk ranking. The PCI scan report template allows you to create a custom risk ranking scale with exceptions for selected QIDs (see Step 3).

Step 2: Run a PCI Internal Scan

Go to VM/VMDR > Scans. To launch an on demand scan, select New > Scan. To schedule a scan, select New > Schedule Scan. For the scan settings: 1) select the asset groups you want to scan (created in the previous step), and 2) select the option profile "Initial Options" or one that you've customized. The "Payment Card Industry (PCI) Options" is not recommended since this has settings tailored for an external PCI scan and it may increase your scan time significantly.

Step 3: Create Your PCI Scan Report

First create a PCI report template. Go to Reports > Templates and select New > PCI Scan Template. Be sure to create a template for each ranking scale (High, Medium, Low) within your organization.

Then create a report, go to Reports > Templates. Hover over your template, and select Run from the Quick Actions menu.

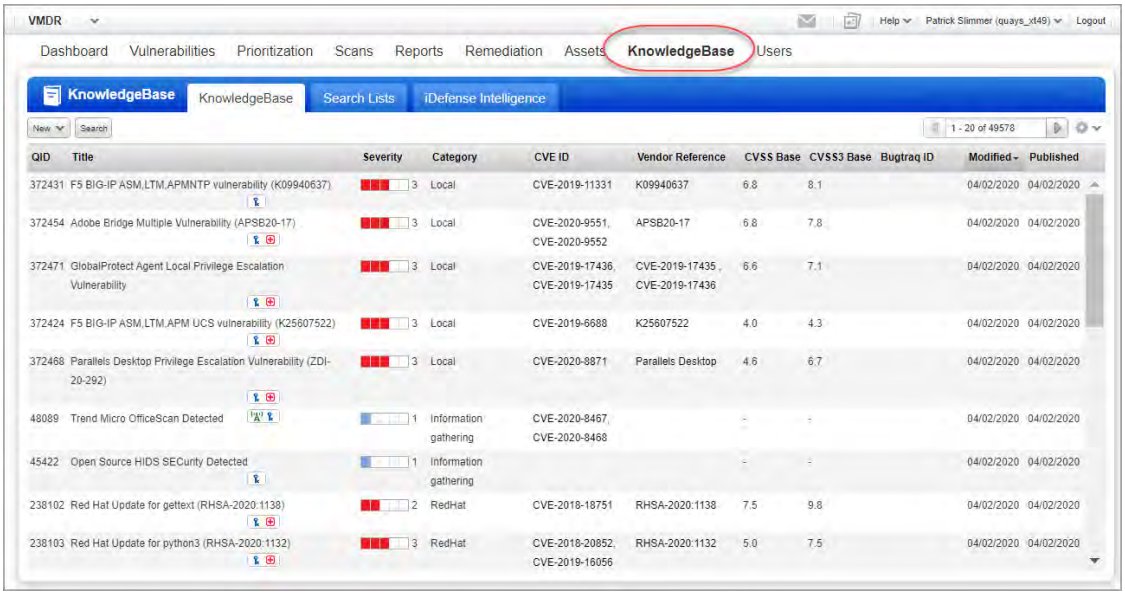
Step 4: Fix Vulnerabilities and Re-Scan

Review your PCI scan reports. If there are any High ranking vulnerabilities they must be fixed. Be sure to re-scan and re-run your reports to confirm that all High ranking vulnerabilities are fixed.

Vulnerability KnowledgeBase

Qualys provides highly accurate vulnerability scanning made possible by the industry's largest and most complete Vulnerability KnowledgeBase, an inventory of thousands of known vulnerabilities that covers all major operating systems, services and applications. Vulnerability checks in the KnowledgeBase are continuously added and updated.

To view the KnowledgeBase, select "KnowledgeBase" on the top menu.



In the upper right corner you'll see the total number of vulnerabilities along with navigation buttons for paging through the list.

The Severity column indicates severity from 1 (minimal) to 5 (urgent). Red represents confirmed vulnerabilities, yellow represents potential vulnerabilities, and blue represents information gathered.

Icons in the Title column indicate the discovery method assigned by the service, patch availability, exploitability, associated malware, and QIDs that correspond to report filters.

Discovery Method. Each vulnerability is assigned a discovery method indicated by these icons:

alone indicates Remote Only discovery. The vulnerability can be detected only using remote (unauthenticated) scanning.

alone indicates Authenticated Only discovery. The vulnerability can be detected only using authenticated scanning.

and indicates Remote or Authenticated discovery. The vulnerability can be detected using remote scanning or authenticated scanning.

Patch Available. indicates that a patch is currently available from the vendor. Note that you can use the Search functionality in the KnowledgeBase to find all vulnerabilities that have or do not have an available patch.

Exploitability. indicates that exploitability information is available. The service correlates exploitability information with service-detected vulnerabilities when known exploits are published by third party vendors and/or publicly available sources.

Associated Malware. indicates that malware is associated with this vulnerability. The service correlates malware information with vulnerabilities when malware threats for vulnerabilities are published in the Trend Micro Threat Encyclopedia.

Not Exploitable due to Configuration. indicates that this QID may be filtered out of reports when the report filter "Exclude QIDs not exploitable due to configuration" is selected. This filter appears in scan reports, patch reports and scorecard reports.

Non-Running Services. indicates that this QID may be filtered out of reports when the report filter "Exclude non-running services" is selected. This filter appears in scan reports, patch reports and scorecard reports.

Scanning Summary

Qualys supports both on demand and scheduled vulnerability scanning. Scanning profiles allow you to tailor the scan based on your selection of scanning criteria. All scans initiate emails with results summaries and links to the saved Scan Results information.

Qualys also provides additional scanning capabilities using other Qualys modules. Check out our video libraries and user guides (select Help > Resources from the top menu).

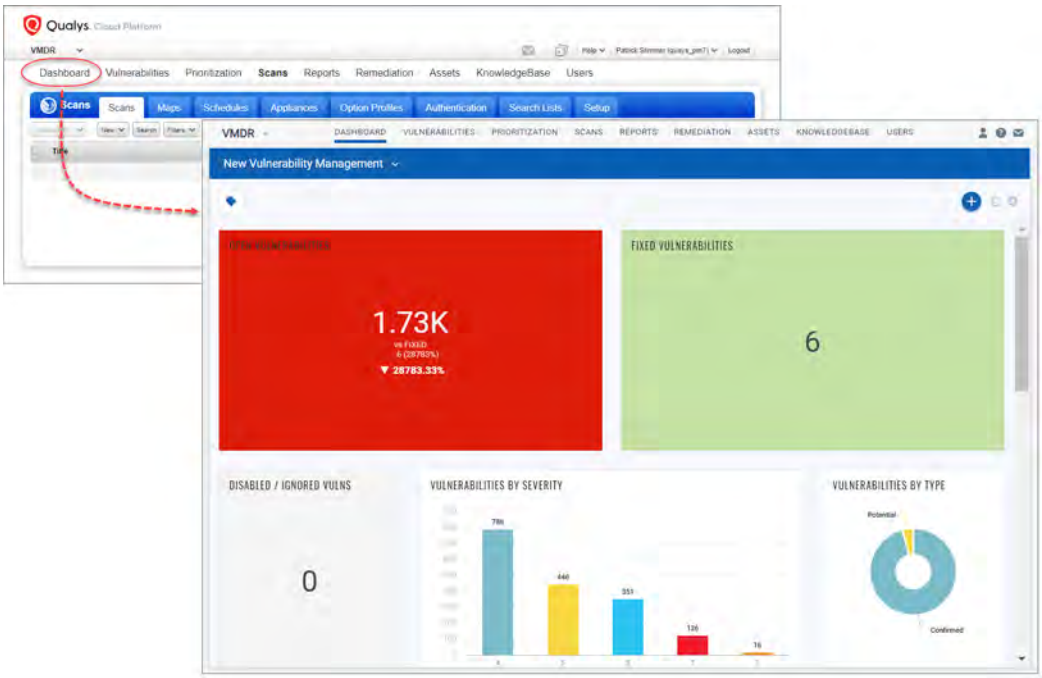
Search, View, Prioritize

Check out our interactive dashboards for a high-level summary of your security and compliance posture based on the latest data available in your account.

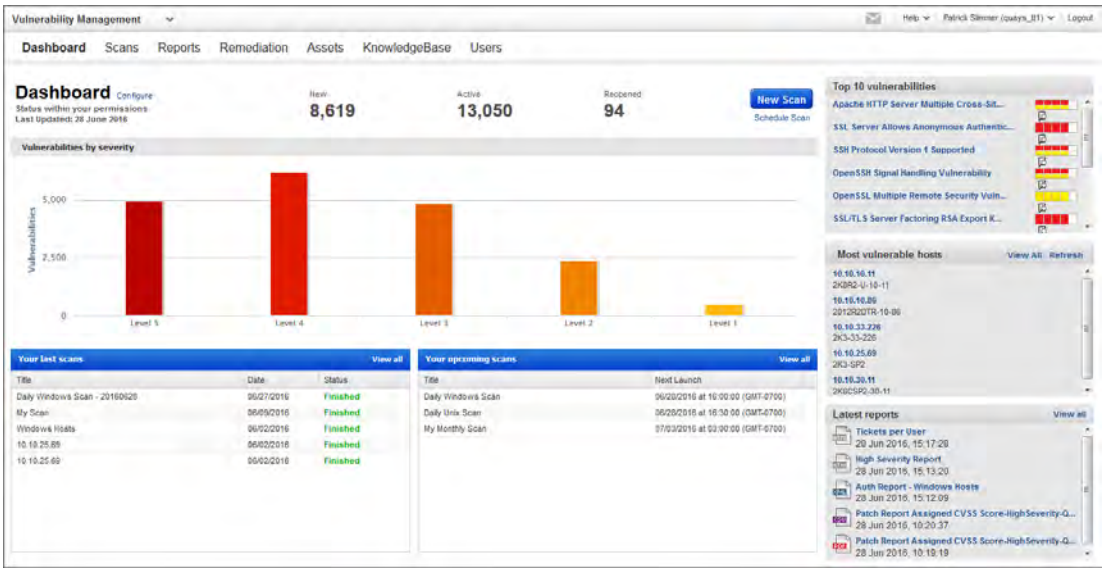
View Your Dashboard

Use the Qualys provided VMDR dashboard to view your security posture. Create multiple dashboards and switch between them. Each dashboard has a collection of widgets showing asset data of interest. Use the Actions menu to manage your dashboards.

To view your dashboard, select “Dashboard” on the top menu.



For accounts that have not been upgraded to VMDR you'll see the classic VM dashboard with a summary of your overall security posture based on the most recent vulnerability scan results. Here's a sample classic VM dashboard.



How do I configure the classic VM dashboard?

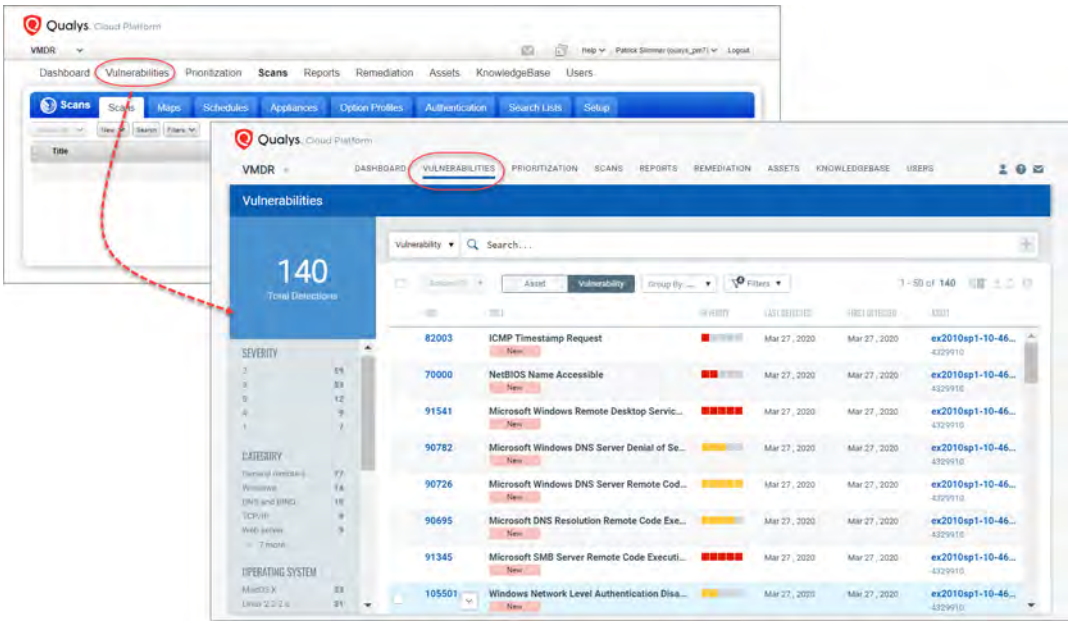
Click the Configure link to select the vulnerabilities and potential vulnerabilities you're interested in. (Note that disabled and ignored vulnerabilities are not included in your dashboard.)

How often is the classic VM dashboard updated?

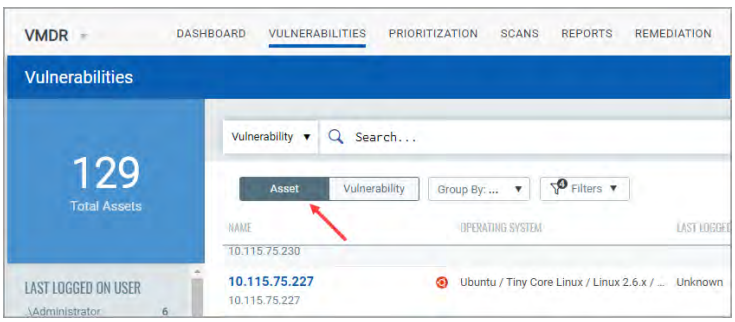
It's updated automatically as new scan results become available. You might want to start a scan from here (if you have scanning permissions). This is a convenient way to get the latest vulnerability data in your dashboard view.

View Asset and Vulnerability Details

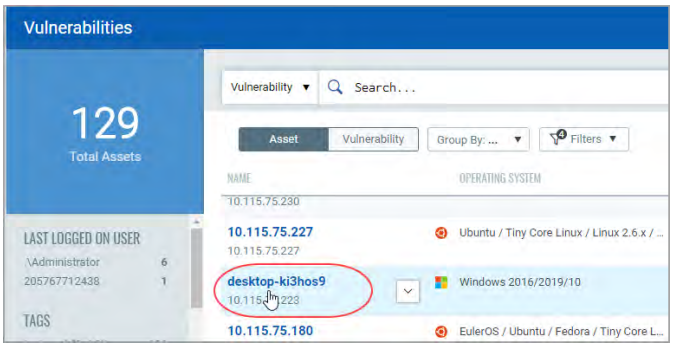
Choose “Vulnerabilities” to get a complete view of vulnerability posture from an asset and vulnerability point of view. (Not seeing this option? This option only appears in accounts that have been upgraded to VMDR.)



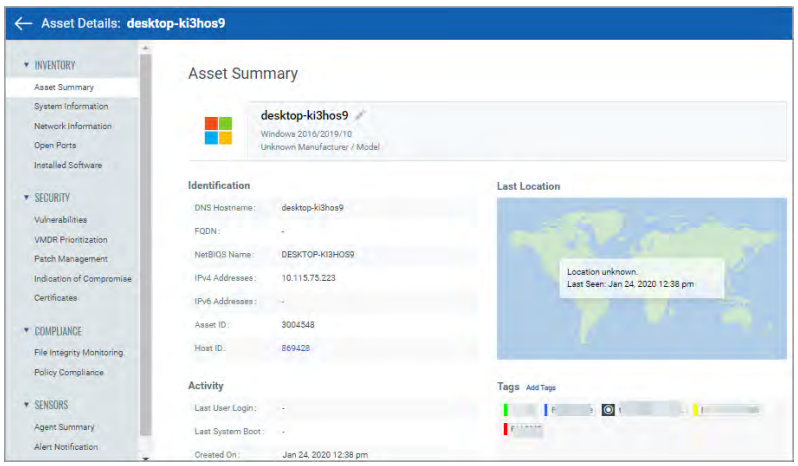
Select “Asset” to view the assets in your inventory. Use the metadata filters, group by options and custom query capabilities to quickly find what you’re interested in.



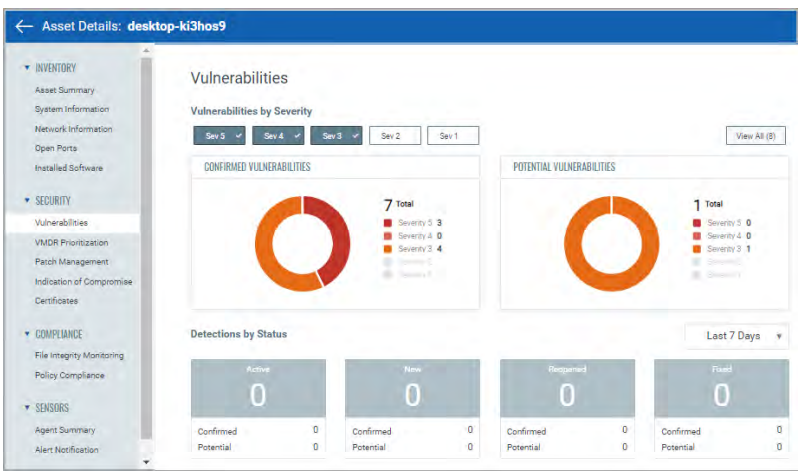
When you find the asset you're interested in, select the asset name link to get details.



You'll get a comprehensive asset view with many up-to-date details. Here's the asset summary of the selected asset

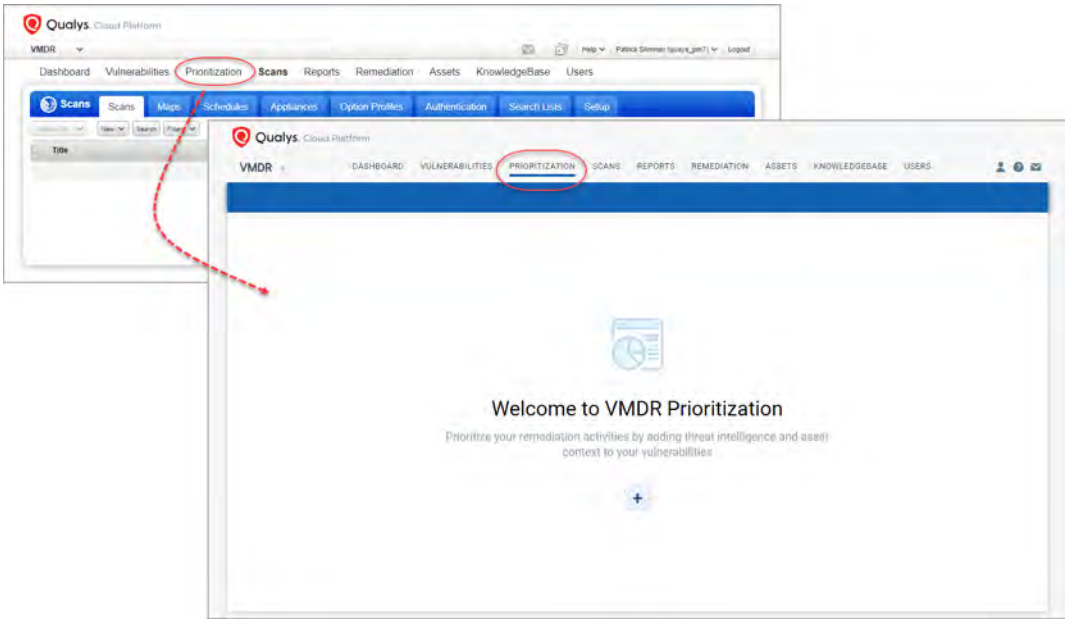


The "Vulnerabilities" section gives you an interactive summary of vulnerabilities on the asset. Choose the severities you want shown, click on widget charts and graphs to drill down further, and choose View for a list of all vulnerabilities.

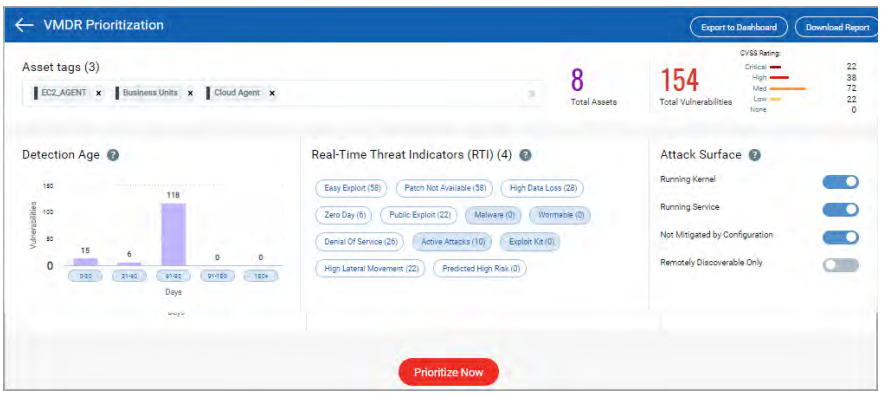


Run a Prioritization Report

Use the VMDR Prioritization report to automatically prioritize the riskiest vulnerabilities on your most critical assets – reducing potentially thousands of discovered vulnerabilities, to the few that matter. (Not seeing this option? This option only appears in accounts upgraded to VMDR. It does not appear in accounts with VMDR experience.)



When generating a report for the first time, simply click the plus icon +. For subsequent reports, you'll go to Reports and click "Create Report". Select asset tags to narrow down your prioritized list to vulnerabilities associated with the assets you select. Then select the filters you want to use for your report: Detection Age, Real-Time Threat Indicators and Attack Surface. See the help for each filter to learn more.



Click "Prioritize Now" to enable the threat intelligence to prioritize the riskiest vulnerabilities on your network for the assets you selected. Once you generate the report, you can proceed with patching the vulnerabilities (if the Patch Management app is enabled in your subscription), export the report in the form of a widget to your dashboard or download the report in CSV format.

Reporting and Remediation

One area that distinguishes Qualys from other Vulnerability Management solutions is its very flexible, comprehensive reporting capabilities. Most other solutions produce rigid reports that reflect, one-for-one, whatever data they have gathered during a scan.

Qualys reports consist of these basic components:

- Network assets included in the report,

- Graphs and charts showing overall summaries and network security status,

- Trending analysis for a given network,

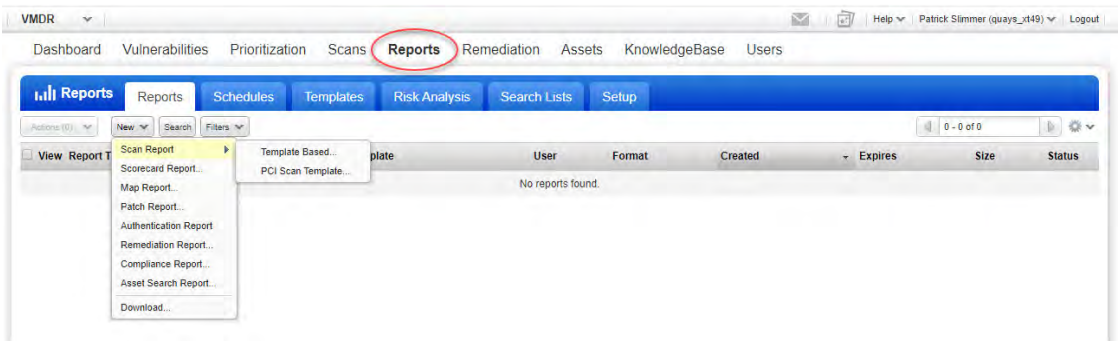
- Information about discovered vulnerabilities, and

- Filtering and sorting options to provide many different views of the data.

Launching Reports

The reporting process works in a very similar way to the scanning process. You launch a report, it runs in the background while you work on other things, you can check the status from the reports list, and when the report is complete, an email summary is sent out with a link to the saved report.

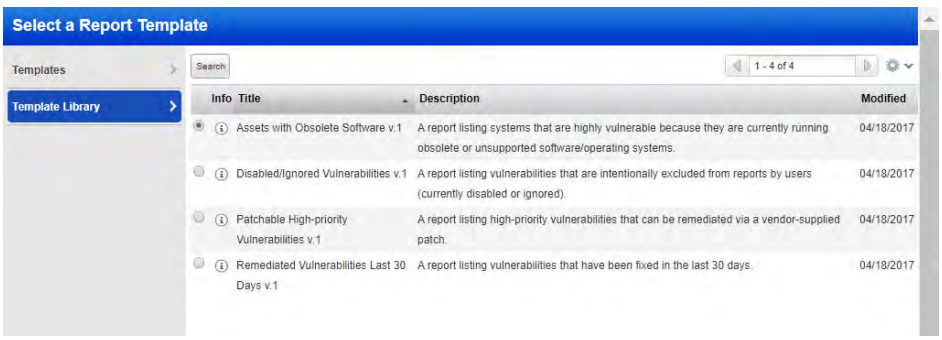
To launch a new report, go to the “Reports” tab and then go to the New menu and select the type of report you want to generate. (Don’t see this option? Go to Reports > Templates and select “Run” from the Quick Actions menu).



Follow the online prompts to provide report details like a report title, report template and report format. Click the “Select” link next to the Report Template field to select a report template. Note there are several report templates provided to help you get started.

Select a template from your account, then click the Select button (below the list).

Or select a template from our Template Library and click the Import button (below the list). You can import a template and use it as is or edit the template to suit your needs.



The hosts to include in your report (the Report Source) is selected by default from the template settings. You can overwrite this by entering values for Asset Groups, IPs/Ranges and/or Asset Tags. When you're ready click "Run" to launch the report.

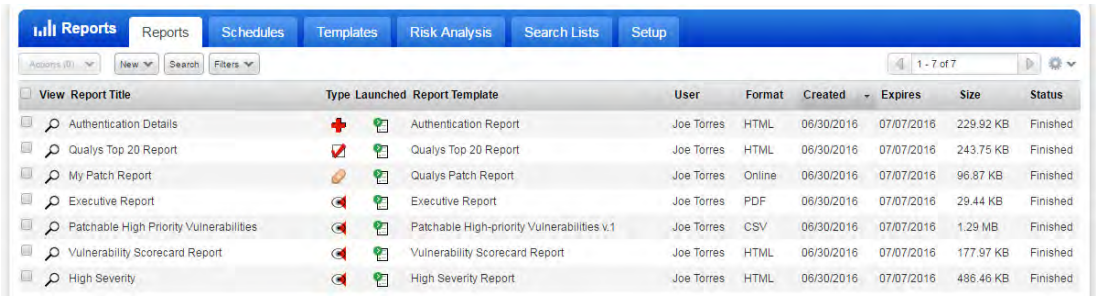
The status of your report appears in a second browser window. Close the window to let the report run in the background. You can check the status of your report at any time from the reports list, and then download the completed report once it's finished. A report completion email notification is also available. When enabled, an email is sent to you when the report is complete. The email includes a report summary and a link to the saved report.

Accessing Reports

When Report Share is enabled, users launch reports, view report status and download completed reports from the reports list according to their user roles and account settings. Additional features enable users with manager privileges to distribute reports to the right people at the right time.

To access shared reports, select "Reports" from the top menu and then select the "Reports" tab. The report history list appears. (The "Reports" tab is not visible if Report Share is not enabled. Jump ahead to Report Templates if this applies to you.)

The reports list is empty until at least one user generates a report. As reports are generated, the list is populated. The sample reports list below shows reports in various formats, created by different users at different times.



View	Report Title	Type	Launched	Report Template	User	Format	Created	Expires	Size	Status
	Authentication Details			Authentication Report	Joe Torres	HTML	06/30/2016	07/07/2016	229.92 KB	Finished
	Qualys Top 20 Report			Qualys Top 20 Report	Joe Torres	HTML	06/30/2016	07/07/2016	243.75 KB	Finished
	My Patch Report			Qualys Patch Report	Joe Torres	Online	06/30/2016	07/07/2016	96.87 KB	Finished
	Executive Report			Executive Report	Joe Torres	PDF	06/30/2016	07/07/2016	29.44 KB	Finished
	Patchable High Priority Vulnerabilities			Patchable High-priority Vulnerabilities v.1	Joe Torres	CSV	06/30/2016	07/07/2016	1.29 MB	Finished
	Vulnerability Scorecard Report			Vulnerability Scorecard Report	Joe Torres	HTML	06/30/2016	07/07/2016	177.97 KB	Finished
	High Severity			High Severity Report	Joe Torres	HTML	06/30/2016	07/07/2016	486.46 KB	Finished

Sharing Reports

Privileges to view reports in the reports list depends on each user's assigned role and assets, as defined for their user account. By default, Managers can view all reports in the subscription, Unit Managers can view all reports in their business unit, and Scanners and Readers can view their own reports.

There's more ways you can easily share reports with others:

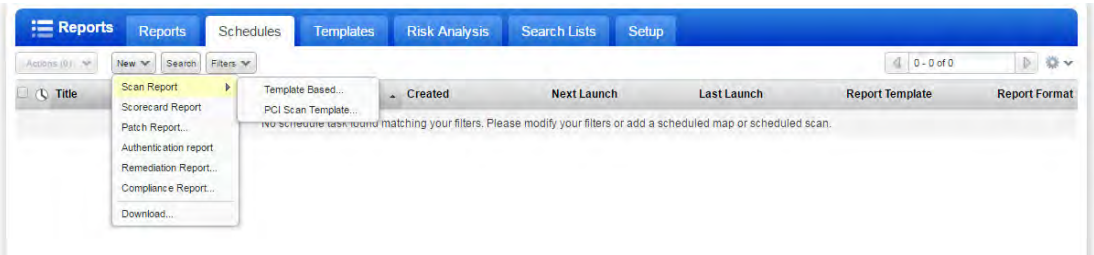
Grant Users Report Access — As a Manager user, you have the ability to grant other users access to reports that they wouldn't typically be able to see based on their user account settings. Report access can be granted for a specific report or for a scan report template.

Securely Distribute PDF Reports — As a Manager user, you have the ability to encrypt PDF reports with a password and distribute them to users via an email distribution list, including users inside and/or outside of the subscription. To do this, go to Reports > Setup > Report Share and select "Enable Secure PDF Distribution" and click "Save". The next time you launch a report with report share, you'll see the option "Add Secure Distribution". Select this option, add a report password, add custom distribution groups with email addresses, select one or more groups for the report, and then launch the report. When the report is completed, an email notification with a secure link to the report is sent to users who will be prompted to enter the report password before viewing the report.

Scheduling Reports

When Report Share is enabled, a Manager user can enable Scheduled Reporting, which allows users to schedule reports to run at specified intervals and define email distribution groups for finished reports. To enable Scheduled Reports click the "Schedules" tab. The first time you click the Schedules tab you'll see the Scheduled Reporting Setup window. Click the "I Accept" button to enable Scheduled Reporting for your subscription.

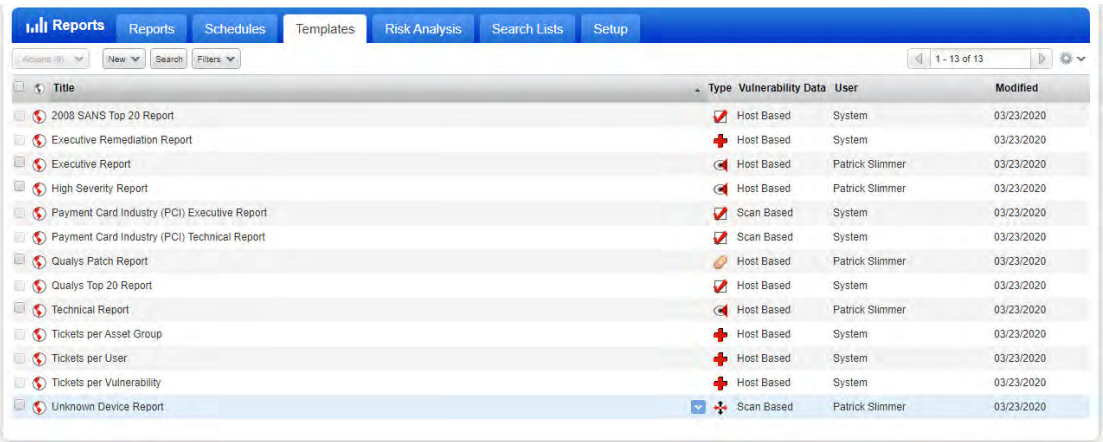
To schedule a report, go to the “Schedules” tab and then go to the New menu and select the type of report you want to schedule.



Follow the online prompts to provide report details as described above for launching a report. Select the “Scheduling” check box to define scheduling and notification options, and then click “Schedule” to save the report task. The scheduled report appears on the Schedules list and runs at its scheduled time. When the report runs, it appears on the Reports tab.

Report Templates

Your account includes pre-defined report templates to simplify report generation. Most reporting is template-based. The report template outlines what information is included in the report and how that information is displayed. To view report templates available in your subscription, select the “Templates” tab under “Reports”.

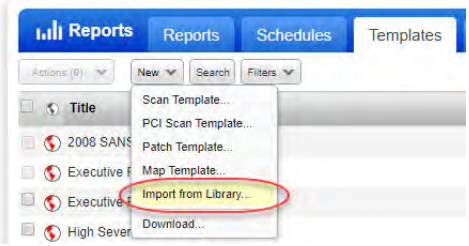


Report types are: for a scan report, for a compliance report, for a map report, for a remediation report and for a patch report.

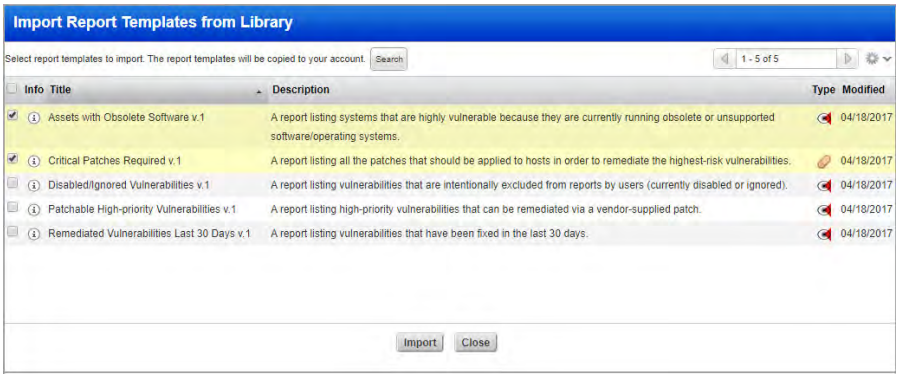
Templates Library

The Template Library provides additional report templates that you can import to your account and use as-is or edit as needed. These templates are designed to address many of your reporting requirements. You can run these report templates at any time.

You can import report templates from the Library while viewing the report templates list. Just go to New > Import from Library.



Select the check box next to each template you want, then click “Import”.



The selected templates are added to your report templates list. If there are vulnerability search lists associated with these templates, the search lists are also added to your account in the search lists data list. Once imported you can use these items as-is or edit them to suit your specific needs. The Library includes a variety of report templates, option profiles and vulnerability search lists. You can import configurations from the Library while viewing your data lists (report templates, option profiles, and search lists) and while stepping through workflows where these configurations are used. Once imported, configurations are saved in your account for viewing and editing.

Create Custom Templates

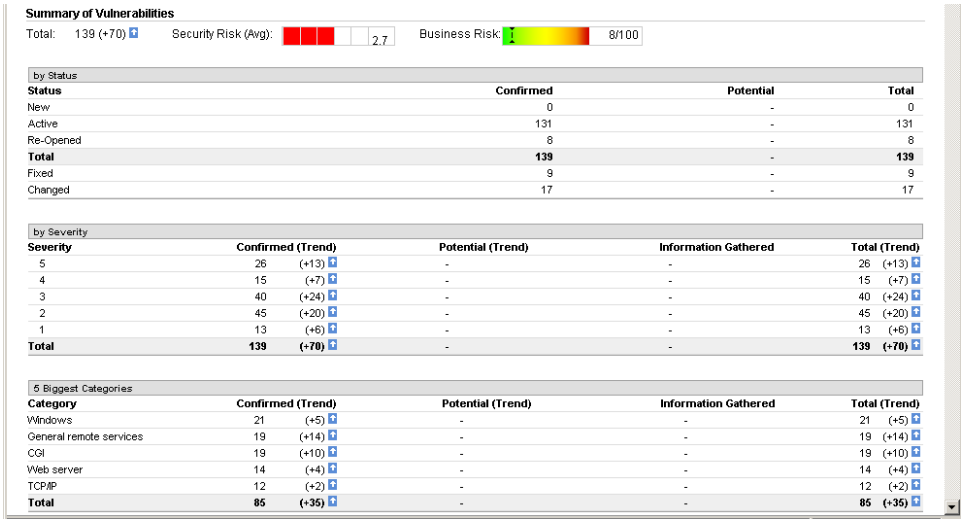
If the provided templates don’t meet your exact needs, you can create custom templates to report on the vulnerability data in your account. Go to the report templates list then select the type of template you want to create from the New menu. Select display and filter options for your report.

Scan reports can be tailored in thousands of different ways, and we suggest you try some different combinations of options to see the resulting output. On the New Template page, begin by giving your report a title, such as “First Scan Report.” Then select different report options in the Findings, Display, Filter and Services and Ports sections of the template. The User Access section allows you to grant certain users access to reports generated from this template. As you finish setting report options, the buttons at the bottom of the page allow you to Save, Save As, Test, or Cancel. You can create on-the-fly reports that give you a snapshot, or you can create templates you will use repeatedly, and therefore will want to save.

Trend Analysis and Differential Reporting

Using the scan report template, select the “Host Based Findings” and “Include trending” options under Findings and choose host targets. Then go to the Display options and select just the first two options under Graphics (“Business Risk by Asset Group over Time” and “Vulnerabilities by Severity over Time”) and then select “Test” at the bottom of the page.

The summary of vulnerabilities section reports statistics on the vulnerabilities detected:



Summary of Vulnerabilities

Total: 139 (+70) Security Risk (Avg): 2.7 Business Risk: 8/100

by Status

Status	Confirmed	Potential	Total
New	0	-	0
Active	131	-	131
Re-Opened	8	-	8
Total	**139**	-	**139**
Fixed	9	-	9
Changed	17	-	17

by Severity

Severity	Confirmed (Trend)	Potential (Trend)	Information Gathered	Total (Trend)
5	26 (+13)	-	-	26 (+13)
4	15 (+7)	-	-	15 (+7)
3	40 (+24)	-	-	40 (+24)
2	45 (+20)	-	-	45 (+20)
1	13 (+6)	-	-	13 (+6)
Total	**139 (+70)**	-	-	**139 (+70)**

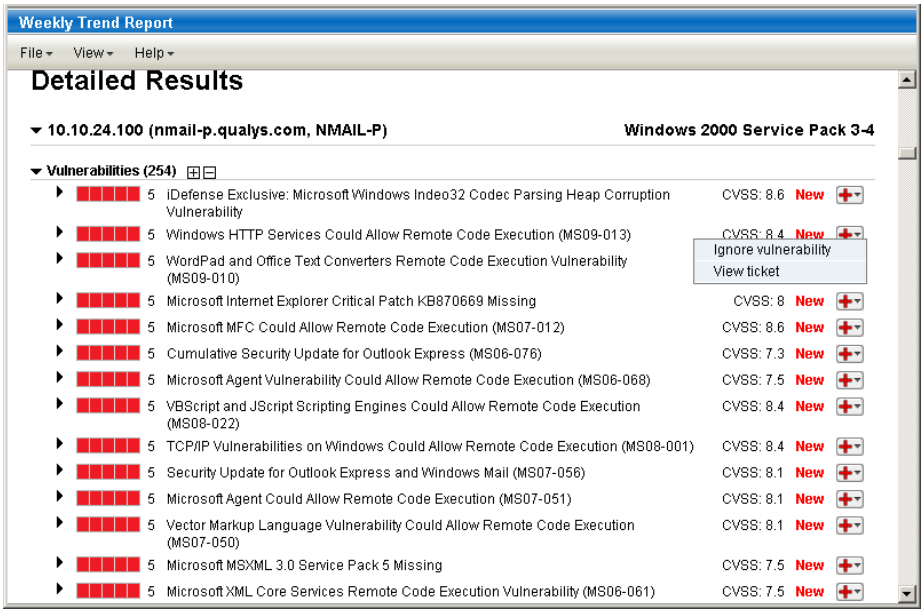
5 Biggest Categories

Category	Confirmed (Trend)	Potential (Trend)	Information Gathered	Total (Trend)
Windows	21 (+5)	-	-	21 (+5)
General remote services	19 (+14)	-	-	19 (+14)
CGI	19 (+10)	-	-	19 (+10)
Web server	14 (+4)	-	-	14 (+4)
TCP/IP	12 (+2)	-	-	12 (+2)
Total	**85 (+35)**	-	-	**85 (+35)**

Following this is the graphical depiction showing business risk by asset group over time. It also shows vulnerabilities by severity over time. This is just one simple example of how our trend analysis reporting can give you a fast overview of business risk and vulnerability trends on a given network.

Qualys allows customers to store host vulnerability data from scan results for an indefinite amount of time. This is very useful for organizations to establish a certain baseline and continue to reference it in order to measure progress. Sample graphs are below.

Detailed Results follow the report graphics. The current status (New, Active, Re-Opened or Fixed) appears for each vulnerability detected on the host. A sample detailed results list is below:



Taking Remediation Actions

There are several remediation actions you can perform directly from scan report with host based findings. In the Detailed Results section, place your cursor over the red cross ( ) and then select an action from the drop-down menu.

Ignore/Activate options:

Ignore vulnerability - This causes the vulnerability to be filtered out of scan reports, host information, asset search results and your dashboard. This action also closes associated remediation tickets for the vulnerability/host/port. (Ignored vulnerabilities always appear in scan reports with scan based findings.)

Activate vulnerability - This option activates an ignored vulnerability on the host. (To take this action your report filter settings must be set to display ignored vulnerabilities.)

Ticket related options:

Create ticket - This will create a new remediation ticket for the host/vulnerability/port. You'll be prompted to specify who the ticket should be assigned to and when the ticket should be resolved. The ticket creation is logged in the ticket history with the name of the user who created the ticket and a time stamp for when the action took place.

View ticket - This will show you ticket information, if a ticket exists for the host/vulnerability/port. From the File menu, click Edit to resolve or close-ignore the ticket, reassign the ticket to another user or add comments to ticket details.

It is best practice to create one or more remediation policies for the subscription to automate the ticket creation process. With a remediation policy in place, tickets are created automatically by the service when detected vulnerabilities match conditions specified in policy rules.

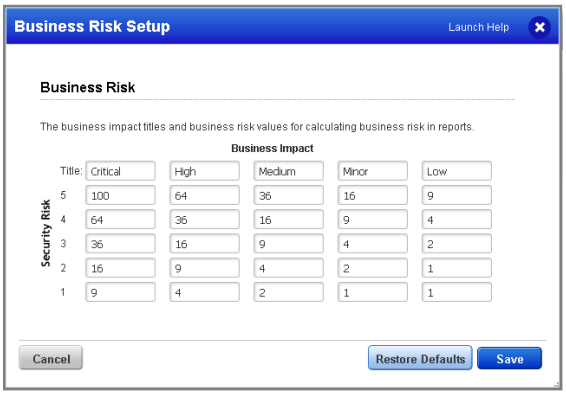
Business Risk Reporting

One of the key functions of a Vulnerability Management solution is remediation reporting and tracking. To do this in the most efficient way, there needs to be some way of associating network assets with various business operations, so that the severity of vulnerability is correlated with business security exposure in order to arrive at a metric for business risk.

Qualys automates business risk reporting while enabling users to tailor it to their enterprise. The system provides a default definition, but it also allows users to modify it to better reflect their own internal metrics.

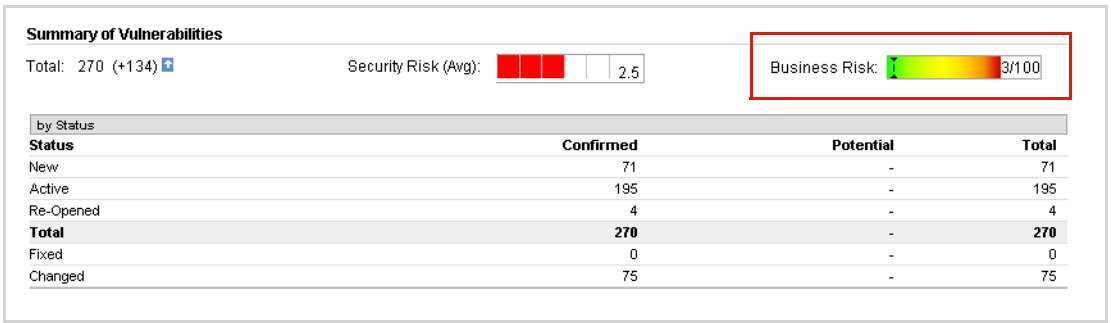
You customize the business risk calculations by going to Reports > Setup > Business Risk. The Business Risk Setup page will appear defined by a matrix with Business Impact columns and Security Risk rows.

So, for example, a security risk of 5 has a business risk of 9 if the asset is associated with a Low impact business operation. On the other hand, it would have a business risk of 100 if associated with a Critical impact operation. The Business Risk Setup page below illustrates this.



You can assign Business Impact values to any asset group you have created. To do this, you select the "Asset Groups" tab under "Assets". Here you will see the asset groups listed along with their IPs, domains, business impact, user, and last modified date. You can change the business impact definition by selecting Edit from the Quick Actions menu, selecting the "Business Info" tab, then setting the Business Impact level. Change it to some other identification, so if it was "Critical," change it to "Medium". Afterward, select "Save".

Note how changing the Business Impact level changes the previous trend and status report results, particularly the Business Risk metric:



CVSS (Common Vulnerability Scoring System)

Qualys displays CVSS v2 and CVSS v3 scores in reports. CVSS was commissioned by the National Infrastructure Advisory Counsel (NIAC) and is currently maintained by FIRST. CVSS is widely supported by security organizations and vendors including: CERT, Mitre, Cisco, Symantec, Microsoft and Qualys.

Want to display CVSS scores in scan reports? First enable the CVSS Scoring feature for the subscription. Go to Reports > Setup > CVSS. Then select the "Enable CVSS Scoring" check box and click "Save". Once enabled, CVSS scores will be calculated for vulnerability/host pairs and displayed in scan reports.

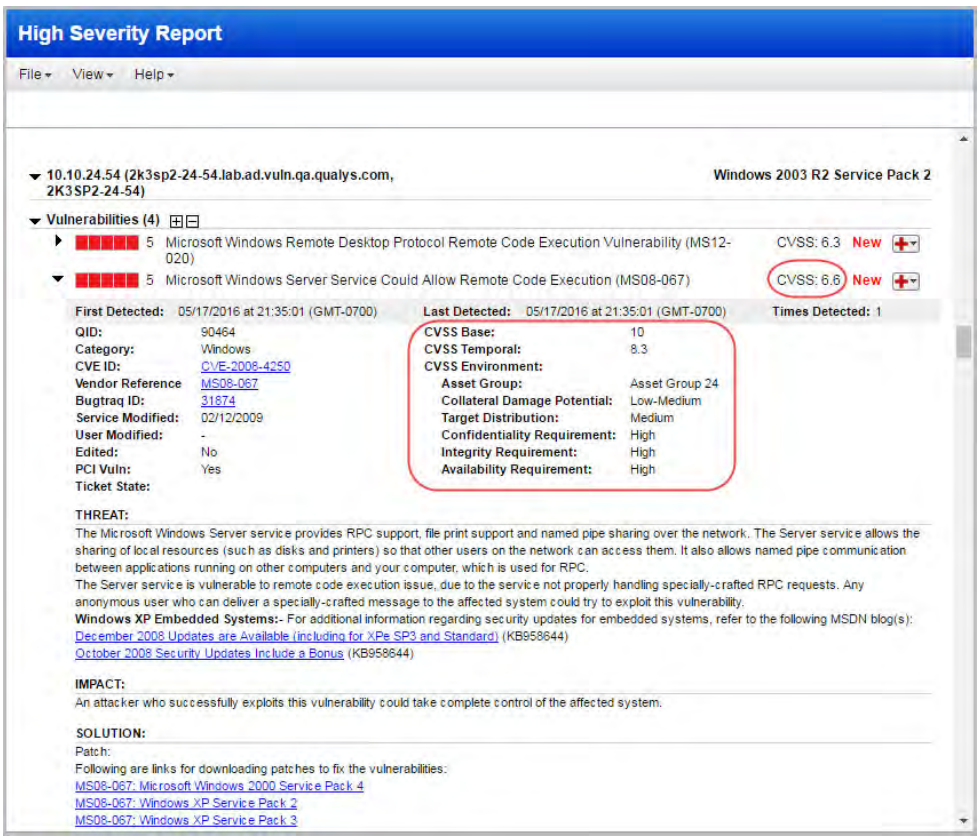
The following values are needed to calculate a CVSS score for a vulnerability:

CVSS Base Score - The Base score measures the fundamental, unchanging qualities of a vulnerability. When the final CVSS score is calculated, the Base score is modified by the CVSS Temporal score and Environmental metrics. The Base score is provided by the service and assigned to vulnerabilities.

CVSS Temporal Score - The Temporal score measures the time dependent qualities of a vulnerability, which may change over time. The temporal score allows for mitigating factors to reduce the overall CVSS score for a vulnerability. The Temporal score is provided by the service and assigned to vulnerabilities.

CVSS Environmental Metrics - The CVSS Environmental Metric group captures the characteristics of a vulnerability that are associated with the user's IT environment. Users define environmental metrics in asset groups. The metrics apply to all hosts in the asset group.

In the sample scan report below, a final CVSS score of 6.6 is displayed for QID 90454 on IP 10.10.24.54. See the vulnerability details for the CVSS Base and Temporal scores assigned to the vulnerability and the CVSS Environmental metrics assigned to the host's asset group.

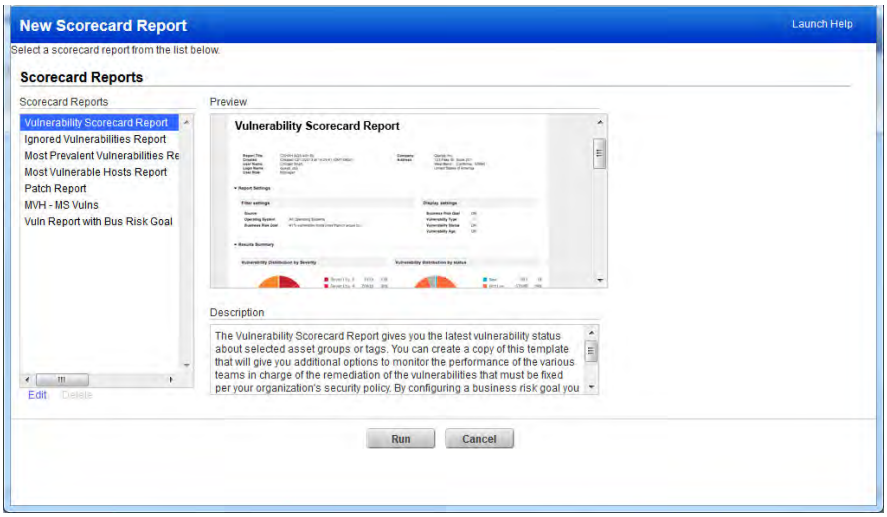


Scorecard Reports

Qualys provides template-based scorecard reports that can be used to communicate the state of security within the enterprise directly to persons in charge of security operations and business line owners.

Scorecard reports provide vulnerability data and statistics appropriate for different business groups and functions. By configuring scorecard reports to use different views and asset groupings, you can create multiple reports based on the same data satisfying both security operations personnel and business line leaders. You can then share each generated report with the people who need it in a format that is meaningful to them.

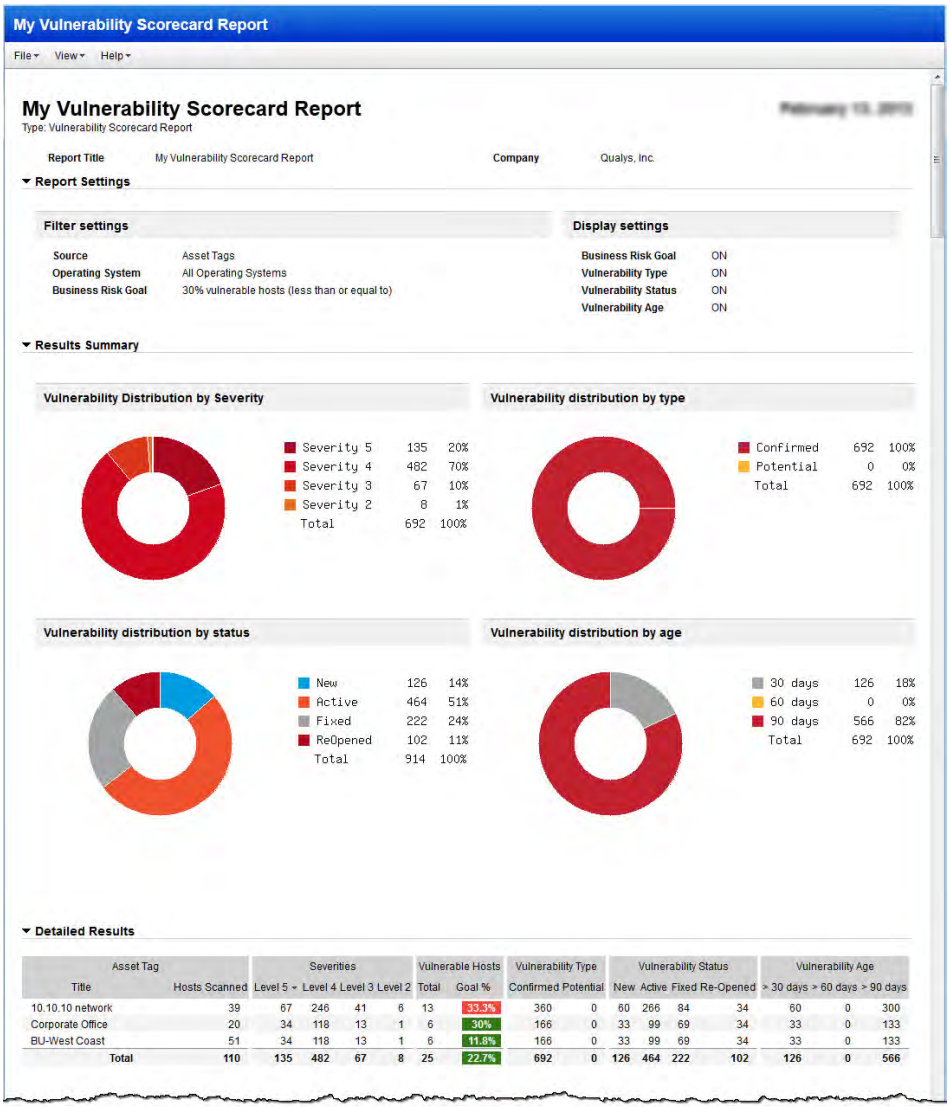
To run a scorecard report, go to VM/VMDR > Reports and select New > Scorecard Report. Select a report template on the left and then click Run to run the report.



You'll be prompted to select hosts to report on and a report format. You can select hosts by asset group, asset tag or business unit. Asset tags can be selected when Asset Tagging has been added to your account and you have accepted the New Data Security Model (go to Users > Setup > Security for information).

Do you want to create custom templates? Simply select a template title and then click Edit (under the list) and enter settings. Once saved you can run the template to create your report.

A sample Vulnerability Scorecard Report is shown below.



In the Detailed Results you see the % of hosts that are vulnerable for each asset tag included in the report. The pass (green) and fail (red) status is determined by the Business Risk Goal setting in the scorecard report template.

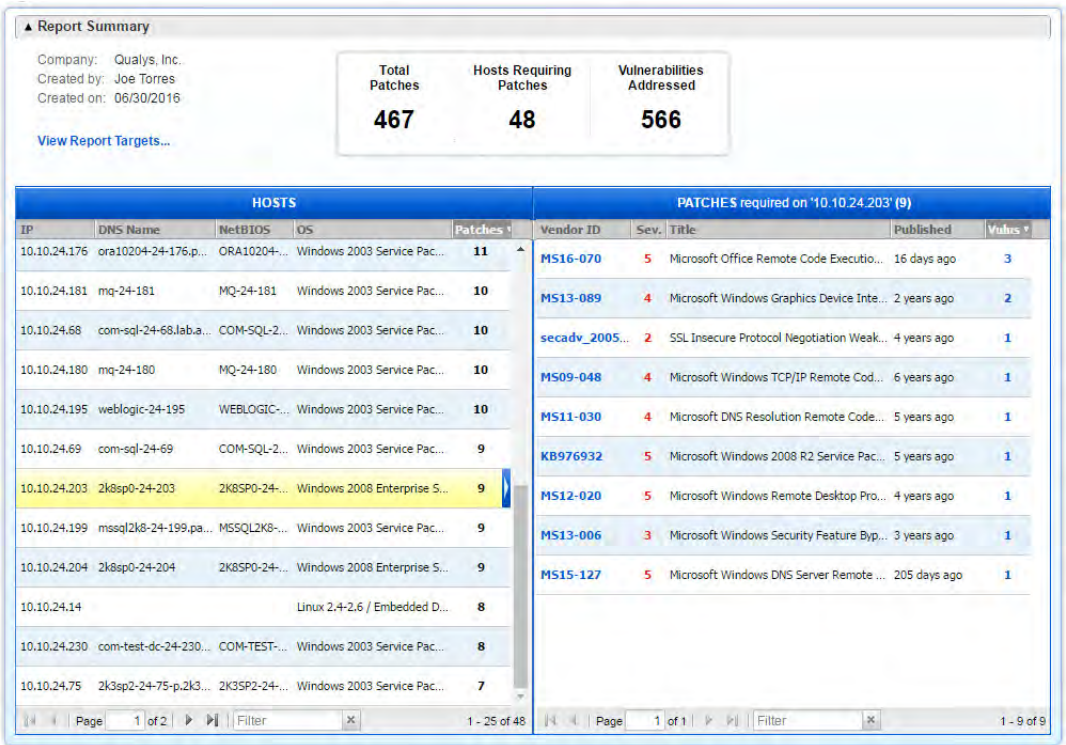
Patch Reports

The Qualys Patch Report is a new feature that helps you streamline the patching process and improve remediation efficiency. The patch report leverages standard Qualys capabilities to provide accurate, actionable and focused reports so you can quickly and efficiently remediate vulnerabilities without applying unneeded, redundant patches.

For the most accurate results in your patch report, be sure that authenticated scanning is used to scan the target hosts. Using authenticated scanning allows the scanning engine to collect the most detailed information about each target host including the host's operating system. When this information is in your account, the service identifies the most appropriate missing patch(es) in your patch report.

Your patch report can be saved in these formats: PDF, CSV and Online Report - this gives you an interactive report with numerous navigation options.

A sample Online Patch Report is shown below. This report was generated using the template “Qualys Patch Report” provided by Qualys. In this report patches are grouped by host. The report summary shows: 467 total patches need to be applied to fix the vulnerabilities on the target hosts, 48 hosts require patches to be applied, and 566 vulnerabilities will be addressed by applying the patches in the report. Host 10.10.24.203 needs 9 patches applied and you can see details on these patches in the right pane.

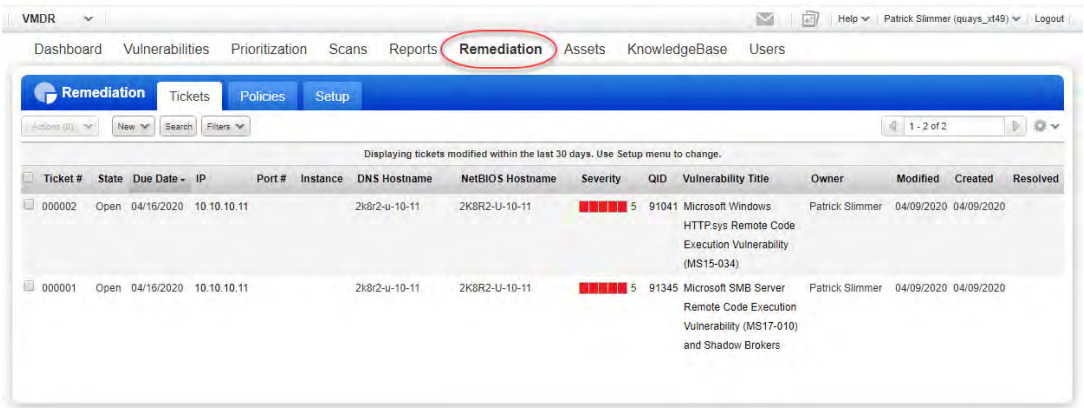


Reporting Summary

Qualys's highly flexible, comprehensive reporting capabilities distinguish it from other Vulnerability Management solutions. Report Share functionality provides Enterprise users with a centralized location for sharing reports with other users. Template based reports and Scorecard reports are available for reporting on vulnerability scan data in your account. The Qualys Patch Report helps you streamline the patching and remediation process. The Template Library includes pre-defined report templates that you can import and use as is or edit as needed.

Remediation Summary

Qualys provides a remediation process that allows you to close the loop in your Vulnerability Management process. This is done with powerful capabilities, such as automatic ticket generation, that separates Qualys from other solutions. User defined policy rules define the conditions that must be met for a ticket to be created (what vulnerabilities detected, on what assets). Tickets are auto created and you'll see Open tickets assigned to you. By default tickets are closed once the vulnerability is confirmed fixed in subsequent scan.



Wait, there's more!

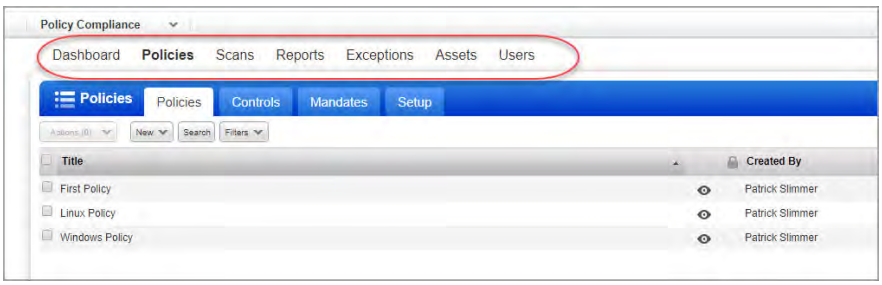
Thank you for evaluating the Qualys Cloud Platform! There's more you can explore.

Policy Compliance

Qualys Policy Compliance (PC) supports auditing host configurations and measuring their level of compliance with internal and external policies based on the latest security benchmarks and standards and centrally tracking compliance status of all your assets.

Qualys also offers Qualys Security Configuration Assessment (SCA) - this is a lightweight service that can quickly perform the configuration assessment of IT assets and centrally track compliance status of all your assets on basis of CIS hardening benchmarks.

To access policy compliance features, select the Policy Compliance application from the picker. You'll see PC workflows along the top menu.



Get informed quickly with video tutorials.

Video Tutorials

Policy Compliance Video Library

Looking for something more? Check out these resources.

User Documentation

Policy Compliance Getting Started Guide

Security Configuration Assessment Getting Started Guide

Add Cloud Agents

Qualys Cloud Agent (CA) extends your security throughout your global enterprise. These lightweight agents are remotely deployable, centrally managed and self-updating. They collect the data and automatically beam it up to the Qualys Cloud Platform, which continuously analyzes and correlates the information in order to help you identify threats and eliminate vulnerabilities.

CA lets you get data for all kinds of assets - on your on-premise systems, dynamic cloud environments and mobile endpoints.

Get informed quickly with video tutorials.

Video Tutorials

Cloud Agent Video Library

Looking for something more? Check out these resources.

User Documentation

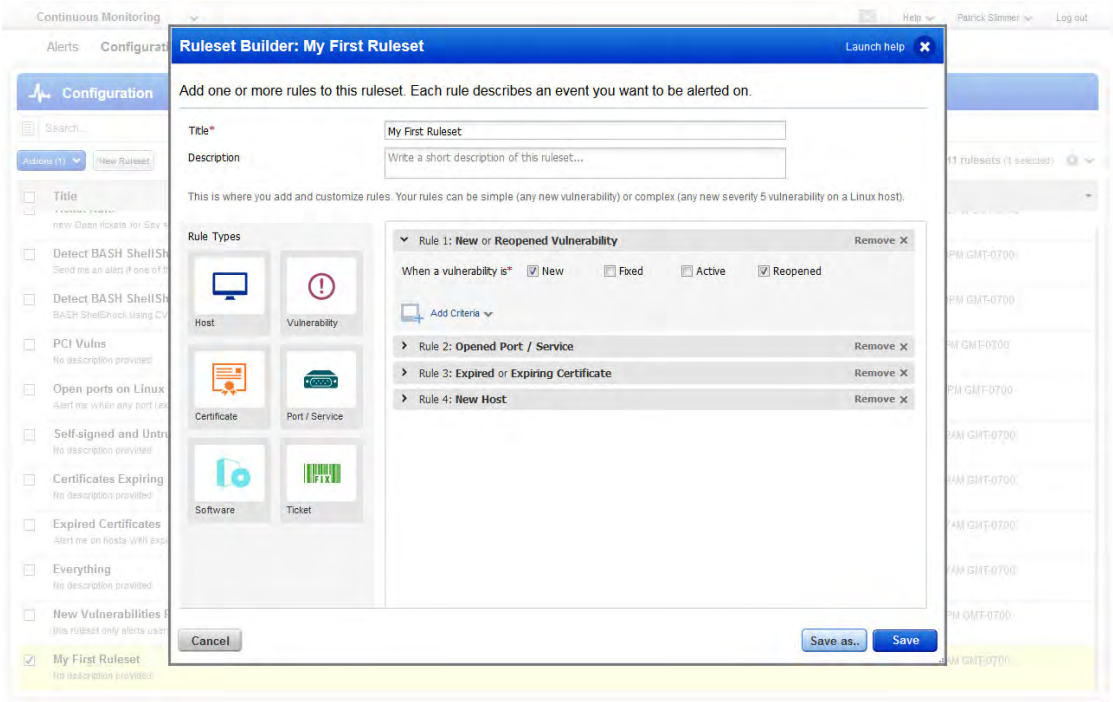
Cloud Agent Getting Started Guide

Cloud Agent API User Guide

Get Real-Time Security Alerts

Qualys Continuous Monitoring (CM) sends new security alerts when certain information is found by the Qualys Cloud Platform. You can choose to track changes on hosts, vulnerabilities and more.

It's easy to get started! Jump over to the Continuous Monitoring app. You'll create a ruleset (what you want to be alerted on) and a monitoring profile (which hosts you want to monitor and who should be notified). Alerts will be generated as soon as scan results are processed.



Get informed quickly with video tutorials.

Video Tutorials

Compliance Monitoring

Scan Your Web Apps and APIs for Vulnerabilities

Web apps, often plagued by vulnerabilities and misconfigurations due to poor coding and faulty hardening policies, can be put on your network by almost anyone. Large organizations have hundreds, even thousands of apps. Qualys WAS gives you visibility and control by finding official and "unofficial" apps throughout your environment, and letting you categorize them.

Unsafe web applications and APIs offer hackers an attractive attack surface and convenient entry point into your IT environment. When breached, web apps can expose massive amounts of confidential business data. Qualys WAS protects you with incisive, thorough, precise scans, scaling up to thousands of web apps and with few false positives. Detects OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection.

Get informed quickly with video tutorials.

Video Tutorials

Web Application Scanning Video Library

Looking for something more? Check out these resources.

User Documentation

WAS Getting Started Guide

WAS API User Guide

Support and Training

Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Free Training and Certification

Browse our Training video library and take online self-paced training for free.

Training and Certification

Our Online Community

Learn from other security professionals like yourself.

Qualys Community

Looking for user guides?

Download API guides, Scanner Appliance guides, Quick Starts, and more.

Qualys Documentation

New Feature Announcements and Platform Status

These additional resources will help you stay informed about new features, API changes and platform status.

Release Notes

New Feature Announcements on Qualys Blog

API Notifications

Platform Status