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 by email at support@qualys.com or by phone at +1 (866) 801 6161.

Again, thank you for evaluating the Qualys Cloud Platform.

Sincerely,

Qualys, Inc.
Table of Contents

Getting Started ................................................................................................................................. 6
Key Features of the UI ........................................................................................................................... 7
Account Setup ........................................................................................................................................ 9
Installing Your Scanner Appliance ........................................................................................................ 9
Creating Network Domains .................................................................................................................. 9
Adding Hosts for Scanning .................................................................................................................... 9
Asset Management............................................................................................................................... 10
User Management ................................................................................................................................. 11
You’re Now Ready ................................................................................................................................ 14

Step 1: Mapping Your Network .......................................................................................................... 15
Running a Map ....................................................................................................................................... 15
Map Results .......................................................................................................................................... 17
Scheduling Maps ................................................................................................................................... 19
Map Targets .......................................................................................................................................... 19
Comparing Maps ................................................................................................................................... 20
Mapping Summary ............................................................................................................................... 21

Step 2: Scanning for Vulnerabilities .................................................................................................... 22
Starting a Scan ........................................................................................................................................ 23
Scan Status ........................................................................................................................................... 25
Scan Results .......................................................................................................................................... 27
Scheduling Scans ................................................................................................................................... 30
Scanner Parallelization ........................................................................................................................... 31
Selective Scanning using Search Lists .................................................................................................... 31
PCI Scans and Compliance ....................................................................................................................... 32
Vulnerability KnowledgeBase .................................................................................................................. 35
Scanning Summary ................................................................................................................................ 36

Step 3: Search, View, Prioritize ............................................................................................................ 37
Your VM Dashboard ............................................................................................................................... 37
AssetView - Search All of Your Assets, All in One Place ........................................................................ 38
Prioritize Vulnerabilities and Active Threats ........................................................................................ 39

Step 4: Reporting .................................................................................................................................... 40
Launching Reports ................................................................................................................................. 40
Accessing Reports ................................................................................................................................. 42
Sharing Reports ...................................................................................................................................... 42
Scheduling Reports ................................................................................................................................. 43
Trend Analysis and Differential Reporting ............................................................................................ 45
Scorecard Reports ................................................................................................................................. 50
Patch Reports ......................................................................................................................................... 52
Reporting Summary .............................................................................................................................. 53

**Step 5: Remediation** ...................................................................................................................... 54
Remediation Policy .............................................................................................................................. 54
Ticket Creation .................................................................................................................................... 56
Remediation Reporting ....................................................................................................................... 58
Remediation Ticket Update Notification .............................................................................................. 59
Remediation Summary .......................................................................................................................... 59

**Step 6: Compliance Security** ....................................................................................................... 60
Policy Compliance Workflow .............................................................................................................. 60
Accessing Policy Compliance Features ............................................................................................. 62
Policy Compliance Summary .............................................................................................................. 63

**Wait, there’s more!** ....................................................................................................................... 64
Add Cloud Agents ............................................................................................................................... 64
Get Real-Time Security Alerts .......................................................................................................... 64

**Contact Support** .......................................................................................................................... 65
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. First time users will be presented with a window to review the Qualys Terms and Conditions (Ts&Cs). Upon accepting the Ts&Cs, you will now be presented with a Welcome screen with a few simple steps to get your first scan running.

At any time you can return to this Welcome page by selecting Quick Start Guide from the menu that appears below your user name. You can select Home Page from this same menu to change the first page that appears when you log in.
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 to you 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 to work in, you’ll see a set of menu options across the top of the screen representing the main sections within the application. Each section provides workflows that are specific to the application you’re in.

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 in a data list 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 > 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. 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.

**Asset Management**

Asset management capabilities provide powerful tools to manage and organize assets.

You can organize assets (scanner appliances, domains and hosts) into asset groups and business units, assign them business impact levels, and so on. 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.

**Tip** - 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:

1. Start with all assets in the subscription.

2. Split assets into logical asset groups.

3. (Optional) Organize asset groups into business units.

**User Management**

User management capabilities allow you to add multiple users with varying roles and privileges.

The most privileged users are Managers and Unit Managers. These users have the ability to manage assets and users. The main difference between Managers and Unit Managers is that Managers have management authority for the subscription (including any business units it may have), while Unit Managers have management authority on an assigned business unit only.

Scanners and Readers have limited rights on their assigned assets. Readers cannot run maps and scans, however they can view scan and map results, run reports, and view/edit remediation tickets.

Auditors may be added to a subscription when the policy compliance application is enabled in order to perform compliance management tasks. These users have limited rights on hosts that have been defined as compliance hosts for the subscription. Auditors cannot run compliance scans, however they can define policies, create policy report templates and run reports based on compliance scan data.
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 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, VIP will be ignored and SAML SSO will be used. (Tip: Managers can require VeriSign VIP or SAML SSO for all users by going to Users > Setup. For VeriSign VIP, select Security. For SAML SSO, select SAML SSO Setup.)

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.
Step 1: 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 on the next page.
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. Note that the menu “Scanner Appliance” appears when your account includes a scanner appliance. When present, select the name of your scanner appliance (required for mapping private use internal IPs) or External for the 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 above, the domain “qualys-test.com” is selected. (Note that 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, you will see the status change 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. Some of the hosts are scannable, meaning that 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.
Comparing Maps

You can easily run multiple maps over some arbitrary time period and immediately see both anticipated and unanticipated changes. You can also compare maps against approved hosts, a user-defined list of hosts approved for a domain.

Configure an Approved Hosts List

Compare saved map results to a customized list of approved hosts for a domain to identify hosts that are not in the list. There can be one approved hosts list per domain. To configure an approved hosts list, go to the “Assets” section and select the “Domains” tab.

Identify the domain you’re interested in, and select “Edit” from the Quick Actions menu. For Managers, the Edit Domain page appears. Click “Configure” next to Approved Hosts to view the Configure Approved Hosts page. For Unit Managers, Scanners and Readers, this page appears automatically.

You’ll see a simple text field where you can directly enter IPs/ranges or paste them in. Not sure which IPs are available? Click “Select IPs/Ranges” for a list of IPs. Then use the search option to quickly find IPs based on a full or partial IP address. Click “Select Asset Group” to add hosts from one or more assets groups in your account. Click “Select Map” to add all detected devices from one or more saved maps. The IP addresses for all devices, including systems, routers, and servers, identified in the map will be added to the approved hosts list. You can then remove individual IPs. Now click “OK” to save the approved hosts list for the domain.
Generate the Unknown Device Report

Generate the “Unknown Device Report” to compare the approved hosts list for a domain with saved map results. Any host that is not in the approved hosts list is considered “rogue” and will appear in the report. To run this report, select “Reports” on the top menu to go to the Reports section. Then go to New > Map Report. Click the “Select” link next to the Report Template field to select the “Unknown Device Report” template. Then select the domain you want to report on and choose 1 or 2 saved map results to compare against the approved hosts for the domain. Select “Run” to start the report. A sample “Unknown Device Report” is shown below:

![Unknown Device Report](image)

Note the status indicators (Active, Added and Removed) in the Status column. These indicators appear when 2 maps are included in the 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.
Step 2: 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 and MySQL. For compliance scans the service also supports MS SQL, Sybase, Checkpoint Firewall, MS IIS, Apache Web Server, IBM WebSphere App Server, Tomcat Server and Oracle WebLogic Server. When enabled, we have the ability to gather more system intelligence on target hosts. For vulnerability scans, trusted scanning is optional.

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 the “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.
Evaluator's Guide
Step 2: Scanning for Vulnerabilities

1) Scan Status Icons. A solid icon (filled-in) means all results available for the scan have been processed, meaning the host scan data (Auto data) has been updated throughout the application, and these results are available for reporting. A hollow icon means results processing is in progress. When a scan is finished and the results have been processed, you’ll see 🔄. If the 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. For a vulnerability scan you also see the number of vulnerabilities detected. A summary statement gives you the status of the scan and whether the results have been processed. In the example above, the scan is finished and all results from the scan have been processed. There were a total of 3 hosts scanned and 6 vulnerabilities detected. 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 this link to see the current status of the scan and details about scanner usage, including which scanners were used to scan target hosts. Note that the Scanners section is only visible in accounts with New Scanner Services enabled.

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. In the following example, the external scanner with IP 10.10.21.120 was used to scan 3 hosts. When a scanner appliance is used, the scanner’s friendly name appears.

![Scan Status (scan/1349210722.43809)](image)

4) View Results. Click this link to open the Scan Results report. You’ll notice that you can also get to the results by clicking the View Results button in the Scan Status window.
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.
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 162 confirmed vulnerabilities associated with IP address 10.10.25.31 running Windows Server 2003 R2 Service Pack 2.
If you click on the title of a vulnerability, you’ll see a comprehensive description of the vulnerability, including threat, impact, solution, compliance and result details.

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 and malware information is shown below.
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 from 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.

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 > Scan. 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

To share a completed PCI scan with your PCI Merchant account follow these simple steps:

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 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. We’ll share (import) the scan to your PCI account. (We’ll add to your PCI account any scanned IPs not already in the account.)

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 > Scan. 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. We use the vulnerability risk rankings High, Medium and Low. By default these are set to the same CVSS scores as required for ASV external PCI scans. Under PCI Risk Ranking, you need to define a custom risk ranking scale by modifying the CVSS base score ranges for High, Medium and Low ranking vulnerabilities. Be sure to create a template for each ranking scale within your organization.

Then you’re ready to create one or more reports, depending on the number of templates you have. To 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.
- ⋄ ⚔ 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.
Evaluated Guide
Step 2: Scanning for Vulnerabilities

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 functionality. For more information, refer to the Policy Compliance Getting Started Guide and the Web Application Scanning Getting Started Guide. These guides are available for download from within your user account in the Resources section (Help > Resources).
Step 3: 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.

Your VM Dashboard

Easily find out where your IT systems are vulnerable to the latest threats & how to protect them. Your VM dashboard provides a quick one-page, printable summary of your overall security posture based on the current vulnerabilities in your account. These include vulnerabilities detected by the most recent scans on the hosts in your account. For each current vulnerability the service assigns the status of New, Active or Reopened. As new vulnerability scan results become available, the dashboard is updated automatically to keep your status up to date.

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

Configure Your Dashboard

Users have privileges to configure their personal dashboard. Click the Configure link to only display the vulnerabilities and potential vulnerabilities you’re interested in. Note that disabled and ignored vulnerabilities are not included in your dashboard.
Launch and Schedule Scans from Your Dashboard

The VM dashboard gives users the ability to immediately launch and schedule vulnerability scans directly from the dashboard. Simply click the New Scan button or the Schedule Scan link.

AssetView - Search All of Your Assets, All in One Place

AV gives you a centralized location where you can view and query all of your asset data instantly. It brings security and compliance information together in one place, and lets you visualize your asset data in many ways.

Just choose AssetView from the module picker and go to “Dashboard”. You can create multiple AV dashboards and switch between them. Each dashboard has a collection of widgets showing asset data of interest.

Tips:
- Click the Add Widget button to add a preconfigured widget or create your own. You’ll select asset data, a search query and layout - count, table, bar graph, pie chart.
- Resize any widget vertically or horizontally, and drag & drop widgets on the page.
- Refresh a widget to see the latest asset data.

Video Tutorials

Introducing AssetView (3m 4s)
Prioritize Vulnerabilities and Active Threats

Threat Protection (TP) helps you visualize and assess active security threats for all of your assets all in one place! Real-Time Threat Indicators (RTI) are correlated per vulnerability automatically for you. This lets you quickly find all about asset exposed to these threats.

Go to “Dashboard” to see your threat exposure, leverage saved searches, and fix priority vulnerabilities quickly. Add widgets with search queries to see exactly what you’re interested in.

Tips:
- You can personalize the default dashboard - add widgets, resize them, move them around to change the layout.
- Click any graph, or widget with number of impacted assets, and jump to details on those assets.
Step 4: Reporting

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. There are few, if any, mechanisms for filtering, regrouping, or synthesizing the data into higher levels of information abstraction. Qualys reports, on the other hand, like quality business intelligence reporting, permit filtering and sorting that allows data to be viewed in different ways.

Qualys reports consist of the following basic components:

- Network assets (IPs and/or Asset Groups) 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.

Report Share functionality provides enhanced reporting capabilities for large amounts of report data, and promotes collaboration and sharing of reports. Users can run reports once and share them with other users. Each report is saved for 7 days. Report Share functionality is enabled for Enterprise accounts automatically.

Launching Reports

With Report Share, 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 (and click the Select button under the list).

Or select a template from our Template Library and click the Import button. You can import a template and use it as is or edit 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.

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. To do this, go to New > Import from Library. The Import Report Templates from Library page appears.

Select the check boxes next to the templates 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:

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. See the next chapter on Remediation, starting on page 54.

**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.


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.

### High Severity Report

<table>
<thead>
<tr>
<th>QID</th>
<th>Category</th>
<th>CVSS Base</th>
<th>CVSS Temporal</th>
<th>CVSS Environment</th>
<th>Asset Group</th>
<th>Collateral Damage Potential</th>
<th>Confidentiality Requirement</th>
<th>Integrity Requirement</th>
<th>Availability Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>90454</td>
<td>Windows</td>
<td>8.5</td>
<td>6.6</td>
<td>High</td>
<td>Asset Group 24</td>
<td>Low-Medium</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

The Microsoft Windows Server service provides RPC support. The print support and named pipe sharing over the network. The Server service allows the sharing of local resources (such as drives and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC. The Server service is a vulnerable remote code execution issue, due to the service not properly handling specially-crafted RPC requests. Any anonymous user who can define a specially crafted message to the affected system could try to exploit this vulnerability.

**Impact:**
An attacker who successfully exploits this vulnerability could take complete control of the affected system.

**Solution:**
Patch. Following are links for downloading patches to fix the vulnerabilities:

- [MS08-067: Microsoft Windows 2000 Service Pack 4](https://support.microsoft.com/en-us/kb/892514)
- [MS08-067: Windows XP Service Pack 2](https://support.microsoft.com/en-us/kb/892514)
- [MS08-067: Windows XP Service Pack 3](https://support.microsoft.com/en-us/kb/892514)
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 > 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.
Step 5: Remediation

Discovering all network assets, scanning various assets for vulnerabilities, and reporting what was found are all critical aspects of Vulnerability Management. As the last piece, having now found those vulnerabilities, you need to eliminate or mitigate them.

Qualys provides a remediation ticketing capability similar to trouble tickets created by a support call center. You, as a manager, can control the policies surrounding such tickets, and assign the responsibility for fixing them. Qualys will note when tickets have been created, and will track in subsequent scans any remediation changes. Manual trouble ticket creation does not scale in an enterprise network with thousands of hosts and vulnerabilities. Therefore, this process is automated via remediation policies, allowing customers to automatically create tickets upon scan completion and assign them to the appropriate user within the organization. Additionally, customers can automate trouble ticket integration into their helpdesk systems using the Qualys API.

Note: Remediation features are not available to Express Lite users.

Remediation Policy

Remediation tickets are created automatically when there’s at least one policy rule in place. The rules in your remediation policy determine how tickets will be created and to whom tickets will be assigned. A sample policy with multiple rules is shown below:

Unit Managers may be granted permission to create business unit specific remediation policies. The rules for business unit policies may be seen under the column Business Unit. The ones displayed as Unassigned are rules for the global policy, created by managers for the subscription.

To allow a Unit Manager to create a business unit remediation policy, edit the user’s account under “Users”. Under Permissions you can check the “Create/edit remediation policy” check box and save the change.
Policy rules use vulnerability search lists to define the conditions that must be met for a ticket to be created. There are two types of search lists: static and dynamic. A static search list includes a specific list of vulnerabilities (QIDs). A dynamic search list consists of a set of vulnerability search criteria (severity levels, CVSS scores, patch availability, products, vendors, etc). When a dynamic search list is used, the service dynamically compiles a list of QIDs based on the criteria defined in the list. Dynamic search lists are updated automatically by the service as new QIDs are added to the KnowledgeBase. Several search lists are provided by the service. You can also create custom search lists for specific purposes.

To create a vulnerability search list, select “Search Lists” from the Scans, Reports or KnowledgeBase section. Then go to New > Static List or New > Dynamic List. For now, let’s create a dynamic search list with confirmed severity levels 4 and 5. In the New Dynamic Vulnerability Search List page, give the search list a title and then select the severity levels in the Criteria section. Click “Save” to save the search list. Saved vulnerability search lists may be used in remediation policy rules, option profiles and scan report templates. We’re now going to create a remediation policy rule using the new dynamic search list.

When you go to the Remediation Policies list for the first time there are no rules. Create policy rules appropriate to the organization’s existing security policy. To do so, go to “Remediation” and select the “Policies” tab. Then go to New > Rule. On the New Rule page, give the rule a title, such as “First Rule”. In the Conditions section, specify the hosts the rule applies to. Then add one or more saved search lists to the rule.
Now go to the Actions section. You may choose to assign tickets to a specific user, to the user who launched the scan resulting in the ticket (the default) or to the user who owns the host. Optionally, select “Create tickets - set to Closed/Ignored” if you want to close and ignore tickets created when the rule conditions are met, or select “Do not create tickets” if you never want tickets created when the rule conditions are met. Click “Save” after making your selections.

The new rule will now show up in the remediation policies list as “First Rule”. The sample rule above results in tickets being created when vulnerability severity levels 4 and 5 are detected. The tickets will be assigned to the user who launched the scan resulting in the detection.

**Ticket Creation**

Now that you have explored the remediation capabilities and created a remediation policy, you are ready to run a scan to create tickets. Launch a scan as you did before. See Starting a Scan for assistance.

When your scan completes, go to the tickets list by selecting “Remediation” on the top menu, and then the “Tickets” tab. Tickets that are in “Open” state and assigned to you are listed.
Click the “Search” option on the top menu bar to find tickets based on various ticket, host and vulnerability attributes.

Select “Info” from the Quick Actions menu for any ticket to view ticket details. View different ticket details in the General Information, Vulnerability Information and Ticket History sections.

The ticket history includes actions taken on the ticket automatically by the service such as when the vulnerability was discovered, when it was fixed, and the remediation policy rule that resulted in the ticket creation. Actions taken by users are also included. To make changes to the ticket, click the “Edit” button. You can change the ticket state, reassign the ticket to someone else, add comments, and so on.

**Manual Ticket Creation**

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

Qualys also has the functionality for out-of-band ticket creation. Users can manually create tickets for any host/vulnerability/port combination directly from scan status reports (Auto). See **Taking Remediation Actions** in the Reporting chapter.
Remediation Reporting

A large network will likely have a very large number of remediation tickets associated with it at any point in time. Thus, any user may also have a large number of tickets. One way for a manager to understand the progress and compliance with remediation policy is to use Qualys to initiate a remediation report.

These remediation report choices are available: Executive Remediation Report, Tickets per Vulnerability, Tickets per User and Tickets per Asset Group.

Run the “Executive Remediation Report” by selecting “Run” from the Quick Actions menu for this template in the report templates list. Follow the online prompts to select report options like report target (asset groups and/or IPs). Leave the default “All tickets” selected. Then click “Run”. Qualys will then run an Executive Remediation Report like the one shown below.

The report summary shows statistics like this:

<table>
<thead>
<tr>
<th></th>
<th>All Tickets</th>
<th>Open</th>
<th>Resolved</th>
<th>Closed</th>
<th>Avg Remediation</th>
<th>Overdue</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>123</td>
<td>18</td>
<td>2</td>
<td>40</td>
<td>20 days</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>99</td>
<td>7</td>
<td>6</td>
<td>30</td>
<td>20 days</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>291</td>
<td>152</td>
<td>15</td>
<td>90</td>
<td>20 days</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>175</td>
<td>135</td>
<td>1</td>
<td>40</td>
<td>20 days</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>83</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>N/A</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>637</td>
<td>635</td>
<td>26</td>
<td>194</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

The status of all Open Tickets appears like this:

The status of all Closed Tickets appears like this:
Then you can see the ticket state changes over time. The graphs showing Ticket State Changes and Open Ticket Trend appear like this:

**Remediation Ticket Update Notification**

You can choose to receive daily remediation ticket updates in your user account. The email notification identifies the status and changes to the tickets in your account over the past day. Tickets assigned to you and tickets based on assets in your account are included.

**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.
Step 6: Compliance Security

Qualys Policy Compliance allows customers to audit and document compliance to internal and external auditors to meet corporate security policies, laws and regulations. This operationalizes Vulnerability Management and Policy Compliance, combining it into a single solution that is delivered as a service. Policy Compliance is available in your account only when it is enabled for your subscription (not available to Express Lite users). The Policy Compliance application provides compliance management features, allowing users to create and manage policies, perform compliance scans, run compliance reports, and manage exception requests.

This chapter will provide you with an introduction to Qualys Policy Compliance and its features. For complete information, refer to the Policy Compliance Getting Started Guide, which is available for download from the Resources section (Help > Resources).

Policy Compliance Workflow

Before You Begin

Add Auditor Users (Optional)

Create users with the Auditor user role to perform compliance management tasks. Auditors can create and manage compliance policies for the subscription, generate reports on compliance data and manage exception requests. Auditors only have visibility into compliance data (not vulnerability data).
Add Custom Controls (Optional)
The service provides technical controls for measuring compliance against a wide variety of
technologies, including operating systems (i.e. Windows 2003) and applications (i.e. Oracle 9i). In
addition to the service-provided controls, users can add custom controls to the subscription
making them available for compliance scanning and reporting. The service supports custom
controls for various Windows and Unix technologies.

Customize Frameworks for the Subscription (Optional)
When users view technical control information the details include a list of frameworks, standards
and regulations that the control maps to. Manager users have the option to customize the list to
only display selected frameworks. This setting is made at the subscription level.

Customize Technologies for the Subscription (Optional)
By default all supported technologies are available when creating policies and viewing controls.
Manager users have the option to customize the list to only display selected technologies. For
example, you can select only Windows technologies and all other technologies will be hidden to
users. This setting is made at the subscription level.

Step 1: Create Policies
A policy is a collection of controls (service-provided or user-defined custom controls) pertaining
to one or more technologies in your environment. Each control in the policy includes a statement
of how the technology specific item should be implemented and one or more checks performed
by the service to validate the control. The policy is later compared to compliance scan results to
identify whether hosts are compliant with the policy.

Step 2: Assign Asset Groups to Policies
When creating or editing a policy, assign asset groups to the policy. Assigned asset groups should
include compliance hosts that are relevant to the technologies in the policy.

Step 3: Run Compliance Scans
Compliance scans identify whether hosts are compliant with user-defined policies. You can
launch a compliance scan on hosts that have been defined as compliance hosts for your
subscription. Before you launch compliance scans, you must create compliance profiles and add
authentication records for trusted scanning.

Step 4: Generate Compliance Reports
Generate specialized compliance reports on host compliance data. Interactive reports let you
change the report source options in real-time to identify the compliance status for individual
hosts and the pass/fail status for technical controls. Template-based reports identify whether
the service was successful in authenticating to hosts and whether hosts are compliant with
user-specified policies.

Step 5: Manage Exceptions
A workflow is provided for exempting certain hosts from certain controls in a policy. Exceptions
are valid until a specified end date as determined by the exception approver. Any user with
compliance management privileges can request an exception. Managers and Auditors then
review exception requests and either accept or reject them.
## Accessing Policy Compliance Features

When enabled, Managers are granted access to compliance management features automatically. Managers can add Auditor users with access to compliance policy management and reporting features at the enterprise level, without vulnerability management capabilities. Sub-accounts may be added/updated to grant these users role-based access to compliance management.

To access policy compliance features, you must first select the PC application from the Module Picker in the top, left corner.

Once in the PC application, you’ll see these options along the top menu:

- **Dashboard** — The dashboard provides a one-page summary of your overall compliance status across all policies in your account, based on the most recent compliance scan results.

- **Policies** — Manage compliance policies and SCAP policies (when SCAP is also enabled for the subscription). A compliance policy is a written statement of a rule that is applied to operating systems and applications, referred to as technologies, in the network environment.

- **Scans** — Compliance scans gather compliance data from hosts in asset groups.

- **Reports** — Reports with multiple views to review compliance status with a particular policy by business unit, asset group or host. (Note Report Share is enabled.)
Exceptions — Exception requests submitted by users. Each request is for a host/control in a certain policy. Managers and Auditors may approve exceptions. Unit Managers may approve exceptions when granted this permission.

Assets — View compliance hosts from the hosts assets list. Go to Assets > Host Assets and then select Compliance Hosts from the Filters menu.

**Policy Compliance Summary**

Qualys provides Policy Compliance functionality for auditing host configurations and measuring their level of compliance with internal and external policies. When enabled, Policy Compliance features are integrated into the Qualys Security and Compliance Suite, allowing users to run compliance scans, generate policy compliance reports, and manage exception requests.
Wait, there’s more!

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

**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.

**Watch the overview** for an introduction to Qualys Cloud Agent Platform.

**Video Tutorials**

- Cloud Agent Platform Introduction (2m 10s)
- Getting Started Tutorial (4m 58s)

**Get informed quickly** about the revolutionary Qualys Cloud Agent Platform.

**From the Community**

- Cloud Agent Platform Announcement
- Cloud Agent Getting Started Guide

**Get Real-Time Security Alerts**

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

It’s easy to get started! Jump over to the Continuous Monitoring module. 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.
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/](http://www.qualys.com/support/).