Preface

Chapter 1  Introduction

What are the Steps? ......................................................................................................... 10
Operationalizing Security and Compliance ............................................................... 11

Chapter 2  Rollout First Steps

First Login.................................................................................................................... ..... 14
Your Qualys account............................................................................................ 14
Update your account settings if needed............................................................ 14
Your Host Assets .................................................................................................. 15
Add Hosts.............................................................................................................. 16
Remove IPs from the Subscription..................................................................... 19
Virtual Hosts ......................................................................................................... 20
Check Network Access to Scanners ................................................................... 20
Review Password Security Settings ................................................................... 20
Adding User Accounts ........................................................................................... 21
User Roles and Privileges.................................................................................... 21
Asset Groups and Business Units ...................................................................... 22
Adding a Manager................................................................................................ 24
About User Account Settings............................................................................... 25
Defining Scope of User Actions............................................................................. 27
Adding Asset Groups .......................................................................................... 28
Adding Scanners and Readers............................................................................ 29
Adding Business Units......................................................................................... 29
Adding Unit Managers to Business Units......................................................... 31
User Hierarchy Chart........................................................................................... 31
Transfer Users to Business Units ...................................................................... 32
Transfer Business Objects to Users .................................................................. 33
Ownership of Business Objects ........................................................................... 33
Deleting Users ....................................................................................................... 34
Installing Scanner Appliances ............................................................................. 35
Manage Your Scanner Appliances ..................................................................... 36
Scanner Capacity Chart ....................................................................................... 37
Scanner Appliances and Asset Groups ............................................................. 38
How to Grant Users Access ............................................................................... 38
Multiple Scanner Appliances and Business Units ............................................ 39
Installing Cloud Agents ....................................................................................... 40
Chapter 3  Vulnerability Scanning

Network Discovery.......................................................................................................... 44
  Launch a Map ........................................................................................................ 45
  View Map Results ................................................................................................. 46
  View Map Results - Graphic Mode .................................................................... 47
Asset Categorization and Workflows ........................................................................... 48
  Add a New Asset Group...................................................................................... 49
  Taking Workflow Actions.................................................................................... 51
Your First Scans............................................................................................................... . 52
  Select Scan Notification....................................................................................... 54
  Launch Vulnerability Scan................................................................................... 55
  Scan Status.............................................................................................................. 56
  Scan Complete Email for Vulnerability Scan .................................................... 58
  View Scan Results ................................................................................................. 60
  About Scanning Events ......................................................................................... 64
Vulnerability KnowledgeBase ....................................................................................... 65
  Vulnerability Severity Levels .............................................................................. 67
  Vulnerability Search ............................................................................................. 69
  Vulnerability Search Lists .................................................................................... 69
  Editing Vulnerabilities ......................................................................................... 72
Customizing Scans........................................................................................................... 74
  Scanner Appliance Setting................................................................................... 74
  Option Profiles Provided ..................................................................................... 75
  View Option Profiles ............................................................................................ 75
  Option Profile Settings ......................................................................................... 76
Current Host Information............................................................................................... 81

Chapter 4  Enterprise Management and Reporting

Enterprise Security Auditing.......................................................................................... 84
  Add Scheduled Scans ........................................................................................... 85
  Review Option Profiles ....................................................................................... 86
  Set Default Option Profile .................................................................................... 87
  Publish Global Option Profiles ........................................................................... 87
  Scan for Selected Vulnerabilities ......................................................................... 87
  Trusted Scanning................................................................................................. 89
  Scanner Parallelization ......................................................................................... 91
Enterprise Reporting ....................................................................................................... 93
  View Report Templates ......................................................................................... 94
  Running Reports with Report Share .................................................................... 95
  Scheduling Reports ............................................................................................... 97
  Sharing Reports ................................................................................................. 98
  Secure PDF Distribution ...................................................................................... 98
  Patch Reports .................................................................................................... 101
  Consultant Reports .............................................................................................. 102
Contents

Report Templates................................................................................................ 103
Download Data Lists as CSV, XML, HTML, MHT ........................................ 103
Remediation Workflow ...................................................................................... 104
  Enable Remediation Workflow ...................................................................... 105
  View Tickets List ......................................................................................... 107
  View Ticket Information ............................................................................... 107
  About the Closed Loop Ticketing System................................................... 108
Customizing Level of Risk ............................................................................... 110
  Customizing Vulnerabilities ........................................................................... 110
  Business Risk in Scan Reports ...................................................................... 111
  Security Risk in Scan Reports ................................................................ ...... 112
  CVSS Scoring ............................................................................................... 116
  Ignoring Vulnerabilities ............................................................................... 119

Chapter 5 Compliance

  Achieving Compliance .................................................................................... 122
  Vulnerability Reporting and Trend Analysis ................................................. 123
    Executive Report with Trending ................................................................. 124
    Asset Search .............................................................................................. 125
    Risk Analysis ............................................................................................ 128
    Vulnerability Compliance Reports ............................................................ 130
  Remediation Reporting .................................................................................. 131
  Payment Card Industry (PCI) Compliance .................................................... 134
    PCI Data Security Standard ......................................................................... 134
    Quarterly PCI External Scans Workflow .................................................... 134
    Quarterly PCI Internal Scans Workflow ..................................................... 136
  Policy Compliance (PC) ................................................................................ 137
    Auditor User Role ....................................................................................... 137
    Policy Editor ............................................................................................... 137
    Policy Manager .......................................................................................... 139
    Policy Compliance Reporting ...................................................................... 140
    Running Template Based Reports ............................................................. 140
    Running Interactive Reports ...................................................................... 140
    Exceptions Management ............................................................................. 142
  Policy Compliance — Current Regulations and Mandates .............................. 143

Chapter 6 Successful Qualys Rollout Case Studies

  Case 1 — Global Online Retailer ................................................................. 148
  Case 2 — Web Meeting Application Provider ............................................. 149
  Case 3 — Global Electronics Manufacturer ............................................... 150
  Case 4 — Global UK Bank ............................................................................ 151
  Case 5 — Large Chemical Company ........................................................... 152
  Case 6 — Global Food Services Company ................................................... 153
Preface

This user guide is intended for security managers and auditors responsible for the successful rollout of Qualys Security and Compliance Suite in the enterprise. Qualys is the widely adopted vulnerability management and policy compliance solution from Qualys, Inc.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,200 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

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

This guide combines many of the best practices gained from our experience with supporting customers of varying sizes and complexity with Qualys rollouts. These projects are large in scale, most often deployed globally on distributed, segmented networks, and frequently involve many users with diverse responsibilities within the enterprise.

As you start your own Qualys rollout, it makes sense for us to share with you our best practices approach so that you can quickly and effectively take advantage of Qualys to automate the process of vulnerability management and policy compliance within your organization.

The goal of this document is to take you step by step through the process of both getting Qualys running in production and learning the best practices that will maximize the value you will receive from enhanced network security.

Let’s get started!
What are the Steps?

We have arranged this guide into the sections described below.

Chapter 2, Rollout First Steps, covers the basics of setting up the service, adding users, defining the scope of user actions, installing Qualys Sensors - Scanner Appliances and/or Cloud Agents.

Chapter 3, Getting Started with Security Auditing, leads you through the steps of running your first scans and understanding scan results. In preparation to this we discuss Qualys tools that help you discover your network and prioritize assets. Once you have performed and reviewed your first scans, we will describe the options for customizing scans.

Chapter 4, Enterprise Management and Reporting, takes you through the steps of implementing a successful Qualys rollout across the enterprise. This is focused on a phased approach that allows you to start out with a basic process and to enhance the process, as required, over time. It involves using Qualys enterprise management tools for security auditing and reporting as well as the remediation workflow feature.

Chapter 5, Compliance, helps you to use Qualys to show the progress you are making in managing your vulnerabilities and the security risk in your network. This will also help you in making the adjustments to your vulnerability management system’s options and processes to achieve your required results. A key element in tracking your progress is how this will assist you in meeting the myriad of regulations which have network security as part of their requirements.

In Chapter 6, Successful Qualys Rollout Case Studies, we have taken real customer examples, from various industries, to help you understand their ingredients for success. You can learn from the challenges they faced and have an implementation plan that leverages their experience.

While this document is intended to assist you with a successful rollout of Qualys, it is important to note that there are many product features that are not outlined here. As you become familiar with Qualys you will find additional features and capabilities. We recommend that you fully explore the application and reference the online help and other resources documents to allow you to take full advantage of the power of the application.

Before we start it is important that we have a common understanding of Qualys benefits and a set of high level best practices which we have found to lead to successful implementations.
Operationalizing Security and Compliance

The amount of risk facing any IT infrastructure is constantly in flux and can be difficult to measure. Any change to a system or its broader computing environment might also change its security posture. While every organization has firewalls and antivirus in place, the limitations of these basic layers of defense are a constant concern for security conscious companies.

Today’s fast-moving viruses and worms have found ways to pass through firewalls and bypass antivirus applications. As the time from vulnerability announcement to common vulnerability exploit continues to shrink, organizations are increasingly faced with the challenge to find more proactive security solutions.

One of the proven ways to reduce the risk of being hit by a worm or virus is through regular network security audits to identify vulnerabilities and correct the weaknesses before they can be exploited. Security risk and policy compliance management makes it possible for a company to take proactive steps to spot rogue devices, identify vulnerabilities, and ensure systems are configured inline with standards and corporate policy.
ROLLOUT FIRST STEPS

The rollout project setup involves building a deployment plan based on network analysis and business objectives, and then distributing vulnerability management and policy compliance responsibility to multiple users. It’s recommended that you do your homework in advance to understand your network environment and its segmentation before you begin network security auditing. With your understanding of the network and the people responsible for managing the various systems and network segments, you will add user accounts, install Scanner Appliances, and assign users asset responsibility by defining asset groups and optionally business units.

To achieve the best rollout project setup in the quickest time, please complete the following activities in the order presented:

- FIRST LOGIN
- ADDING USER ACCOUNTS
- DEFINING SCOPE OF USER ACTIONS
- INSTALLING SCANNER APPLIANCES
- MANAGE YOUR SCANNER APPLIANCES

Note: The rollout project setup requires Manager user privileges. If you are the subscription owner, then your user account has these privileges by default. You may choose to add additional Manager users to assist with the rollout project setup. We will discuss adding users as well as user roles and privileges in this chapter.
FIRST LOGIN

Be sure to complete your first login and check to be sure that you are ready to start security auditing activities using the account.

BEST PRACTICES

Be sure to complete your account registration. Follow the instructions provided, starting with the Qualys “Registration - Start Now” email and ending with accepting the terms and conditions.

Check configurations before you begin. It’s recommended that you view the IP addresses in your account, add IP addresses and virtual hosts as needed, classify assets in your account, check network accessibility to target hosts, and review password security options for the subscription.

ROLLOUT STEPS

Your Qualys account

When your new subscription is created, you will receive an email notification titled Qualys Registration - Start Now. This email includes a secure link to your user login ID and password (this is a one-time only link).

After completing the registration steps, you will receive an email notification titled Qualys Registration - Complete.

Soon we will discuss adding user accounts to the subscription. When you add user accounts, each new user will receive a Qualys Registration email and will need to complete the same registration process.

Update your account settings if needed

The user menu (top right) give you several options, available to you all the time.

- Change your password
- Change your default Home Page
- View your account settings
- Return to the Quick Start Guide
Your Host Assets

Qualys provides methods for asset classification to support managing network security in dynamic and distributed networking environments.

At this time you will want to view the hosts in your account and select the host tracking method to be used. For a new subscription, hosts in the account are tracked by IP address and the tracking method can be changed to DNS hostname or NetBIOS hostname. Optionally, you may enter asset tags (host attributes) and an asset owner.

The hosts in your account may be used as targets for vulnerability and compliance scans. To view the hosts in your account, go to Assets > Host Assets.

Click (Expand range) next to a range to view hosts in the range.

Click (View host information) next to a host to view comprehensive host information, including the host’s attributes, current vulnerabilities and tickets as well as an activity log listing actions involving the host.
Chapter 2 — Rollout First Steps
First Login

The host assets list displays all hosts in your account. All hosts may be the target for a vulnerability scan. Compliance hosts may be the target for a compliance scan, when the policy compliance module is enabled in the subscription. To view compliance hosts only, select Filters > Compliance Hosts.

Managers can view information on the total IPs purchased and total IPs in subscription in the Account Info section (go to Help > Account Info). Please contact Support or an Account representative for help with purchasing more IPs.

Add Hosts

To add hosts, go to New > IP Tracked Hosts. (You’ll see you have the option to select the DNS or NetBIOS tracking method if hosts in your network are assigned IP addresses dynamically.) Use the wizard to enter your new hosts.
Host IPs

In the Host IPs section enter IP addresses/ranges. Multiple entries are comma separated.

The policy compliance module may be enabled in your account. If so, the check box “Add to Policy Compliance Module” appears. Select this box if you want the new hosts to also be added to the policy compliance module. When selected you can perform vulnerability scans and compliance scans on the hosts.

Host Attributes

In the Host Attributes section, enter host attributes (optional). The host attributes are displayed in host security views throughout the application, and in scan status reports (automatic). Initially the names are set to Location, Function, and Asset Tag. Go to Setup > Host Attributes if you want to customize host attribute names.
Chapter 2 — Rollout First Steps

First Login

Click the “Add” button to add the hosts.

**Take Actions on Hosts**

Select hosts already added to your account and take actions on them using the Actions menu. You can edit host attributes (one host at a time, or bulk edit), add/remove hosts from asset groups, and add hosts for compliance scans.
Remove IPs from the Subscription

Managers can remove IPs from the subscription. Once an IP is removed, the host data is not recoverable. Please review these possible consequences before removing IPs:

- IPs will be deleted from Asset Groups.
- Scheduled Scans will be deactivated at the next launch (except when the target includes asset groups only and at least one asset group has remaining IPs).
- Automatic host data will be purged, also Tickets and Exceptions will be deleted.

To remove IPs, go to New > Remove IPs.

Select the IPs you want to remove and then click Remove.
Virtual Hosts

Depending on your network configuration, you may want to add virtual hosts to your subscription. A virtual host is defined as a single machine that acts like multiple systems, hosting more than one domain (FQDN). Adding virtual host configurations ensures that the scanning service analyzes all specified domains associated with each IP address scanned, possibly increasing the number of vulnerabilities detected. To view the virtual hosts in your account, go to Assets > Virtual Hosts. From the virtual host list you can add a new virtual host configuration by going to New > Virtual Host.

Check Network Access to Scanners

Important details about External Scanners and Scanner Appliances are shown on the About page (go to Help > About). Be sure that your network permits access between the scanners and the IPs to be scanned.

External Scanners. External Scanners for external (perimeter) scanning are located at the Secure Operating Centers (SOCs), datacenters maintained by Qualys. External scanners must be able to access target IPs for perimeter scanning (see Help > About).

Scanner Appliances. Scanner Appliances for internal scanning are installed on your internal network, inside your corporate Intranet. Scanner appliances must be able to access target IPs for scanning your internal network (see Help > About).

Review Password Security Settings

Your Qualys login ID is permanent and assigned by Qualys. Your password is a randomly generated “strong” password. You can change your password if you wish at any time from your account menu.

Manager users have the ability to allow user-defined passwords. This option is not enabled in new subscriptions. To enable this option, go to Users > Setup > Security, and select “Allow user defined passwords”. Any password security settings you make will apply to all user accounts in the same subscription.
**ADDING USER ACCOUNTS**

You can easily assign assets to multiple users within the enterprise. By assigning responsibility for security auditing and vulnerability remediation on assigned assets, you can distribute this responsibility to multiple users.

**User Roles and Privileges**

Qualys has a user role-based model for assigning user privileges. Pre-defined user roles grant specific privileges, including access to assets. Multiple users with the same user role may be added.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Summary of privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>- Most privileged user role with access to all assets</td>
</tr>
<tr>
<td></td>
<td>- Discovery (maps), security auditing (scans), reporting, remediation</td>
</tr>
<tr>
<td></td>
<td>- Manage assets and users</td>
</tr>
<tr>
<td></td>
<td>- Set subscription policies and global configurations</td>
</tr>
<tr>
<td></td>
<td>- Typical users: Chief Security Officer, Security Manager</td>
</tr>
<tr>
<td>Auditor</td>
<td>This role is available when the policy compliance module is enabled</td>
</tr>
<tr>
<td></td>
<td>- Manage policies, exception requests, and compliance reporting</td>
</tr>
<tr>
<td></td>
<td>- Access to all compliance hosts in the subscription</td>
</tr>
<tr>
<td></td>
<td>- Typical users: Security Auditor, Third Party Consultant</td>
</tr>
</tbody>
</table>
## User Role | Summary of privileges
--- | ---
Unit Manager | - Discovery (maps), security auditing (scans), reporting, remediation
- Access to assets (IPs, domains, appliances) in asset groups assigned business unit
- Manage assets and users in assigned business unit
- Typical users: Division Manager, Regional Manager

Scanner | - Discovery (maps), security auditing (scans), reporting, remediation
- Access to assets (IPs, domains, appliances) in asset groups assigned to the user’s account
- Typical users: Security Engineer, IT Administrator, Inside Consultant

Reader | - Reporting and remediation only
-- Access to assets (IPs, domains) in asset groups assigned to the user’s account
- Typical users: Executive, Outside Consultant, Auditor, IT Assistant

Contact | - No access to the Qualys user interface
- Receive summary email notifications for scans and maps
-- Receives notifications for assets (IPs, domains) in asset groups assigned to the user’s account. (A Contact user account exists for administrative purposes and can be edited by Managers A Contact user cannot log in to the user interface or make API requests using this account.)
- Typical users: Monitoring or tracking device, Auditor, Alert System

## Asset Groups and Business Units
User accounts grant users access to certain hosts, based on user role. Sub-account users — Scanner, Reader, Contact — are assigned asset groups. Unit Managers are assigned a business unit consisting of asset groups. For a subscription with multiple users and assets, you’ll want to organize your assets as shown in the diagram below.
Chapter 2 — Rollout First Steps
Adding User Accounts

Figure 2-2. Organizing Assets into Asset Groups and Business Units

Starting with all the assets in the subscription, you create logical asset groups. Each Scanner and Reader account is assigned one or more asset groups. You have the option to go one step further and define business units including asset groups and users. Each business unit must be assigned one or more Unit Managers who have management responsibility for a limited set of assets in the subscription.

**BEST PRACTICES**

**Add at least one user account.** Qualys recommends that you add at least one new user account. We suggest that you add a Manager or Unit Manager to begin, although a user account with any role except Contact is fine. If the subscriber account is lost or misplaced, this makes it possible for Qualys Support to reset the password for the subscriber account while retaining all saved results and user configurations for the subscription.

**Add users with management responsibility first — Managers and Unit Managers.** These users will have management responsibility for the rollout project and they will have the ability to add more users.

**Create a flexible solution.** Delegating roles and responsibilities to multiple users involves creating a flexible solution that adapts to operating environments and maintains global standards. Refer to “Defining Scope of User Actions” for developing an approach to building the solution for your organization.
**ROLLOUT STEPS**

**Add at least one user account.** Add at least one new user account with privileges to access the Qualys web application. To add a new user select Users from the top menu and then select New > User. See “Adding a Manager” and “Adding Scanners and Readers” for help.

**Add a Unit Manager.** If you wish to use a business unit you need to add a Unit Manager. See “Adding Unit Managers to Business Units” for information.

**Review user account information.** Gain an understanding of user account information and privileges for the various user roles. Apply this information when setting up multiple users.

**Adding a Manager**

As the subscriber, your user account is automatically assigned the Manager role. You can choose to add another Manager user so that there is redundancy at the Manager level for the subscription. All Managers have full privileges.

To add a user, go to Users. From the user’s list select New > User. Using the new user wizard, enter user settings.

Under General Information, provide the user’s name and contact information.

![New User Wizard](image)
Under User Role, select the user role “Manager”. (The service automatically adds Managers to the Unassigned business unit).

Under Notification Options select email notifications for the user. After creating the account, the user has the ability edit these settings.

After you save the account, the new user will automatically receive a registration email with a secure link to the credentials for their new account and login instructions.

**About User Account Settings**

The user account settings have common sections for all users. The sections Asset Groups and Extended Permissions appear for users with certain roles.

<table>
<thead>
<tr>
<th>User Account Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>General information about the user, including name and contact information.</td>
</tr>
<tr>
<td>User Role</td>
<td>The user role and business unit. A business unit is required for a Unit Manager.</td>
</tr>
<tr>
<td>Options: Notification</td>
<td>Several email notification options are available. A user may choose to edit these settings:</td>
</tr>
<tr>
<td></td>
<td>- Latest Controls (when PC is enabled)</td>
</tr>
<tr>
<td></td>
<td>- Latest Vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>- Scan Complete Notification</td>
</tr>
<tr>
<td></td>
<td>- Scan Summary Notification (vulnerability scans only)</td>
</tr>
<tr>
<td></td>
<td>- Map Notification</td>
</tr>
<tr>
<td></td>
<td>- Report Notification (when Report Share is enabled)</td>
</tr>
<tr>
<td></td>
<td>- Exception Notification (when PC is enabled)</td>
</tr>
<tr>
<td></td>
<td>- Daily trouble ticket updates</td>
</tr>
<tr>
<td></td>
<td>- Scanner Appliance heartbeat check</td>
</tr>
</tbody>
</table>
Chapter 2 — Rollout First Steps
Adding User Accounts

Options: SAML SSO
Qualys supports SAML SSO for user authentication. When this feature is enabled for the subscription, Managers have the option to enable SAML SSO for new users or for selected users.

Using SAML SSO, Qualys acts as a Service Provider and provides cloud security and compliance services. Your organization's SSO solution acts as an Identity Provider that manages usernames, passwords and configurations used to authenticate users for our services.

Note that users with SAML enabled for UI access do not have API access.

Options: VeriSign Identity Protection (VIP)
Qualys includes support for VeriSign Identity Protection (VIP) two-factor authentication. Managers have the option to require VIP authentication for all subscription users or for specific users. Any user can opt in.

When VIP authentication is required for a user account, logging into the user interface is a two-part process. First the user provides their Qualys credentials (login name and password) followed by their VIP credentials (VIP credential ID and one-time security code).

Asset Groups
(Appears only for Scanner, Reader, Contact) Use this section to assign asset groups. Refer to “Adding Scanners and Readers.”.

Permissions
(Appears only for Unit Manager, Scanner Reader) Select extended permissions.
- Add assets (Unit Manager)
- Create/edit remediation policy (Unit Manager)
- Create/edit authentication records/vaults (Unit Manager)
- Create option profiles (Unit Manager, Scanner)
- Create/edit virtual hosts (Unit Manager, Scanner)
- Purge host information/history
- Manage compliance
- Manage web applications
**DEFINING SCOPE OF USER ACTIONS**

The scope of user actions is defined by each user’s user role and other user account properties, including asset group responsibility. The diagram below illustrates a sample subscription with multiple users and two business units.

![Diagram of user and asset groups]

**Using Asset Group Conventions**

By applying conventions for organizing and naming your asset groups, you can more effectively manage vulnerabilities and their remediation.

Flexible asset groups support any organizational method you desire. Asset groups can be defined by importance, priority, location, business function or ownership. It’s often the case that rollout projects organize assets in a number of different ways. Keep in mind that the same asset may be defined in multiple asset groups.

Asset group names appear throughout the application for quick identification. It’s recommended that you adopt a naming scheme for your asset groups. An asset group’s grouping method can be reflected in its name for example.

When the policy compliance module is enabled, asset groups containing compliance hosts are assigned to user-defined policies for compliance testing and reporting.
**BEST PRACTICES**

**Understand your network and the people managing the systems.** Evaluate the number of users you expect and what their responsibilities will be, and then match them to asset groups and business units accordingly.

**Follow asset grouping guidelines.** When creating asset groups, apply some conventions for naming and organizing them. As an option, you may use the asset management workflows from map reports and asset search reports to add assets to asset groups. See Chapter 3 for information.

**ROLLOUT STEPS**

**Add asset groups and business units.**

**Add user accounts.** Add Managers, Unit Managers, Scanners and Readers as appropriate for your rollout project.

**View users and their asset groups.** Refer to the Hierarchy Chart to assist with building teams and managing users.

**Adding Asset Groups**

To add a user — except a Manager user — there must be asset groups in your account before you can add the user account. For a Scanner, Reader or Contact, asset groups are assigned directly to the user account. A business unit includes asset groups. Each Unit Manager is assigned to a business unit and inherits the asset groups in their assigned business unit.

To add an asset group go to Assets > Asset Groups. From the asset groups list, select New > Asset Group.

In the new asset group wizard, enter an asset group title, following some naming convention, and other settings in the sections provided.

<table>
<thead>
<tr>
<th>Asset Group Section</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPs</td>
<td>IP addresses/ranges to be used as scan targets.</td>
</tr>
<tr>
<td>Domains</td>
<td>Domains to be used for network discovery targets.</td>
</tr>
<tr>
<td>Scanner Appliances</td>
<td>Scanner Appliances for internal scanning of devices on the Intranet, inside the corporate network. This section appears only when a Scanner Appliance is available in your account. See “Installing Scanner Appliances.”</td>
</tr>
<tr>
<td>Business/CVSS Info</td>
<td>Business information, including a business impact level used for calculating business risk in reports. An impact level of “High” is automatically assigned to new asset groups.</td>
</tr>
</tbody>
</table>
Adding Scanners and Readers

For a Scanner or Reader when you use the wizard to add or edit a user account, you grant the user access to assets for scanning (IP addresses, domains and Scanner Appliances) by assigning asset groups in the Asset Groups section. Simply add asset groups to the Assigned Asset Groups list on the right.

![New User](image)

Notes about adding users within a business unit: Unit Managers can create Scanners and Readers for their own business units. When a Unit Manager adds a new user, the asset groups in the Available list correspond to the asset groups in the Unit Manager’s business unit. Unit Managers are responsible for managing assets and users in their own business unit.

Adding Business Units

A business unit consists of asset groups so you must add asset groups before you begin. There are two workflows for adding a business unit. You can do this when adding a Unit Manager account (see “Adding Unit Managers to Business Units” below) or when viewing the business units list.

To add a business unit from the business units list, go to Users > Business Units. From the business units lists, select New > Business Unit.
Using the new business unit wizard, enter a business unit name. In the Assets section, assign the business unit assets for scanning (IP addresses, domains and Scanner Appliances) by moving selected asset groups to the Assigned Asset Groups list. One asset group is required. In the Users section you can assign users to the asset group (optional).

Managers can limit the number of new IP addresses that Unit Managers can add, when these users have accounts with permission to add assets. To enable these controls, go to Setup > Business Units and select the option “Enable limiting the number of new IPs that Unit Managers can add”.

When enabled, Managers have the option to assign a New IP Limit to a business unit. The New IP Limit is the total number of new IP addresses (not already in the subscription) that Unit Managers can add. A unique New IP Limit may be assigned to each business unit.
Adding Unit Managers to Business Units

Manager users can choose to add a Unit Manager to a new or existing business unit. A Unit Manager can be assigned to only one business unit, and this user has the option to add additional users to the same business unit — Unit Managers, Scanners and Readers.

To add a new user, go to Users. From the user accounts list, select New > User. Using the wizard, select the Unit Manager user role and a business unit name. Tip: Click the New Business Unit button to add a new business unit, if it doesn’t already exist.

User Hierarchy Chart

The user hierarchy chart provides a list of users in the subscription according to the organization’s business structure. To view this chart, go to Users and then select Filters > Hierarchy Chart. See the sample chart below. The asterisk denotes the subscription contact (Manager) and the contact for each business unit (Unit Manager).
Transfer Users to Business Units

Managers have the ability to transfer existing users to a business unit using a simple workflow within the business unit. The user transfer workflow supports the smooth transition of users and their configurations.

When adding or editing a business unit, the users section shows users assigned to the business unit and users in the subscription who may be added. You may sort and view the users list in many ways — by user name, user role, business unit and asset group.

To add users, go to the Users section and move users, already in the subscription, to the Assigned Users list (on the right) and then click Save.

The transfer wizard appears. In the Options section confirm the user transfer and select options. You may choose to keep users’ personal configurations and asset groups. Please be aware that if you move users’ personal configurations without the asset groups, it’s possible user configurations may need to be modified after the transfer (for example, in order for user schedules to run as defined). For more information, see the online help.
Transfer Business Objects to Users

Managers and Unit Managers have the ability to transfer business objects from one user to another in the subscription. Business objects that can be transferred include asset groups, option profiles (scan settings), report templates, scan schedules, and search lists. The ability to transfer business objects from one user to another supports organization changes to infrastructure and responsibility over time.

Ownership of Business Objects

When editing a business object such as an asset group, you can assign an owner for the object using the Owner drop-down menu in the top section.

The Owner menu lists all users who can be assigned the asset group. Possible assignees depend on the role of the manager making the transfer and the user’s business unit.

<table>
<thead>
<tr>
<th>Manager Doing Transfer</th>
<th>Owner’s Business Unit</th>
<th>Possible New Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>Unassigned</td>
<td>Manager or Scanner in current owner’s business unit</td>
</tr>
<tr>
<td>Manager</td>
<td>Custom</td>
<td>Manager in Unassigned business unit - or - Unit Manager in current owner’s business unit</td>
</tr>
<tr>
<td>Unit Manager</td>
<td>Custom</td>
<td>Unit Manager or Scanner in current owner’s business unit</td>
</tr>
</tbody>
</table>
In the case where a Manager transfers an asset group from a user in a custom business unit to a Manager (in the Unassigned business unit), the asset group automatically remains in the custom business unit so that users in the custom business unit can continue to use it.

**Deleting Users**

Managers and Unit Managers have the ability to delete users. Managers can delete any user in the subscription, while Unit Managers can delete users in their own business unit.

To delete a user from the user accounts list, select the check box next to the user you wish to delete, and then select Actions > Delete. It’s possible to select multiple check boxes to delete multiple users in bulk.

Confirm the user delete action. You’ll have the option to delete the user’s scan results. Also you’ll have the option to transfer the user’s business objects to another user. These objects include profiles, report templates, asset groups, scheduled tasks, authentication records, policies, exceptions, vulnerability tickets and search lists.

**Map and Scan Results.** When map and scan results are deleted results will no longer be available to other users for reporting.

**User Business Objects.** Assign the user’s business objects to another user or select “No New Owner”. Possible assignees are Managers plus other users with the same or greater user role as the user you are deleting. For example, if deleting a Scanner, the New Owner menu lists Managers plus Unit Managers and Scanners in the user’s same business unit. When “No New Owner” is selected, the user’s personal business objects are deleted.
INSTALLING SCANNER APPLIANCES

Installing Qualys Scanner Appliances allows you to scan for security vulnerabilities on your internal network. The number of Scanner Appliances for your enterprise will depend on the size and configuration of your network. Once installed, each Scanner Appliance keeps itself updated with the latest vulnerability signatures via its connection to the Qualys Cloud Platform.

BEST PRACTICES

Plan for Scanner Appliance installations. First evaluate your network setup and access to the Qualys platform. Qualys Support is available to assist you with network evaluation and analysis to determine the recommended number of Scanner Appliances for your organization.

Place Scanner Appliances as close to targets as possible. It's best to place Scanner Appliances as close to scan targets as possible to minimize latency and maximize bandwidth for scanning traffic, which is much heavier than reporting traffic.

ROLLOUT STEPS

What are the installation steps. This depends on whether you’ll install a physical or virtual appliance. Download the latest user guide for the step by step instructions.

Qualys Scanner Appliance User Guide
Qualys Virtual Scanner Appliance User Guide
Qualys Offline Scanner User Guide

Once your scanner is installed you can take actions within your Qualys account.

Grant users access to Scanner Appliance. Only Managers can view/access newly installed Scanner Appliances. You can grant other users access.

Manage your Scanner Appliances. Just to to the scanner appliances list.

Check out the Scanner Capacity Chart. This chart shows the percentage of used capacity for the appliance over the past 7 days. Also the service calculates a capacity trend so you can track usage over time.
Manage Your Scanner Appliances

The Appliances list helps you understand the status of each appliance and to see available capacity for scanning.

1) Readiness for Scanning. 🟢 indicates that the scanner appliance is currently connected to the New Scanner Services and is ready to process scans. You can also see whether the appliance is currently busy with a scan. 🟡 indicates the appliance is busy.

2) Appliance Type. 🟢 indicates that the scanner appliance is a physical appliance. 🟡 indicates a virtual appliance. Mouse over any icon for details.

3) Appliance Summary. Includes the number of heartbeat checks missed, and the latest software versions of the scanning engine and vulnerabilities signatures. If the appliance does not have the latest software installed then you’ll see a yellow indicator.

4) Understand the Available Capacity. You’ll see the amount of capacity currently available for the appliance. This helps you better understand which scanner appliances get the most use and which appliances are available for scanning.
Scanner Capacity Chart

You can see the Scanner Capacity chart by going to the appliance information window (select Info from the Quick Actions menu). The chart shows the percentage of used capacity for the appliance over the past 7 days. (Note this chart appears only when New Scanner Services is enabled for your account.)

The Scanner Capacity chart shows the capacity of the appliance within the past 7 days, calculated in 15 minute increments. Place your cursor over any point in the chart to see the used capacity for that moment in time, expressed as a percentage. For example Used Capacity: 18% means the appliance used 18% of its capacity and 82% of its capacity was available at that time. You’ll see the date and time the capacity was calculated.

A trend line shows you the capacity trend, calculated in 6 hour intervals. Every 6 hours the service takes an average of the used capacity and shows this in the middle of a 6 hour window. For example, for the period 3pm to 9pm the average appears at 6pm. Average over 6 hours: 10% means the average of the used capacity was 10% and 90% of its capacity was available for the 6 hour window.
Scanner Appliances and Asset Groups

You’ll want to assign scanner appliances to asset groups
- This allows you to manage which Scanner Appliances are used to scan which target IPs.
- It gives you a way for you to make Scanner Appliances available to users with limited privileges (Scanners, Readers, Unit Managers).

Where do I manage my asset groups? Go to Hosts > Asset Groups. From there you can add a new asset group or edit an existing one. In the asset group wizard, go to the Scanner Appliances section and move appliances to “Scanner Appliances Added to Group.”

How to Grant Users Access

Manager users are granted access to a newly installed Scanner Appliance automatically. Other users (Unit Managers, Scanners, Readers) are not granted access to a newly installed Scanner Appliance without authorization. Managers can grant other users access following these steps:

1) Add the Scanner Appliance to one or more asset groups.

2) If you have custom business units and you want to grant access to users in these business units, add the asset groups containing the Scanner Appliance to the business units.

3) Assign the asset groups containing the Scanner Appliance by editing each user account. (Managers and Unit Managers can perform this step).
Multiple Scanner Appliances and Business Units

Here’s suggested flow for effective global management when you subscription has multiple scanner appliances and business units.

1) (Manager) Add a master asset group for each business unit, where each master asset group contains all IPs and domains for an individual business unit. Since these asset groups are created by a Manager, they can be edited only by Manager users. Note Scanner Appliances will be added to these asset groups later (in Step 6)

2) (Manager) Add business units by adding a master asset group to each.

3) (Manager) Add the first Unit Manager to each business unit.

4) (Manager or Unit Manager) Add more users to each business unit. Unit Managers have the ability to add additional users (e.g. Unit Managers, Scanners, Readers) to their assigned business unit.

5) (Manager or Unit Manager) Install Scanner Appliances. Keep in mind - after completing this step, only Managers have privileges to view and manage the appliances.

6) (Manager) Assign installed Scanner Appliances to the master asset group for each business unit. Completing this step makes the Scanner Appliances for each business unit available to Unit Managers.

7) (Manager or Unit Manager) Manage the installed Scanner Appliances. A Manager can manage all appliances assigned to all business units. A Unit Manager can manage appliances assigned to their own business unit.
Chapter 2 — Rollout First Steps
Installing Cloud Agents

INSTALLING CLOUD AGENTS

Qualys Cloud Agent is our revolutionary platform that supports security assessments in real time, without the need to schedule scan windows and manage credentials for scanning. You can choose to install cloud agents instead of scanner appliances for continuous security data collection. These lightweight agents can be installed anywhere - any host such as a laptop, desktop, server or virtual machine - in minutes.

All agent installations are managed in Qualys Cloud Agent. We’ll help you create activate keys, download and install agents, and activate your agents for various capabilities including Vulnerability Management (VM), Policy Compliance (PC), and more.

Log into your account and choose Cloud Agent from the application picker.

We recommend the Qualys Cloud Agent Quick Start Guide as the place to get started. Select “Quick Start Guide” below your user name at any time to see this guide.
The Quick Start Guide gives you an interactive tutorial with links to helpful information, user guides and videos.

**Recommended user guides**

- Qualys Cloud Agent Getting Started Guide
- Qualys Cloud Agent Install Guide for Windows | Linux | Unix | Mac
VULNERABILITY SCANNING

Getting started with security auditing involves learning about Qualys security audits and developing an approach to security auditing that will meet your organization’s network security goals. Typically multiple users participate in security auditing. It’s important to demonstrate the value of Qualys to gain the trust and confidence of the operating teams and outsourcers. The best way to do this is to support them in their first experiences with security auditing and to provide them with guidelines, which are the focus of this chapter.

Qualys gives users the ability to learn more about their network environment first, before launching security audits on an enterprise scale. In fact this is reported by many customers with successful rollouts as an ingredient for their success with their rollout project. This chapter discusses network discovery and workflow features that are designed to assist users with learning more about their networks.

To get started with security auditing in the quickest time, please complete the following activities in the order presented:

- NETWORK DISCOVERY
- ASSET CATEGORIZATION AND WORKFLOWS
- YOUR FIRST SCANS
- VULNERABILITY KNOWLEDGE BASE
- CUSTOMIZING SCANS
- CURRENT HOST INFORMATION
**NETWORK DISCOVERY**

Network discovery produces a baseline map of your network infrastructure from which you can identify and categorize assets. Depending on your network, there may be more than one network domain to discover.

The network discovery feature identifies network devices and reports comprehensive information about them. Starting with a domain name you supply such as “mycompany.com”, the service uses the domain’s DNS to discover hosts and gather information about hosts. Map results are available in both text and graphic formats.

**BEST PRACTICES**

**Perform network analysis before you begin.** Perform network analysis with the Security and Network teams at the outset of the project to produce a working inventory of your organization’s assets.

**Use Qualys mapping to understand your network.** Use the Qualys mapping feature to produce a map of your network and learn about the devices it contains. Check the map results and compare against your own asset inventory.

**ROLLOUT STEPS**

View the domains in your account in the Domain Assets section. Run an on demand map for a target domain using the profile “Initial Options” and view the map results. To make the maps manageable, you may choose to run multiple maps on separate network segments. Then schedule one or more maps to run weekly, and run differential reports to measure network changes.

![Figure 3-1. Network Discovery workflow](image-url)
Launch a Map

Go to Scans > Maps. Then select New > Map.

In the Launch Map window, enter a map title, select an option profile (the profile "Initial Options" is recommended to get started) and map targets under Target Domains. For the map target, you may specify any combination of IPs/ranges, domains and asset groups. When Scanner Appliances are in your account, select a scanner option on the Scanner Appliance menu. Click Launch to start the map.

For each map request, we’ll create one or more maps, depending on the map targets you specify. When multiple maps are created, they’ll share the same map title.
You can track the map’s progress on the Maps tab. You’ll see the status Running when the map is in progress, and the status Finished indicates the map has completed. You can cancel a map in progress at any time by selecting the map (row) and then selecting Actions > Cancel.

View Map Results

From the maps list you can view map results when the map status is Finished. To view map results, go to the maps list (go to Scans > Maps). Mouse over a map (row), click ▼ and then select View from the Quick Actions menu. A Report Summary is followed by a Results section with information on discovered hosts.

Host indicators in the Results section provide additional host information. A - Approved host for the domain. S - Scannable host, already in the subscription. L - Host was alive at time of discovery. N - Host in the domain’s netblock. In the Hosts section, you can view host details for each discovered host.

Click the right arrow next to any host to view a list of open services on the host. You’ll find the discovery method used to detect each service along with the port that the service was found to be running on (if available).

For a scannable host, click the host IP address to view detailed, current host information.
View Map Results - Graphic Mode

Go to View > Graphic Mode from the menu at the top of your report. Qualys will prepare a graphical representation of the map in a separate window. Here is an example:

Click on any host in the map to see details in the Preview pane (below). You’ll see basic information on the discovered host, its OS, and how it was identified:
ASSET CATEGORIZATION AND WORKFLOWS

Qualys provides the workflow needed to research, identify and classify the assets that you want to scan and monitor for security issues.

User definable asset groups allow users to prioritize assets. Each asset group consists of IPs for scanning, domains for network discovery, and optionally Scanner Appliances for internal scanning of private use internal IPs.

Key features of asset groups are:

- Logical asset grouping. By organizing assets into logical asset groups, you can control the scope of your scans, making scan results and remediation tasks more manageable.

- Assign business value to assets. A business impact level assigned to each asset group identifies asset criticality. The higher the impact level, the higher the potential for business loss if compromised. An asset group’s impact level is used to calculate business risk in reporting.

- Track business risk by asset group. This gives users flexibility in managing cases where assets in a subscription have different business priorities, possibly even different priorities when devices are a part of multiple applications and/or business units.

BEST PRACTICES

Perform network analysis before you begin. As a reminder to one of our best practices under “Network Discovery”, be sure to perform network analysis with the Security and Network teams to produce a working inventory of the organization’s assets. Your analysis will assist with prioritizing assets using Qualys.

Use discovery scans (maps). Use the Qualys mapping feature to understand the assets on your network and to assist with prioritizing those assets.

Use a phased approach to asset prioritization. Our customers with successful rollouts use a phased approach that is integrated with their Qualys security management program:

Phase 1. Define initial asset groups. Typically customers define by location, function, importance, or ownership and assign user responsibility following steps in Chapter 1, Rollout First Steps.

Phase 2. Run first scans following steps in “Your First Scans.” Update asset groups based on findings from first maps and scans.

Phase 3. Run trend reports to identify network changes and update asset groups based on the findings.
Some of our customers that have completed successful rollouts offer this advice:

- Consider your reporting goals and check that your asset groups will meet your reporting needs.
- Customer quote: “Trend reporting works well when you scan the same hosts every week. If the hosts change from week to week, the trend results are not meaningful.”
- Customer quote: “I would have had better, more meaningful reports more quickly, if I had setup asset groups differently from the start of my project.”

**ROLLOUT STEPS**

**Add Asset Groups that reflect business operations.** Based on your network analysis, create asset groups and assign business priority to them accordingly. Asset groups should be defined according to network segments, business units, asset location and function. You have the option to use the Qualys workflow to first discover assets and then add them to asset groups.

**Take Workflow Actions.** From a map report, take workflow actions to manage hosts on your network. For example, you can take workflow actions to add hosts to asset groups and add hosts to the subscription so that they can be scanned.

**Assign Scanner Appliances to asset groups.** When Scanner Appliances will be used, be sure to assign the Scanner Appliances to the appropriate asset groups. This will allow users to run distributed scans across multiple Scanner Appliances on asset groups that include Scanner Appliances.

**Add a New Asset Group**

When viewing map results, the service provides a workflow making it easy for you to add hosts listed in your map results to a new asset group. You may select hosts that are Scannable, meaning that they already exist in your account. The S indicator in the right-side legend indicates that these hosts are scannable. To select hosts, select the check box next to each scannable host you want to add.
After selecting hosts, go to the Actions menu at the top of your report window and select “Add to a new Asset Group” from the drop-down menu, and then click Apply.

The asset group wizard appears and you will notice the IPs you selected are assigned to the asset group automatically. Use the IPs section to add IPs, the Domains section to add domains, and the Business/CVSS Info section to assign business impact values. When there are Scanner Appliances in your account, use the Scanner Appliances section to add appliances.

The Scanner Appliances section for a sample asset group appears in Chapter 2 in the section “Installing Scanner Appliances.”

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 automatically for a new asset group.

When CVSS Scoring is enabled for the subscription, CVSS metrics appear and you can assign values. The CVSS metrics are used to calculate CVSS scores for vulnerabilities in scan status reports. For a new asset group, the service sets these values to “Not Defined” by default, following the CVSS Version 2 standards.
More information on business risk and CVSS scoring in reports is covered in the next chapter in “Enterprise Reporting.”

**Taking Workflow Actions**

Workflow actions allow you to take actions on selected hosts. When viewing map results, the Actions drop-down menu allows you to take several actions on selected hosts. The same workflow actions are available in map reports (using map templates) and other UI views such as the Asset Search Report and the Risk Analysis Report. Some actions are also available when viewing Host Assets and Domain Assets.
YOUR FIRST SCANS

Vulnerability scans analyze your network for vulnerabilities, using the Vulnerability KnowledgeBase hosted by the service, the industry’s largest and most comprehensive database of vulnerability signatures. Compliance scans may be performed when the policy compliance module is enabled in the subscription and the user has compliance management privileges. Compliance scans analyze your network using a library of technical controls hosted by the service. The option profile applied to each scan identifies customizable scan settings. See “Customizing Scans.”

BEST PRACTICES

Important! Do not scan your entire network at first. Instead start with a host, then a few hosts, move to a subnet or organizational unit, and then to an entire Class B or Class C. By limiting the scope of your first scans your scan results and remediation tasks are manageable. When you want to scan multiple IPs, use asset groups or asset tags as scan targets, instead of individual IPs.

Here are rollout steps for first scans that are used by several customers with successful rollout projects:

1. Select an option profile. For a vulnerability scan, we recommend “Initial Options” to get started. You can configure option profiles to customize scans. See “Customizing Scans.”
2. Scan 1 host and review the scan results.
3. Scan 1 subnet and review the scan results.
4. Determine which IP assets you want to scan on a regular basis, including workstations and all network devices including printers, routers, switches, servers, and wireless access points. Then create asset groups with these assets, or assign tags to them (use the AM application).
5. Scan your asset groups or asset tags and review the scan results.
6. Review your initial scan reports with management. This is an important step to ensure your continued success with Qualys within the organization.

Take steps towards setting expectations. While offering many tremendous benefits, scanning for security vulnerabilities can have potential impact to certain systems and configurations. Keep in mind that there can be issues with software not reported to the public or issues that we are not aware of. It’s recommended that you review the known issues covered in the Qualys document “Potential Impact to Systems” that is available in the Resources section (go to Help > Resources > Qualys Support). Publicizing this document to all parties involved will help to gain the trust and confidence of operating
teams and outsourcers. Our experience is that executive support of your security and compliance program and corporate communications to the parties involved in advance of your first scans is an advantage, leading to successful experience with scanning.

**Rollout Steps**

**Launch Scans.** The scan feature allows you to test the security of one or more hosts identified in your map report. By launching a scan on a selected host, you’ll receive a detailed scan report with the vulnerabilities detected on the target host.

![Scan workflow diagram](image)

**Figure 3-2. Scan workflow**

**Run scans on asset groups.** Before running scans define asset groups based on the host identification and prioritization steps you’ve already taken.

**Select option profile.** When launching a scan you’ll be required to select an option profile with scan settings. It’s recommended that you use the initial option profile provided by the service (for a vulnerability scan) to get started. You can create custom profiles with different settings. For trusted scanning, enable authentication in a profile and add authentication records with login credentials. See “Customizing Scans.”
Chapter 3 — Vulnerability Scanning
Your First Scans

**Review initial scan results.** As you are getting started, pay close attention to your scan results so that you can refine your scans and possibly your asset groups to best suit your organization’s needs. Next steps will involve setting up scheduled scans on your asset groups so that scans run automatically and new scan results are available for reporting. See “Add Scheduled Scans” in the next chapter.

**Select Scan Notification**

You can opt in to receive the Scan Complete Notification by editing your account under Notification Options. You can select “On” or “Off” for “Scan Complete Notification” and “On” or “Off” for “Scan Summary Notification (vulnerability scans only)”. 
Launch Vulnerability Scan

Select Scans from the top menu. Then from the scans list, select New > Scan.

In the Launch Vulnerability Scan window, enter a title for tracking (optional) and select target hosts (asset groups and/or IP addresses). For Option Profile, we recommend “Initial Options” to get started (see “Option Profile Settings”). When there are Scanner Appliances in your account, select a scanner option (see “Scanner Appliance Setting”). Click Launch to start the scan.

You’ll notice you can select asset tags as target hosts 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).

The scan status window appears automatically to show you the scan job status. You can safely close this window and open again from the scans list.
Scan Status

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

1) Scan Status Icons. A solid icon (filled-in) means all results available for the scan have been processed, meaning the host scan data (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/1349216272.43009)](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.

**Take Actions on Scans**

You can easily take actions on scans in the scans list. To act on multiple scans select the check boxes next to the scans and then select an option from the Actions menu (above the list). To act on a single scan, hover of a scan, click  and then select an action from the Quick Actions menu.

**Pause / Resume.** Select to pause a scan in progress, or resume a paused scan. When a scan is paused, scan results for hosts already scanned are saved. The scan remains paused until a user resumes or cancels the task (note the service cancels a paused scan automatically after 10 days). Once resumed, the remaining hosts will be scanned and all scan results will be combined into one scan results report.

**Cancel.** Select to cancel a scan in progress.

**Delete.** Select to delete one or more saved scans. Once deleted the saved scan results are not longer available for viewing and reporting.

**View.** Select to view scan results in HTML format for a finished scan, or scan status for a running scan.

**Download.** Select to download scan results in: PDF, HTML (.zip), MHT, XML or CSV.

**Relaunch.** Select to rescan a selected scan without having to enter the scan settings again. You will have the option to override the previous settings before relaunching.
Scan Complete Email for Vulnerability Scan

The Scan Complete email notification is sent when the scan status is “Finished” and you have turned on the option “Scan Complete Notification” in your account under Notification Options. Each email includes a scan summary and a secure link to the saved scan results report.

A sample Scan Complete email for a vulnerability scan is below showing vulnerability counts and trends. (For the first scan of a host in your subscription, there will be no trend information.)

From: Qualys Support
To: jkim@qualys.com
Date: Mon, Jun 04, 2017 at 10:44 AM
Subject: Qualys: Scan Completed

-----------------------------------------------------------------------------------------------------------

Email scan summary by Qualys

Scan Title (Status) : My First Scan
Start Date              : 06/04/2017 at 09:59:22 (GMT-0700)
Duration                 : 00:04:38
Target Groups          : No Group
Hosts Scanned  : 1
Active Hosts      : 1
Option Profile         : Initial Options
Launched By          : Jason Kim (quays_ak12)
Company               : Qualys, Inc.
Launch Type          : On demand
Scan Status     : Finished
Next Action     : None

-----------------------------------------------------------------------------------------------------------

Summary of discovered Vulnerabilities (Trend)

Severity 5 "Urgent" : 1 (-8)
Severity 4 "Critical" : 2 (-15)
Severity 3 "Serious" : 7 (-13)
Severity 2 "Medium" : 5 (-11)
Severity 1 "Minimal" : 1 (-3)
Total                 : 16

Summary of Potential Vulnerabilities
Severity 5 "Urgent" : 3 (+3)
Severity 4 "Critical" : 1 (+1)
Severity 3 "Serious" : 0 (=)
Severity 2 "Medium" : 2 (-2)
Severity 1 "Minimal" : 0 (-1)
Total : 6

Summary of Information Gathered
Severity 3 "Serious" : 4
Severity 2 "Medium" : 6
Severity 1 "Minimal" : 16
Total : 26

(+)(-)(=): Difference with previous detection for each host/vulnerability pair. For a complete explanation of trend information, refer to the online help.

Click here to view your full scan report:

For more information, please email your primary contact:
mailto:nwood@qualys.com

(c) Copyright 1999-2017 Qualys, Inc. All rights reserved.
http://www.qualys.com
Chapter 3 — Vulnerability Scanning
Your First Scans

View Scan Results

To view scan results for a completed scan (scan with status Finished), go to the scans list (go to Scans). Mouse over a scan (row), click and then select View from the Quick Actions menu. The scan results appears in a new window. Use the File menu to print the results and download to your file system in these formats: PDF, HTML, MHT and XML.

The service uses pre-defined settings for displaying scan results and those settings are not customizable.

The Report Summary gives a summary the scan task. Additional sections in the vulnerability scan results provide details about the vulnerabilities detected. Scrolling down, the Summary of Vulnerabilities is followed by Detailed Results.
The Summary of Vulnerabilities includes graphs.
Chapter 3 — Vulnerability Scanning
Your First Scans

Detailed Results

Detailed Results show a list of detected vulnerabilities sorted by host and characterized by operating system. The severity level icon is Red for a Confirmed vulnerability, Yellow for a Potential Vulnerability, and Blue for information gathered (see the Appendix for descriptions of the vulnerabilities and severity levels).

Click on a vulnerability title to see vulnerability details. THREAT is a description of the threat posed by the vulnerability, IMPACT describes the impact of the vulnerability if exploited, and SOLUTION is a verified solution for the issue provided by the service. Scrolling down further, additional details may be provided.

Compliance

COMPLIANCE information describes various government and industry-specific regulations that are associated with a detected vulnerability.
Exploitability

EXPLOITABILITY information may appear with vulnerability 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. Sample EXPLOITABILITY section:

Associated Malware

ASSOCIATED MALWARE information may appear with vulnerability details. 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 MALWARE section:

Results

RESULTS shows scan test results returned by the scanning engine, if any. Sample section:
About Scanning Events

Qualys has minimal impact on your network since its inference-based scanning engine intelligently runs only tests applicable to each target host.

Vulnerability scanning is a dynamic process that involves several main events. The standard behavior for these events is described below. You can modify this behavior by customizing an option profile and applying the profile to the scan request.

**Host Discovery.** The service checks availability of target hosts. For each host, the service checks whether the host is connected to the Internet, whether it has been shut down and whether it forbids all Internet connections. The service pings each target host using ICMP, TCP, and UDP probes. The TCP and UDP probes are sent to default ports for common services on each host, such as DNS, TELNET, SMTP, HTTP and SNMP. If these probes trigger at least one response from the host, the host is considered “alive”. If the host is not “alive” then the scan process will not proceed. The types of probes sent and the list of ports scanned during host discovery are configurable in the option profile applied to the scan.

After host discovery, these events occur dynamically: port scanning, operating system detection, service discovery and authentication to hosts.

**Port Scanning.** The service finds open TCP and UDP ports on target hosts. The list of TCP and UDP ports scanned is configurable in the option profile.

**Operating System Detection.** The service attempts to identify the operating system installed on target hosts. This is accomplished through TCP/IP stack fingerprinting, OS fingerprinting on redirected ports, and is enhanced by additional information gathered, such as NetBIOS information gathering.

**Service Discovery.** When a TCP or UDP port is reported as open, the scanning service uses several discovery methods to identify which service is running on the port, and confirms the type of service running to obtain the most accurate data.

**Authentication.** The service authenticates to target hosts. Authentication to hosts is optional for a vulnerability scan. For a vulnerability scan with authentication enabled, the service authenticates to target hosts based on the selected authentication types in the option profile and the authentication records in the user account. If authentication to a host is not successful, the service performs vulnerability assessment without authentication. (Note: For a compliance scan, authentication is required.)

**Assessment.** The assessment scanning event occurs after all previous events. The service begins vulnerability assessment using the information gathered about each target host in the previous scanning steps. The service scans for all vulnerabilities in the KnowledgeBase or a selected list of vulnerabilities, based on the user’s scan settings. The service runs vulnerability tests that are applicable to each target host based on the information gathered for the host.
VULNERABILITY KNOWLEDGEBASE

Vulnerabilities are used for vulnerability scanning and reporting. Qualys has the industry’s largest and most complete 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, without requiring software to install and maintain.

In the upper right corner, you’ll see the total number of vulnerabilities next to options for paging through the list. Using the arrow icons you can go to the next page, previous page, first page and last page. Using the page selector drop-down menu, you can jump to a list section.

Each entry in the vulnerabilities list provides summary information about a particular vulnerability, including the QID (Qualys ID), vulnerability category, title and severity level. Links to related CVE names and vendor references are displayed when available.

Want to view vulnerability information? Mouse over a vulnerability (row), click and then select Info from the Quick Actions menu. Use the wizard to drill down to various sections with general information, QID details, descriptions for impact, threat and solution, and correlation information for exploitability and associated malware.

You’ll notice the Title column includes icons for vulnerability identification. You can mouse over the icons to understand their meaning.
These icons indicate the assigned Discovery Method.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
<td>Remote Discovery Only. When the Remote Discovery icon appears without the Authenticated Discovery icon, the vulnerability can be detected only using remote (unauthenticated) scanning.</td>
</tr>
<tr>
<td>👤</td>
<td>Authenticated Discovery Only. When the Authenticated Discovery icon appears without the Remote Discovery icon, the vulnerability can be detected only using authenticated scanning. Hover your mouse pointer over the icon to see the authentication technology type(s).</td>
</tr>
<tr>
<td>🕵️‍♂️ 👤</td>
<td>Remote or Authenticated. When both the Remote Discovery icon and the Authenticated Discovery icon appear together, the vulnerability can be detected using remote scanning or authenticated scanning. Hover your mouse pointer over the Authenticated Discovery icon to see the authentication technology type(s).</td>
</tr>
</tbody>
</table>

These icons provide additional information about a vulnerability.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>The severity level has been edited (by a Manager). The text content (Impact, Threat, Solution) and/or the severity level may have been edited.</td>
</tr>
<tr>
<td>🔴</td>
<td>A patch is available.</td>
</tr>
<tr>
<td>🔭</td>
<td>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.</td>
</tr>
<tr>
<td>🔵</td>
<td>Malware information is associated with this issue. The service correlates malware information with vulnerabilities when malware threats for vulnerabilities are published in the Trend Micro Threat Encyclopedia.</td>
</tr>
</tbody>
</table>
Vulnerability Severity Levels

Qualys vulnerabilities are automatically classified by severity level in vulnerability scan reports.

**Confirmed Vulnerabilities**

A Confirmed Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote attackers. Depending on the severity of the security risk, a successful exploitation of a Confirmed Vulnerability can vary from the disclosure of information to a complete compromise of the host.

<table>
<thead>
<tr>
<th>Severity icon</th>
<th>Severity level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="5-Urgent" /></td>
<td>5 - Urgent</td>
<td>Intruders can easily gain control of the host, which can lead to the compromise of your entire network security.</td>
</tr>
<tr>
<td><img src="image" alt="4-Critical" /></td>
<td>4 - Critical</td>
<td>Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information.</td>
</tr>
<tr>
<td><img src="image" alt="3-Serious" /></td>
<td>3 - Serious</td>
<td>Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders.</td>
</tr>
<tr>
<td><img src="image" alt="2-Medium" /></td>
<td>2 - Medium</td>
<td>Intruders may be able to collect sensitive information from the host. With this type of information, intruders can easily exploit known vulnerabilities specific to software versions.</td>
</tr>
<tr>
<td><img src="image" alt="1-Minimal" /></td>
<td>1 - Minimal</td>
<td>Intruders can collection information about the host and may be able to use this information to find and exploit other vulnerabilities.</td>
</tr>
</tbody>
</table>

**Potential Vulnerabilities**

A Potential Vulnerability is a vulnerability that we cannot confirm exists. In these cases, at least one necessary condition for the vulnerability is detected. The only way to verify the existence of this type of vulnerability would be to perform an intrusive scan on your network, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate potential vulnerabilities further. The service can verify the existence of some potential vulnerabilities when trusted scanning is enabled.
### Severity icon

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 - Urgent</td>
<td>If the vulnerability exists, intruders can easily gain control of the host, which can lead to the compromise of your entire network security.</td>
</tr>
<tr>
<td>4 - Critical</td>
<td>If the vulnerability exists, intruders can possibly gain control of the host or there may be potential leakage of highly sensitive information.</td>
</tr>
<tr>
<td>3 - Serious</td>
<td>If the vulnerability exists, intruders may be able to gain access to information stored on the host, including security settings. This could result in potential misuse of the host by intruders.</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>If the vulnerability exists, intruders may be able to collect sensitive information from the host. With this type of information, intruders can easily exploit known vulnerabilities.</td>
</tr>
<tr>
<td>1 - Minimal</td>
<td>If the vulnerability exists, intruders can collect information about the host and may be able to use this information to find and exploit other vulnerabilities.</td>
</tr>
</tbody>
</table>

### Information Gathered

Information Gathered is a vulnerability that includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered issues include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 - Serious</td>
<td>Intruders may be able to detect highly sensitive data, such as global system user lists.</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>Intruders may be able to determine the operating system running on the host and view banner versions.</td>
</tr>
<tr>
<td>1 - Minimal</td>
<td>Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and firewalls.</td>
</tr>
</tbody>
</table>

The half red/half yellow severity level icon (-half red-half yellow) identifies a vulnerability that may be confirmed in some cases during a scan. If the vulnerability is confirmed, it appears as a vulnerability with a red severity level in the scan results. If the vulnerability cannot be confirmed, it appears as a potential vulnerability with a yellow severity level.
Vulnerability Search

When viewing the KnowledgeBase, click Search above the list area to search for vulnerabilities by attributes. Many options are provided, including QID (vulnerability ID), vulnerability title, discovery method, authentication type required for detection, vulnerability severity levels, whether the vulnerability has patches, has a certain vendor reference and more.

![Search Dialog](image)

Scroll down to search for vulnerabilities by vendor and/or product associated with them. Vendor and product information is provided by NIST as part of CVE information. Important! Not all vulnerabilities (QIDs) have an associated vendor and product information from NIST. This means if you search for a certain vendor name, the search results may not list all QIDs associated with that vendor.

Vulnerability Search Lists

A search list identifies a set of vulnerabilities that users can add to business objects in their accounts. Search lists provide a convenient and flexible way for users to select vulnerabilities for custom scans (in option profiles), scan reports (in scan report templates) and automatic ticket generation (in remediation rules). Users may define custom search lists including any number of vulnerabilities, and the service provides a library of ready-made search lists that users can import.

There are two types of search lists: Static and Dynamic. For a static list, the user defines a vulnerability list consisting of vulnerability IDs (QIDs). For a dynamic list, the user defines vulnerability search criteria so the vulnerability list is updated automatically over time.
For example, a user may define a dynamic list with all Apache vulnerabilities and add this to an option profile. A dynamic list is created by the service when a scan is launched with this option profile. In this way, the dynamic list is updated automatically as new Apache QIDs are added and new patch information becomes available.

To view the search lists in your account, click KnowledgeBase on the top menu and then click the Search Lists tab.

There are many ways to use vulnerability search lists in your account. Here are a few ways you can use search lists:

- Create a static list of QIDs for troubleshooting and verifying Windows authentication. (See the help topic “Verifying Authentication (Vulnerability Scans)” for a list of QIDs to include.)
- Create a static list of QIDs to exclude from scans.
- Create a dynamic list for an always up-to-date Microsoft patch Tuesday scan report, scan option profile and remediation rule.
- Create a dynamic list of QIDs flagged for PCI compliance.
- Create a dynamic list of QIDs for a particular vendor or product, such as Apache, Cisco, Microsoft, or Sendmail.
- Create a dynamic list of QIDs that are remotely exploitable on the .net framework.
Import Search Lists from the Library

The Search List Library contains both pre-configured static and dynamic search lists provided by the service.

To import search lists from the library, select New > Import from Library. Select the check boxes next to the search lists you want and click Import. The selected search lists appear in your search lists data list.

Add Static Search List

A Static search list identifies a saved list of vulnerabilities (QIDs). Using static search lists is useful when you want to include a specific list of QIDs for testing, reporting and remediation.

To add a static search list, go to KnowledgeBase > Search Lists. From the search lists area, select New > Static List. Enter a title to identify the list. Go to the QIDs section and select vulnerabilities from the KnowledgeBase that you want to add. You may select any number of vulnerabilities for the list.

Add Dynamic Search List

A Dynamic search list identifies a set of vulnerability search criteria such as severity level, category, CVSS score, patch availability, etc. The service creates a list of vulnerabilities at run time based on the search criteria. Using dynamic search lists is useful when you want the service to automatically include QIDs that are newly added to the KnowledgeBase and QIDs that are updated with new information like patch availability.
To add a dynamic search list, go to KnowledgeBase > Search Lists. From the search lists area, select New > Dynamic List. Enter a title to identify the list. Under Criteria, select vulnerability search criteria.

**Editing Vulnerabilities**

Editing vulnerabilities gives Managers greater control over how vulnerabilities appear online and within reports and how they are prioritized for remediation. Customized settings are global and appear to all users in the subscription.

To edit a vulnerability, go to the KnowledgeBase. From the vulnerabilities list, select a vulnerability (row), click and then select Edit from the Quick Actions menu. Use the Edit Vulnerability wizard to edit settings. You can change the severity level, disable the vulnerability, and add custom comments for the Threat, Impact and Solution. The Restore Defaults option allows you to reset the vulnerability settings to the defaults provided by the service.
OVAL Support

OVAL stands for the Open Vulnerability and Assessment Language, which is an international information security baseline standard to check for the presence of vulnerabilities and configuration issues on computer systems. The OVAL standard includes vulnerability definitions and schemas.

Qualys supports the OVAL standard, including OVAL definitions for Windows file and registry tests plus compound tests. Using Qualys you can add OVAL version 4.0, 4.1 and 4.2 vulnerabilities to the KnowledgeBase.

To add an OVAL vulnerability (Manager only), go to the KnowledgeBase. From the vulnerabilities list, select New > OVAL Vulnerability and follow the workflow provided. Once added, any user in the subscription can scan and report on the OVAL vulnerability.
CUSTOMIZING SCANS

Qualys supports customization of scans, giving users the ability to scan specific ports and specific vulnerabilities as needed, to enable trusted scanning, and to fine-tune parameters. These scan options are specified in profiles. When launching or scheduling scans, users apply an option profile to the task. For vulnerability scans, Qualys provides pre-defined option profiles, and users with scanning privileges can create custom profiles.

BEST PRACTICES

Use “Initial Options” to get started. Qualys provides the “Initial Options” profile with standard settings based on our experience with supporting Qualys users.

Learn about the option profiles provided. Review the option profiles provided and use them to run scans before creating new profiles.

ROLLOUT STEPS

Scanner Appliance setting. External scanners are available for external scanning. When there are Scanner Appliances in your account, you may select another scanner option. Note that you cannot select external scanners to scan private use internal IPs.

View your option profiles. The service provides pre-defined profiles in your account for vulnerability scans. Other profiles may also be listed. View the list of option profiles to learn about them. You can create, edit, delete, and view profiles from the option profiles list.

Edit option profiles. Add, edit, and delete option profiles as needed. Before launching a compliance scan, you need to create at least one compliance profile.

Scanner Appliance Setting

The Scanner Appliance setting for a scan may be set to one of these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>This option is set by default when there are no Scanner Appliances in your account. Select this option to use external scanners for external (perimeter) scanning.</td>
</tr>
<tr>
<td>Scanner Appliance name</td>
<td>Select a Scanner Appliance name to use a particular Scanner Appliance for internal scanning.</td>
</tr>
</tbody>
</table>
Chapter 3 — Vulnerability Scanning
Customizing Scans

Option Profiles Provided

These option profiles are provided by the service for vulnerability scans:

- Initial Options. Qualys recommends this as a starting point for new users.
- Qualys Top 20 Options. Use to scan for the Qualys Top 20 real-time vulnerabilities.
- SANS 20 Options. Use to scan for the SANS Top 20 vulnerabilities, published by The SANS Institute. (Important: The SANS Top 20 list was last updated in 2008. For more accurate information on the most prevalent and critical real-world vulnerabilities use the Qualys Top 20 list.)
- Payment Card Industry (PCI) Options. Use to perform a scan that analyzes whether target hosts are compliant with the Payment Card Industry Data Security Standard (PCI DSS). See “Online Merchants and Retailers” in Chapter 5.

View Option Profiles

To view the option profiles in your account, go to Scans > Option Profiles.
Chapter 3 — Vulnerability Scanning
Customizing Scans

Option Profile Settings

An option profile is applied to each vulnerability scan task. Each option profile consists of many settings. You can customize these settings when editing an option profile. The option profile “Initial Options” is provided by the service to assist you with getting started with vulnerability scans.

To edit an option profile, go to Scans > Option Profiles. From the option profiles list, select an option profile (row), click ➕ and then select Edit from the Quick Actions menu.

Option Profile — Scan Settings

The settings in the Scan section affect how the service performs scans.

<table>
<thead>
<tr>
<th>Scan Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned TCP Ports</td>
<td>Select which TCP ports are scanned.</td>
</tr>
<tr>
<td></td>
<td>Initial setting: Standard Scan (about 1800 ports)</td>
</tr>
<tr>
<td>Scanned UDP Ports</td>
<td>Select which UDP ports are scanned.</td>
</tr>
<tr>
<td></td>
<td>Initial setting: Standard Scan (about 180 ports)</td>
</tr>
</tbody>
</table>
### Scan Option Description

<table>
<thead>
<tr>
<th>Scan Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform 3-way Handshake</td>
<td>Specify whether 3-way handshake with target hosts is performed. After a connection between the service and the target host is established, the connection is closed. This option should only be enabled when your network does not allow a SYN packet to be followed by an RST packet.</td>
</tr>
<tr>
<td>Authoritative Option</td>
<td>Specify whether the authoritative option is enabled. When enabled, the results from light port scans and scans on customized port lists affect the vulnerability status for all vulnerabilities on target hosts, not just vulnerabilities detected on the scanned ports.</td>
</tr>
<tr>
<td>Scan Dead Host</td>
<td>Specify whether dead hosts are scanned. A host that does not respond to service checks and pings is considered dead and scan processing is terminated. Enabling this option causes the scan processing to continue and this may substantially increase scan time.</td>
</tr>
<tr>
<td>Load Balancer Detection</td>
<td>Specify whether load balancer detection is enabled. When enabled, the service attempts to determine the number of web servers behind each load balancer and reports this information in scan results (QID 86189).</td>
</tr>
<tr>
<td>Performance</td>
<td>Specify the overall performance level for scans. This level consists of individual performance settings, including the maximum number of hosts to scan in parallel, the maximum number of processes to run in parallel per host, and packet delay. Select a pre-defined performance level (Normal, High, Low) or create a custom one.</td>
</tr>
</tbody>
</table>

Initial setting: Disabled
### Scan Option

**Password Brute Forcing**

Specify the level of password brute forcing performed by scans. You may select No Brute Forcing, System, or Custom.

When System is selected, the service attempts to guess the password for each detected login ID on each target host. Select a level from the menu (from Minimal to Exhaustive).

When Custom is selected, the service uses the brute force lists saved in the option profile to test login combinations on target hosts.

Initial setting: No Brute Forcing

### Vulnerability Detection

Select the vulnerabilities that you would like to scan for:

Select one of these settings (required):
- “Complete” to scan for all vulnerabilities, except OVAL.
- “Custom” to scan for a custom set of vulnerabilities. When selected you are prompted to add one or more search lists. Up to 10 search lists may be added.
- “Select at runtime” allows the user to select vulnerabilities at runtime (for on demand scans only).

Select these settings as appropriate (optional):
- “OVAL checks” to scan for user-defined OVAL vulnerabilities.
- “Basic host information checks” for a Custom scan to ensure vulnerabilities that identify basic host information are included (such as operating system and hostname).
- “Exclude QIDs” to exclude certain vulnerabilities from scans. When selected you are prompted to add one or more search lists.

Initial setting: Complete

### Authentication

Specify whether to enable authenticated trusted scanning for Windows, Unix/Cisco IOS, Oracle, Oracle Listener and/or SNMP. When enabled, credentials specified in authentication records in your account will be used for authentication to hosts.

Initial setting: Disabled
**Option Profile — Additional Settings**

The settings in the Additional section affect how the service performs host discovery for both maps and vulnerability scans. The initial settings are recommended as best practice in most cases and should be customized only under special circumstances.

<table>
<thead>
<tr>
<th>Scan Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Enumeration</td>
<td>Specify whether to enable Windows Share Enumeration. When enabled, the scanning engine checks Windows shares that are readable by Everyone and returns the number of files for each share on each host. (Only available if the Dissolvable Agent is accepted for the subscription.) Initial setting: Disabled</td>
</tr>
</tbody>
</table>

Additional settings include:

- **Host Discovery**
  - **TCP Ports**
    - Standard Scan (13 ports)
    - Additional (max: 1-6, 1024)
  - **UDP Ports**
    - Standard Scan (5 ports)
    - Custom
  - **ICMP**

- **Blocked Resources**
  - Specify ports protected by your firewall/IDS. This option overrides TCP and UDP port settings on the Scan tab and is only applicable to scans.
  - Predefined firewall blocked ports
  - Custom port list
Additional section settings in an option profile are described below.

<table>
<thead>
<tr>
<th>Additional Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Discovery</td>
<td>Specify which probes are sent and which ports are scanned during host discovery. Settings affect how the service detects hosts and determines if hosts are alive.</td>
</tr>
<tr>
<td></td>
<td>Initial settings:</td>
</tr>
<tr>
<td></td>
<td>TCP Ports - Standard Scan (maximum 20 ports)</td>
</tr>
<tr>
<td></td>
<td>UDP Ports - Standard Scan (maximum 6 ports)</td>
</tr>
<tr>
<td></td>
<td>ICMP - Enabled</td>
</tr>
<tr>
<td>Blocked Resources</td>
<td>Specify which ports are blocked and which IP addresses are protected by your firewall/IDS. This option applies to scans only, not maps. If scans trigger your firewall or IDS it’s likely that the scans will be aborted. Note: The recommended method for allowing the service access to your network is to add the scanner IP addresses to your firewall/IDS white list. Initial setting: Disabled</td>
</tr>
<tr>
<td>Ignore firewall-generated TCP RST packets</td>
<td>Some filtering devices, such as firewalls, may cause hosts to appear alive by sending TCP Reset packets using host IP addresses. Initial setting: Disabled</td>
</tr>
<tr>
<td></td>
<td>When this option is enabled for scan tasks, the service ignores all TCP Reset packets. When specified for map tasks, the service ignores TCP Reset packets generated by one or more filtering devices.</td>
</tr>
<tr>
<td>Ignore firewall-generated SYN-ACK packets</td>
<td>Some filtering devices, such as firewalls, may cause hosts to appear alive when they aren’t by sending SYN-ACK packets. When this option is enabled, the service attempts to discover if TCP SYN-ACK packets are generated by filtering devices. If so, all TCP SYN-ACK packets originating from these devices are ignored. Initial setting: Disabled</td>
</tr>
<tr>
<td>Do not send ACK or SYN-ACK packets during host discovery</td>
<td>Some firewalls are configured to log an event when out of state TCP packets are received. When this option is enabled, the service does not send out of state ACK and SYN-ACK packets during host discovery. Initial setting: Disabled</td>
</tr>
<tr>
<td></td>
<td>Note: If you enable this option and the option “Perform 3-way handshake” (in the Scan section), then the option “Perform 3-way handshake” takes precedence.</td>
</tr>
</tbody>
</table>
CURRENT HOST INFORMATION

After hosts are scanned, you can view current host information from several spots in the user interface, including your host assets list, asset search report and remediation tickets. The host information view includes current vulnerability status and configurations that include the host, such as asset groups, business units, users and remediation tickets. Compliance and exception status is listed when the policy compliance module is enabled.

To view current host information, go to Assets > Host Assets. Navigate to a host in the list and click (View host information) next to the host. The Host Information pop-up appears. You will see many sections in the host information view. You can expand a section by clicking the section title.

The Vulnerabilities section identifies the current vulnerabilities based on the most recent vulnerability scan of the host.

The Compliance section appears when the policy compliance module is enabled. This section lists the compliance policies that apply to the host with current compliance status.
An enterprise management program should include plans for security auditing, reporting and remediation. It’s recommended that you form an enterprise management plan addressing these constituent parts and publish the plan to all parties involved. When developing your plan, keep in mind that it’s best to start with a phased approach to security auditing, reporting and remediation with realistic goals.

For enterprise management to be successful, it’s important to understand the needs of the different parties involved. Learning when it’s best to schedule scans and maps often requires discussion with multiple corporate groups — users responsible for scanning as well as IT and network groups. Be sure to document your procedures thoroughly and set expectations within the organization on the frequency and scope of security auditing.

To implement an enterprise management program in the quickest time, please complete the following activities in the order presented:

- ENTERPRISE SECURITY AUDITING
- ENTERPRISE REPORTING
- REMEDIATION WORKFLOW
- CUSTOMIZING LEVEL OF RISK
ENTERPRISE SECURITY AUDITING

Develop a security auditing plan for your enterprise. This involves determining frequency of scans for both ad hoc and scheduled scans, as well as user responsibility. Documenting your plan will assist with building internal confidence.

Before you begin, be sure to complete the rollout steps discussed in Chapters 2 and 3.

BEST PRACTICES

Define a scanning policy. Determine how frequently scans will occur and who will be responsible for which scans. Since your trend reports will incorporate scan results, consider your reporting requirements when defining your scanning policy.

Schedule scans. Our customers are most successful and see the most remediation progress by running scheduled scans on a regular basis. Following this best practice ensures that there are scan results data that can be incorporated into trend reports at all times.

ROLLOUT STEPS

Add scheduled scans. Setup scheduled scans to run on a regular basis. We recommend that you scan hosts at least monthly. Separate scheduled tasks running at different times may be easily setup to do this.

Review your option profiles. Review your option profiles for vulnerability scans. You can view the option profiles list and detailed information about each profile. Be sure to review the default option profile and understand its function.

Define option profiles. Qualys provides option profiles for vulnerability scans that you can use right away. You may edit the option profiles provided or create new ones to suit your organization’s needs. (For compliance scans, you need to create at least one compliance profile). Settings in option profiles enable scanning for selected vulnerabilities and trusted scanning. Manager users can create global option profiles which are automatically published to user accounts with scanning privileges.

Check Scanner Appliance status. From your scanner appliances list you can view detailed information about the scanners in your account and identify whether they have passed the most recent health check and whether they are currently performing scans.

Use Scanner Parallelization for large scans. Use the scanner parallelization feature to distribute scanning across multiple Scanner Appliances in parallel to increase scan speed when scanning a large number of hosts. This feature is available for on demand and scheduled scans.
Add Scheduled Scans

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.

To add a new scheduled task, go to Scans > Schedules. From the schedules list, select New > Vulnerability Schedule Scan. Use the wizard to enter a schedule title and settings.

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

Please note:

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

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

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

Each vulnerability scan is assigned an option profile. The settings in the profile affect the way the service performs scans on target hosts.

To view your option profiles, go to Scans > Option Profiles. The option profile list includes the service-provided profiles and any profiles created by you or other users in the subscription.

The “Initial Options” profile has settings that we recommend as a starting point for new users. See “Option Profiles Provided” in Chapter 3.

Users privileges to option profiles depends on the user’s assigned user role and assets.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Option Profiles in list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>- all profiles in the subscription (global and user created)</td>
</tr>
<tr>
<td>Unit Manager</td>
<td>- profiles created by the user</td>
</tr>
<tr>
<td></td>
<td>- profiles created by other users in the same business unit</td>
</tr>
<tr>
<td></td>
<td>- global profiles</td>
</tr>
<tr>
<td>Scanner</td>
<td>- profiles created by the user</td>
</tr>
<tr>
<td></td>
<td>- global profiles</td>
</tr>
<tr>
<td>Reader</td>
<td>- global profiles</td>
</tr>
</tbody>
</table>

You can add an option profile, which may be applied to vulnerability scans, by editing a profile provided by the service or creating a new one. See “Customizing Scans” in Chapter 3 for details on the scan settings.
Set Default Option Profile

The “Initial Options” profile is designated as the default option profile for vulnerability scans and maps in a new subscription. The default profile ensures consistency in scanning and scan results when there are multiple users running scans. A Manager user may edit this profile or designate another profile as the default.

Publish Global Option Profiles

Global option profiles can be created to publish profiles to multiple users, which is important for achieving consistency in reporting and compliance with government and industry-specific regulations. Global option profiles may be created for the subscription and for business units. Only users with management privileges can create global option profiles.

<table>
<thead>
<tr>
<th>Global — Subscription</th>
<th>Global option profiles that are available to all users in the subscription. Only Managers can create these profiles.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global — Business Unit</td>
<td>Global option profiles that are available to all users in the same business unit. Only Unit Managers can create these profiles for their own business unit.</td>
</tr>
</tbody>
</table>

To designate an option profile as a global option profile, edit the profile and select the option “Make this a globally available option profile”.

Scan for Selected Vulnerabilities

You can scan for selected vulnerabilities — a very useful way to check for the most recent worm outbreak, the latest vulnerabilities announced by Microsoft on the second Tuesday of every month. To enable this type of scanning you must make selections in the option profile, in the Scan section under Vulnerability Detection.
When “Complete” is selected the service runs all vulnerability checks in the KnowledgeBase, except any custom OVAL checks. Select “OVAL checks” to include OVAL checks.

Select “Custom” to scan for a custom set of vulnerabilities in one or more search lists. When you select “Custom” the search list section opens, as shown below, and you are prompted to add search lists. Select Add Lists and select search lists (up to 10) with the vulnerabilities you want to exclude from scanning, and then click OK. When “Custom” is selected, we recommend you select “Basic host information checks”.

The “Exclude” option is used to exclude certain vulnerabilities. When this option is selected, you are prompted to select search lists (similar to the “Custom” option). Select Add Lists and select search lists (up to 10) with the vulnerabilities you want to exclude from scanning, and then click OK.
Trusted Scanning

Trusted Scanning allows organizations to systematically audit their network infrastructure without the burden of deploying agents on every desktop and server. With trusted scanning, more system intelligence is gathered from target hosts.

Qualys offers trusted scanning for Windows, Unix, Oracle, SNMP, Cisco IOS, VMware, IBM DB2, MS SQL Server (for compliance scans) and more. Oracle Listener authentication allows users to obtain a list of Oracle System IDs (SIDs) discovered behind the Listener. With this list you can create Oracle records for the SIDs and perform trusted scans.

Good to Know:

- For vulnerability scans, authentication to hosts is required for trusted scanning. If authentication to a host fails the service performs standard scanning for vulnerabilities. Scan results will show vulnerabilities detected, if any.

- For compliance scans, authentication to hosts is required. If authentication to a host fails, the host is not scanned.

Add Authentication Records/Vaults

Authentication records and vaults identify credentials to be used for authentication to selected hosts. Managers and Unit Managers may create/edit authentication records/vaults.

Managers have permission to create authentication records/vaults and edit any authentication record/vault created by any user.

Unit Managers who are granted the permission “create/edit authentication records/vaults” in their user account will have permission to create these configurations. A Unit Manager with this permission will have the ability to: create authentication records which contain IP addresses in their own business unit, edit any authentication record which contains at least one IP address in their own business unit, create new authentication vaults, and edit their own vaults. Managers may grant any Unit Manager this permission; a Unit Manager who has this permission in their own account may grant this permission to another Unit Manager in the same business unit.

To add a new authentication record, go to Scans > Authentication. Then select New and a record type, for example Windows Record or Unix Record.
When defining a Windows or Unix record, you have the option to use an authentication vault in your account. To add a new authentication vault, select New > Authentication Vaults to go to the vaults list. From the vaults list, select New > Cyber-Ark PIM Suite, New > Thycotic Secret Server, or New > Quest Vault (for Quest One Privileged Password Manager, formerly e-DMZ Par).
Configure an Option Profile

For a vulnerability scan, authentication is enabled in an option profile. Select authentication types that you want to use. When you launch a scan we’ll look for authentication records corresponding to the authentication types you’ve selected and attempt authentication using the matching records.

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. Such an increase in scan speed allows scanning all ports when required.

The scanner parallelization feature allows you to distribute a scan task to multiple Scanner Appliances, when the scan target includes asset groups. When enabled, the scan task is distributed to multiple Scanner Appliances in parallel. The first 5 Scanner Appliances added to each target asset group make up the pool of scanners used to scan the group’s IP addresses. At the completion of the scan, the service compiles a single report with scan results.
Scanner parallelization is available for both on demand and scheduled scans. To select this scanner option, select “All Scanners in Asset Group” from the Scanner Appliance drop-down menu. (This menu appears when Scanner Appliances are in your account.)

The service can apply the “All Scanners in Asset Group” option for scanner parallelization when you submit a scan task on asset groups. If you wish to submit a scan task on individual IP addresses/ranges instead of asset groups, a Scanner Appliance must be applied to the task.

During scan processing, if a Scanner Appliance is not available for some reason, perhaps because it is offline, the service automatically distributes the scan task to another appliance in the same asset group.

A scan task may be distributed across Scanner Appliances that have the same software versions — vulnerability signatures and scanner — at the time of the scan. If one of the Scanner Appliances in the pool has a software version that does not match the other Scanner Appliances, then it will not be used. If some Scanner Appliances have identical software versions and others do not, then appliances with the most matching versions are used, regardless of whether the software is the most current. For example, if 3 appliances have the same software version and the other 2 appliances have a different version, then the 3 appliances with the same software version are used.
ENTERPRISE REPORTING

Develop a network security reporting plan for your enterprise. This involves determining frequency of running reports, as well as user responsibility. Documenting your plan will assist with building internal confidence.

We’ll be discussing reporting capabilities that are available when your account has Report Share enabled - this is a subscription level feature. Report Share allows users to run all report types and share them automatically with other users. Want to know if this is enabled for your account? Go to VM > Reports. If you see the Reports tab then Report Share is enabled.

BEST PRACTICES

Define a reporting policy. Determine the types of reports needed, who will review the various reports, who will be responsible for producing the reports, and the frequency with which they will be produced.

Regularly run reports. Our customers are most successful and see the most remediation progress by running reports on a regular basis. We recommend that you run status and trend reports at least monthly, and status reports in between as needed.

ROLLOUT STEPS

View templates and run reports. Several pre-defined report templates are available to all users at any time. Run these reports right away to view your security status.

Define report templates. Global templates can be created by users with management privileges and published to all users for consistency in reporting.

Schedule reports. By scheduling reports you can run reports at a particular time and ensure the latest scan results information is included.

Report sharing. Run all report types and share them with other users from a central location. You can schedule reports to run at a certain date and time in the future when this feature is enabled for your subscription. Completed reports are available to users based on user role. Managers and Unit Managers have the ability to distribute reports to the right people at the right time.

Download data lists. Most data lists throughout the user interface can be downloaded to these formats: CSV, XML, HTML, and MHT.
Chapter 4 — Enterprise Management and Reporting
Enterprise Reporting

View Report Templates

Several reporting options are offered through template-based reports for all report types. Several report templates are provided and others are available in the Template Library, allowing you to quickly create reports based on data in your account. Scan and map reports are fully customizable through templates.

To view the available report templates, go to Reports > Templates.

The Type column identifies the type of report: ⚒ for a scan report, ✔ for a compliance report, ✡ for a map report, 🔧 for a remediation report and 🔱 for a patch report. To run a report, click Run (✔) next to a report and follow the prompts. When Report Share is enabled the report is launched using the Report Share functionality.

Users’ privileges to report templates depends on their assigned user roles and assets.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Report Templates available to Run and Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>- all templates in the subscription (global and user created)</td>
</tr>
<tr>
<td>Unit Manager</td>
<td>- templates created by the user</td>
</tr>
<tr>
<td></td>
<td>- templates created by other users in the same business unit</td>
</tr>
<tr>
<td></td>
<td>- global templates</td>
</tr>
<tr>
<td>Scanner</td>
<td>- templates created by the user</td>
</tr>
<tr>
<td></td>
<td>- global templates</td>
</tr>
<tr>
<td>Reader</td>
<td>- templates created by the user</td>
</tr>
<tr>
<td></td>
<td>- global templates</td>
</tr>
</tbody>
</table>
Running Reports with Report Share

Report Share provides a centralized location for launching, sharing and managing reports. When Report Share is enabled in your account, you launch a report as follows. Select Reports from the top menu and click the Reports tab. From the reports list, select New > Scan Report > Template based. The New Scan Report window appears.

A scan report for the High Severity Report template is below. When you select a report template, the template settings appear automatically for format and report source. You can choose to override these settings.

Enter report settings: Enter a title, select the report format and template, review the report source (asset groups and/or IP addresses) and update settings if needed. To run an on-demand report: Click Run. Your report will be launched right away and you can view it in the reports list.

The “Scheduling” option allows you to schedule a report as part of the run report workflow. A separate workflow for scheduling reports is also available from the Reports > Schedules tab. See “Scheduling Reports.”
Enterprise Reporting

The finished report and its status appears on the Reports tab where you can track its progress. Once the report is Finished, click to view the report.

For each report, this information is provided: the report title, type, the report template, the user who launched the report, the report format, the date/time when the report was created, the report expiration date, the report size (in megabytes), and the report status (percentage complete or Finished).

A report is saved in your account for 7 days after its creation date by default. Each user is assigned a storage space limit in Report Share (scan and map results are not included in this space). Managers can adjust the user limit (go to Reports > Setup > Report Share).

Use the Actions menu (above the list) to take actions on one or more selected reports.

Select Delete to delete one or more saved reports if you want to delete them before they expire (by default reports expire in 7 days).

Select Cancel one or more running reports.

Use the Quick Actions menu to take actions on a selected report.

Select Info to view report information. From the information page, Managers, Unit Managers and Auditors can grant users access to the report.

Select Download to download the report in the saved format to the local file system.

Select Schedule to schedule the report to run again at a later time or on a recurring schedule.
Scheduling Reports

Scheduled reporting allows users to automatically generate reports at scheduled times. For example, you can schedule reports to run at important milestones, like the last day of the quarter, without having to depend on someone logging in to do it. Scheduling reports is possible when Report Share is enabled for your subscription and a Manager has enabled the Scheduled Reporting feature.

Select the “Scheduling” option under Report Options to enter schedule settings. This option is available in the new report workflow and in the report schedule wizard (go to Reports > Schedules, select New and then a report type).

Select “Notification” if you want to send an email notification when the report is complete. The report will be sent according to the report distribution method set for your subscription as shown. (To configure this, go to Reports > Setup > Schedule Reports). You can password protect the report and limit the total number of downloads.
Sharing Reports

Sharing reports allows business line managers to distribute reports to the right people at the right time. Managers and Unit Managers have the ability to share reports with users who do not have access to reports due to their assigned user roles. By default reports are available to users based on their user role.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Reports in Report History List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>- reports launched by all users in the subscription</td>
</tr>
<tr>
<td>Unit Manager</td>
<td>- reports launched by the user</td>
</tr>
<tr>
<td></td>
<td>- reports launched by other users in the same business unit</td>
</tr>
<tr>
<td>Scanner</td>
<td>- reports launched by the user</td>
</tr>
<tr>
<td>Reader</td>
<td>- reports launched by the user</td>
</tr>
<tr>
<td>Auditor</td>
<td>- compliance reports based on compliance scan data</td>
</tr>
<tr>
<td></td>
<td>launched by all users in the subscription</td>
</tr>
</tbody>
</table>

Managers and Unit Managers can share reports and scan templates. To share a completed report, go to the Reports tab, select a report and then select Info from the Quick Actions menu. Go to the User Access section and click the Add button. To share all reports generated from a scan template, go to the Templates tab and edit the template. Go to the User Access section and add users to the access list.

Good to Know:

- Users may be granted access to reports containing IPs which the users do not have privileges to.
- Users may be granted access to reports generated in a business unit outside of the user’s own business unit.

Secure PDF Distribution

Using secure PDF distribution Managers and Unit Managers have a one step solution to generate PDF encrypted reports and securely distribute them to users outside of the application via email. When a PDF encrypted report is generated, it is saved in Report Share and users on the distribution list receive an email with a secure link to the PDF report. To view a PDF encrypted report, each user is prompted to enter the report password.

Secure PDF Distribution is an optional feature that can be enabled for the subscription by a Manager on the Reports Share Setup page (go to Reports > Setup > Report Share).
Once Report Share is enabled for the subscription, Managers and Unit Managers will see the Add Secure Distribution link when launching reports.

Click the link Add Secure Distribution to enter the encryption password and select the user distribution list.

Encryption — Enter a password and then confirm the password in the fields provided. If your subscription has enabled user-defined passwords, then the security settings for user-defined passwords on the Setup > Security page are enforced.

Important: The user who launches the report must communicate the password to all users who will access the report, including the email recipients in the distribution groups and Qualys users who will access the report from the report history list.
Enterprise Reporting

Chapter 4 — Enterprise Management and Reporting

Distribution List — Select one or more distribution groups, identifying the target email recipients. A recipient may be any user, with or without an account for the subscription. Click the Add Group link to select a distribution group for the current report you are launching. The Add Distribution Group window appears, displaying your saved distribution groups.

![Add Distribution Group](image)

Select one or more groups from the Distribution Groups list and then click “Add to list”. The groups will appear under Recipient Groups in the new report window. (If you need to add a group first, click the New button (on the right).)

**Automatic Report Distribution**

*Note: Acrobat Version 7 or greater is required to view secure PDF reports.*

When a secure PDF report is completed in Report Share, the service automatically makes the report available to users. The report is distributed automatically via email and the report history list. From the report history list Managers and Unit Managers may view secured PDF reports from the report history list, like other reports, based on their user role access privileges.

A secured PDF report is identified in the report history list with the Secured PDF format (PDF 🗝️) in the Format column. Users are prompted to enter a report password each time they select a PDF encrypted report to view or download.
Patch Reports

The Qualys Patch Report 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 was used to scan the hosts selected for the report. 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.

Qualys provides a pre-configured patch template “Qualys Patch Report”. Using this template you can identify the patches you need to apply right away.

Your patch report can be saved in these formats: PDF, CSV and Online Report. The Online Report format provides a feature-rich user interface including numerous ways to navigate through your report content. HTML content is displayed in your browser using Ext, a client-side Java framework.

A sample Online Patch Report is shown below. This report was generated using the pre-configured template “Qualys Patch Report”. In this report patches are grouped by host.

This patch report summary shows: 196 total patches need to be applied to fix the vulnerabilities on the target hosts, 14 hosts require patches to be applied in order to fix the vulnerabilities, and 318 vulnerabilities in the user's account are addressed in the report.
(1) To view the target asset groups and/or IPs: Click “View Report Targets”.

(2) To sort the HOSTS list by a host attribute: Click a host attribute (column title) in the HOSTS list. The arrow next to the column title indicates the sort order: ascending (Up arrow) or descending (Down arrow). Click the column title again to toggle the sort order.

(3) To view the missing patches for a particular host: Move your mouse pointer over a host in the HOSTS list and click the host row. The missing patches for the host appear in the PATCHES list (on the right). In the PATCHES header you’ll see the number of missing patches for the selected host. In this case, there are 13 missing patches for the host 10.10.24.47.

(4) To page through the HOSTS list: Use the arrow keys (under the list area) to page forward and backward through the list. Enter a number in the field provided to jump to a certain page number.

(5) To apply a filter to the HOSTS list: Enter a string in the Filter field (under the list area). The HOSTS list will be updated to display only hosts with attributes matching the string you enter. For example, if you enter “10.10.25.6” the report will display only IP addresses including that string.

(6) To read the vendor’s security bulletin related to a patch: Click the vendor ID link for a patch in the PATCHES list.

(7) To view the vulnerabilities that will be fixed after applying a patch on a host: Refer to the Vulns column for a patch in the PATCHES list. Click the number of vulnerabilities link to view a list of vulnerabilities which the patch will fix (this link is available if “QIDs that will be fixed by each patch” is selected in the patch template used).

**Consultant Reports**

*Consultant reports apply only to Consultant subscriptions. Consultants have the ability to create consultant templates and generate consultant reports specific to their customers’ needs. These formats are supported: PDF, HTML, MHT, XML, CSV and Microsoft DOCX.

Using the consultant template you can define the report layout and filtering options similar to scan report templates. The consultant template includes configurations for cover page, customer information and report summary.*
Report Templates

Report templates give you great flexibility in creating custom report templates. There are several report templates available to choose from.

You might want to customize reports using a report template. You can import a template from our library and customize it. Also you can create new templates. Just go to Reports > Templates and then select New > template type (for example, New > Scan Template), configure the options and click Save.

Global report templates can be created to publish templates to multiple users. Just edit the report template and select the option called “Make this is a globally available template”.

<table>
<thead>
<tr>
<th>Global — Subscription</th>
<th>Global templates that are available to all users in the subscription. Only Managers can create these templates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global — Business Unit</td>
<td>Global templates that are available to all users in the same business unit. Only Unit Managers can create these templates for their own business unit.</td>
</tr>
</tbody>
</table>

Download Data Lists as CSV, XML, HTML, MHT

The data list download option is available for most data lists throughout the application, giving users more ways to report on security and compliance within the IT infrastructure. Just go to a data list, select Download from the New menu and select a format (CSV, XML, HTML, or MHT). The downloaded content will mirror the data list view as it appears in your browser.

The data list is downloaded to a file on the local file system in this format:

`DL_<datalist_name>_<user_login>_<date>_<format_extension>`

For example:

`DL_scan_history_acme_dd_20071030.csv`
Remediation Workflow

Qualys provides fully secure audit trails that track vulnerability status for all detected vulnerabilities. As follow up audits occur, vulnerability status levels — new, active, fixed, and re-opened — are updated automatically and identified in trend reports, giving users access to the most up-to-date security status. Using Remediation Workflow, the service automatically updates vulnerability status in remediation tickets, triggering new tickets, ticket updates and closure in cases where vulnerabilities are verified as fixed.

Remediation Workflow is an optional feature that is not enabled in new Qualys subscriptions. When this feature is enabled, new tickets are created automatically, based on newly available scan results and the Manager-defined policy consisting of policy rules. The remediation policy specifies conditions for ticket creation and user assignment.

Figure 4-1. Automatic Ticket Creation

Users take action on tickets by fixing vulnerabilities, adding comments, and reassigning to other users as appropriate. Role-based access controls determine which users have the ability to view which tickets, ensuring that only the appropriate users can access tickets and take action on them.

As new vulnerability assessment data becomes available, Qualys automatically updates the ticket information, including ticket history and current vulnerability data.

Before you begin, be sure to complete the rollout steps discussed in Chapters 2 and 3.
BEST PRACTICES

Set achievable remediation goals. Defining user roles and responsibilities as well as prioritizing assets will assist with developing achievable goals with remediation. Our customers report that they were surprised at the large number of tickets produced from their first security audits with the remediation workflow feature enabled.

Develop a phased approach. When getting started with a rollout project, many customers report that they are surprised at the large number of remediation tickets initially created.

Regularly run and publish remediation reports. Your remediation reports show remediation status and progress over time. We recommend that you run remediation reports at least monthly. It’s a good idea to run remediation reports with the same frequency that you run vulnerability status and trend reports.

ROLLOUT STEPS

Enable Remediation Workflow. To do this, you add a remediation policy with one or more policy rules. Optionally, set remediation policy options to grant privileges to alter ticket state. Also, you can enable Unit Managers to define a remediation policy for their business unit.

Take action on tickets. Typically multiple users are involved with taking action on tickets. Their activities involve fixing vulnerabilities, and optionally editing tickets by adding comments, reassigning to different users, or marking as ignored.

Run remediation reports. There are remediation reports for management and technical analysis that you can run at any time. See “Remediation Reporting” in Chapter 5.

Enable Remediation Workflow

To enable Remediation Workflow and the automatic creation of remediation tickets, you must create a remediation policy that consists of one or more policy rules. Also, there are remediation policy options that you may configure. New rules and options are applied to subsequent scans automatically.

Set Remediation Policies

Remediation policies identify rules used to create and update tickets based on most recent scan results. Managers and Unit Managers may view, create and edit remediation policies.

To view remediation policies, go to Remediation > Policies. Rules are listed in priority order, where the first rule is applied to the new scan results first. To add a new rule select New > Rule.
For each rule, define conditions for automatic ticket creation. You may select target hosts or vulnerabilities:

Target Hosts - Enter a combination of asset groups, IPs and/or IP ranges.

Vulnerabilities - Add vulnerability search lists. Up to 10 search lists may be added.

You choose whether tickets will be assigned to a specific user or ignored. Tickets may be assigned to the user running the scan. When assigned to a user, a deadline is set so tickets are assigned a due date. The deadline is set to 7 days by default (so tickets will be assigned due date 7 days in the future).

The policy rules are applied to all scans run by all users. A business unit policy may be defined by Unit Managers who are granted this permission (by Managers). When defined, the business unit policy is applied first and then the subscription policy.

Set Remediation Options

To set remediation options, go to Remediation > Setup > Remediation. Transition options can be set by Managers. The timeframe option allows any user to configure the timeframe used to display tickets in the tickets list; tickets modified within the timeframe will be displayed.
View Tickets List

Tickets are created automatically by the service after a remediation policy has been defined. To view the tickets in your account, select Remediation from the top menu. This is the starting point for viewing tickets and taking actions on them.

Click Search on the top menu bar to view the ticket search options. You can search by attributes of tickets, hosts and vulnerabilities. For example, you can search by ticket number, due date, asset IP address, ticket state, vulnerability title and severity level. You can also search for a user’s associated tickets, which are tickets not owned by the user but based on assets in the user’s account.

View Ticket Information

Each remediation ticket tracks a vulnerability detected on a particular host. The ticket lifecycle starts when a vulnerability is detected during a scan and it matches a rule in the remediation policy, a new ticket is created and automatically assigned to a user. Over time the service automatically tracks the vulnerability/IP pair in the remediation ticket where the remediation status is maintained based on the most recent scan results.

Every remediation ticket has a unique ticket number with vulnerability information and ticket history, including a history of ticket actions and links to saved scan results for each related scan.

To view ticket information, go to Remediation > Tickets. Click next to a ticket you’re interested in and then select Info from the Quick Actions menu. By selecting Edit from the Quick Actions menu you can mark the ticket resolved and assign to another user.
Chapter 4 — Enterprise Management and Reporting  
Remediation Workflow

## About the Closed Loop Ticketing System

Qualys includes a closed loop ticketing system that ensures that remediation tickets are managed through specific ticket states. The ticket states are: Open, Resolved, and Closed. New tickets are opened automatically and only by the service. Tickets are resolved and closed as described below.

### Closing Open Tickets

It is the ticket owner’s responsibility to fix the vulnerabilities associated with their tickets or mark their tickets as “Ignored”. Tickets may be closed by one of the methods below.

**Method a.** Two steps.  
- a-1) After fixing vulnerabilities, users edit tickets and mark them Resolved.  
- a-2) During the next scan, the service verifies that the vulnerabilities are fixed and closes the tickets.

**Method b.** One step.  
A user fixes vulnerabilities. During the next scan, the service verifies that the vulnerabilities are fixed and closes the tickets.
**Method c.** One step. Users ignore tickets they don’t plan to fix. Ignored tickets remain in the closed state until a user chooses to reopen them by editing the tickets.

**Reopening Closed Tickets**

Resolved and closed tickets may be reopened by one of the methods below.

**Method a.** One step. The service automatically reopens tickets previously marked as Resolved when the vulnerabilities related to the Resolved tickets are detected in subsequent scans.

**Method b.** One step. The service automatically reopens tickets previously closed by the service when the vulnerabilities are detected again in subsequent scans. (The service closes tickets automatically when vulnerabilities related to tickets are verified as fixed.)

**Method c.** One step. Users have the option to reopen previously ignored tickets.
CUSTOMIZING LEVEL OF RISK

Using Qualys you can customize the level of risk within your own subscription. These settings affect all users in the subscription.

BEST PRACTICES

Understand your security policy and review risk levels. Applying your existing security policy to risk level settings will ensure that security risk and compliance information presented and reported on is most meaningful and accurate to your organization.

Regularly run reports. Our customers are most successful and see the most remediation progress by running reports on a regular basis. We recommend that you run status and trend reports at least monthly, and status reports in between as needed. Be sure to publish reports to all teams and individuals with security management responsibility.

ROLLOUT STEPS

Customize vulnerabilities Several pre-defined report templates are available to all users at any time. Run these reports right away to view your vulnerability status and your most important vulnerability information.

Review business risk setup and edit as appropriate. Qualys provides a default business risk setup that is a good starting point for business risk calculations. It’s recommended that you review the setup settings and adjust to match your security policy and reporting practices.

Enable CVSS scoring. Qualys supports CVSS scoring using this industry standard scoring technique that allows organizations to take into consideration their own security metrics. For a new subscription, CVSS scoring is not enabled by default. You can enable CVSS scoring so that CVSS scores appear with vulnerability details.

Ignore vulnerabilities Ignoring vulnerabilities on a host/port combination provides a method for filtering out vulnerability instances from application views and reports.

Customizing Vulnerabilities

Users with the Manager role can edit vulnerabilities in the KnowledgeBase to affect how vulnerabilities are displayed in user interface views and in reports. All customizations are global, affecting all users in the subscription. These attributes may be edited: the severity level, text descriptions for threat, impact and solution, and the disabled vulnerability flag. See “Vulnerability KnowledgeBase” in Chapter 3.
Business Risk in Scan Reports

Qualys scan reports illustrate the security and business risk status based on the value of the assets to business operation. Both the criticality of the hosts, as defined by target asset groups, and the severity of the vulnerabilities detected are taken into consideration when calculating business risk.

You’ll see the overall Business Risk rating in scan reports based on current vulnerability status. This appears under Summary of Vulnerabilities, next to the average security risk.

Tell me about the Business Risk rating

Business risk is expressed as a value from 0 to 100. Generally the higher the business risk value the higher the potential for business loss if security is compromised through the exploitation of the detected vulnerabilities. For example, a severity level 5 vulnerability on a host in an asset group with a “Critical” business impact represents a much greater risk than the same vulnerability on a host in an asset group with a “Low” business impact.
How is business risk calculated?

We reference the business risk table for your subscription to evaluate your current vulnerabilities and their severity levels. All users can view the business risk lookup table to reference its settings - just go to Reports > Setup > Business Risk (see the sample below).

First we’ll calculate security risk for each asset group based on the vulnerabilities detected and their associated severity levels (see Security Risk in Scan Reports below). Then we’ll look up the business impact level for the asset group based on its security risk. For example, in the case where security risk is 4 and business impact is Medium, the business risk is 16.

Security Risk in Scan Reports

The Summary of Vulnerabilities section of your scan report shows the average security risk value for all hosts in the report (hosts matching filters). Security risk is first calculated for each host in the report. Then the average of the security risk values for all hosts is calculated and displayed in the summary. Important: The filters set in the scan report template will affect the number of hosts and the types of vulnerabilities that appear in your report.

This description of security risk applies to scan reports generated from scan report templates.
Average Security Risk in Summary

The Summary of Vulnerabilities section of the scan report shows the average security risk for all hosts in the report.

These factors are used when calculating the average security risk:

- security risk for each host (the highest severity level detected or the average severity level detected, see below)
- number of hosts matching filters (hosts in the report matching the filters set in the scan report template)

Note that the average security risk for the report displays the average for all hosts in the report, and is not affected by the sorting method applied to the Detailed Results section. See “Security Risk in Detailed Results” below.

The following formula is used for calculating the average security risk.

\[
\text{Average Security Risk} = \frac{\text{Sum of Security Risk Values for all hosts in the report}}{\text{Number of hosts matching filters}}
\]

Security Risk for each Host

We’ll tell you how security risk is calculated for each host in your reports. The security risk calculation includes vulnerabilities and potential vulnerabilities. Information gathered are not included in the calculation.

In a Scan Based report, security risk is equal to the highest severity level detected across all vulnerabilities and potential vulnerabilities on the host. For example, if the highest severity level detected on the host is severity level 4 (whether confirmed or potential), then the security risk for the host is 4.

In a Host Based report, security risk is either 1) the average severity level detected (default), or 2) the highest severity level detected. The calculation method used depends on the security risk configuration enabled for the subscription. You can choose to include or not include hosts with no vulnerabilities. Managers define configuration settings on the Security Risk Setup page (Reports > Setup > Security Risk).

View the sample reports below showing the security risk value. (Keep in mind, to see the security risk value, you must select the “Text Summary” option under Detailed Results in the scan report template.) For these reports, detailed results are sorted by host, the “Text Summary” option is selected in the scan report template, and active vulnerabilities and potential vulnerabilities are included.
Example Security Risk is set to “Average severity level detected”:

![Security Risk Table]

### By Severity

<table>
<thead>
<tr>
<th>Severity</th>
<th>Confirmed</th>
<th>Potential</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

### By Rapid Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Confirmed</th>
<th>Potential</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>RPC</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

### Vulnerabilities (4)

- 2 Hidden RPC Devices
- 2 TCP Sequence Number Fingerprinting (Denial of Service)
- 2 UDP Constant IP Identification Field Fingerprinting Vulnerability
- 1 ICMP Timestamp Request

### Potential Vulnerabilities (1)

- 5 Stack Format String Vulnerability
Example Security Risk is set to "Highest severity level detected":

If you sort detailed results by host, then the service shows the security risk for each host. All vulnerabilities and potential vulnerabilities detected on each host are included in the security risk calculation. If you sort detailed results by some other method, like operating system, the service shows the security risk for the hosts with the same operating system. All vulnerabilities and potential vulnerabilities detected on hosts with each operating system are included in the calculation.
CVSS Scoring

CVSS stands for Common Vulnerability Scoring System (CVSS), the emerging open standard for vulnerability scoring (using a scale of 1 to 10). CVSS was commissioned by the National Infrastructure Advisory Counsel (NAIC) and is currently maintained by FIRST (www.first.org/cvss). CVSS is widely supported by security organizations and vendors including: CERT, MITRE, Cisco, Symantec, Microsoft and Qualys.

Qualys supports CVSS Version 2 and CVSS Version 3.

CVSS scores are displayed in many places for vulnerabilities and potential vulnerabilities throughout the application when the CVSS Scoring feature is enabled in your account. When enabled, CVSS Base and Temporal scores are displayed in vulnerability scan reports and compliance reports that include vulnerability details, as well as in online views of hosts, tickets and vulnerabilities. Also, final CVSS scores are calculated and displayed in automatic scan reports.

Enable CVSS Scoring

CVSS Scoring is a subscription level feature that can be enabled by Managers only. To enable CVSS scoring in the subscription, go to Reports > Setup > CVSS and select “Enable CVSS Scoring”.

![CVSS Setup](image)
CVSS Scoring Elements

Several factors affect the CVSS score calculated for a vulnerability: CVSS Base score, Temporal score and Environmental metrics.

**Figure 4-2. Scan Status Report (Auto) with CVSS Scores**

**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. Metrics apply to all hosts in the group.

- **Collateral Damage Potential.** This environmental metric represents the possibility for loss in physical equipment and property damage.

- **Target Distribution.** This environmental metric represents the relative size of the field of the target systems susceptible to the vulnerability.

The following Security Requirements metrics enable users to customize the CVSS score.

- **Confidentiality Requirement.** This environmental metric represents the impact that loss of confidentiality has on the organization or individuals associated with the organization.

- **Integrity Requirement.** This environmental metric represents the impact that loss of integrity has on the organization or individuals associated with the organization.

- **Availability Requirement.** This environmental metric represents the impact that loss of availability has on the organization or individuals associated with the organization.
CVSS Base Scores Supplied from NIST

Qualys has standardized on NIST scoring for CVSS Version 2.0 Base scores. CVSS Base scores are displayed in many locations throughout Qualys.

For some vulnerabilities, a Qualys generated score may be displayed. When the service looks up the latest NIST score for a particular vulnerability, it’s possible that NIST lists the CVSS Base score as 0 or does not provide a score. In this case, the service then determines whether the severity of the vulnerability warrants a higher CVSS Base score. If so, a Qualys generated score is displayed with the footnote [1].

View Final CVSS Scores

The sample automatic scan report below shows CVSS scores. The final CVSS score appears in the detailed host results in the vulnerability summary line. In this report the vulnerability with QID 90278 has a final CVSS score of 4.1.
Ignoring Vulnerabilities

Vulnerabilities and Potential Vulnerabilities detected on a host/port combination may be marked as ignored for the subscription. All users with scanning privileges can ignore vulnerability instances. Ignoring vulnerabilities provides a method for filtering out vulnerability instances from application views and reports.

You can ignore vulnerability instances while viewing vulnerabilities in scan status reports (automatic) and asset search results. Select a vulnerability in the report, place your cursor over the red cross (x) next to a vulnerability instance and select Ignore vulnerability from the drop-down menu.

The Ignored Vulnerabilities Report lists ignored vulnerabilities defined for your account. See “Patch Reports.”
COMPLIANCE

Automated trend reporting gives users the ability to compare security audit results over a period of time, putting a spotlight on vulnerability and compliance trends and overall security posture. Trend reporting on a regular basis is a security management best practice. Producing trend reports allows you to document your progress and publicize your success within the organization. Remediation reporting on vulnerability scan data provides detailed host information including the current status of all vulnerabilities detected on each host.

Qualys allows you to comply with information security regulations and other industry standards. It’s recommended that you learn about these security regulations and standards and incorporate best practices towards achieving compliance.

To track progress and achieve policy compliance using Qualys most effectively in the quickest time, the following activities are involved:

- **Achieving Compliance**
- **Vulnerability Reporting and Trend Analysis**
- **Remediation Reporting**
- **Payment Card Industry (PCI) Compliance**
- **Policy Compliance (PC)**
- **Policy Compliance — Current Regulations and Mandates**
Chapter 5 — Compliance
Achieving Compliance

**ACHIEVING COMPLIANCE**

Organizations are required by law to comply with a growing number of government and industry-specific regulations designed to safeguard electronic data from information security breaches. Companies that do not fully comply and stay up-to-date with information security regulations face serious consequences including heavy fines and legal action. Using Qualys, you can take advantage of Qualys’s secure and permanent reporting audit trail to document and demonstrate compliance.

**BEST PRACTICES**

**Perform vulnerability management on a regular basis.** Perform security auditing, trend reporting and remediation following the guidelines provided in this guide.

**Connect vulnerability management practices with policy compliance objectives.**

**Stay informed and up-to-date on regulations and their requirements.**

**ROLLOUT STEPS**

**Run trend reports and publish to auditors.** Refer to “Remediation Reporting” to run appropriate reports and publish them to your auditors.

**Run compliance reports.** The service provides a wide variety of template-based reports for achieving compliance with a wide variety of security standards and regulations, including Payment Card Industry (PCI) Data Security Standard (DSS), HIPAA, GLBA, SB 1386, Sarbanes-Oxley, FISMA, the CobIT information technology standard plus others. Interactive compliance reports are available when the policy compliance module is enabled.

**Use Qualys Payment Card Industry (PCI) Module.** The Payment Card Industry (PCI) Compliance feature provides a workflow for achieving compliance with PCI DSS requirements for quarterly PCI external scans and quarterly PCI internal scans.

**Use Qualys Policy Compliance (PC) Module.** The policy compliance module provides customers with a way to audit and document compliance to internal and external auditors to meet corporate security policies, laws and regulations.

**Understand current regulations.** Refer to “Policy Compliance — Current Regulations and Mandates” for information about the current regulations for which many companies today must demonstrate compliance.
VULNERABILITY REPORTING AND TREND ANALYSIS

Qualys provides very flexible, comprehensive reporting capabilities with functionality for filtering, grouping, and synthesizing security assessment data in your account. This allows customers to store security assessment data for an indefinite amount of time, providing a way for organizations to establish a certain baseline and continue to reference it in order to measure progress.

Pre-defined report templates are provided so that you can easily run reports right away. These include the Executive Report, the High Severity Report and the Technical Report. Additional template-based reports are provided when the policy compliance module is enabled in the user account. Custom trend report templates may be setup as needed for reports based on vulnerability assessment data.

BEST PRACTICES

Regularly run trend reports. Our customers report the best remediation progress as the result of producing trend reports on a regular basis.

Check first trend reports. Check your first trend reports to be sure that the trending information is both meaningful and useful for your organization. It’s possible that you may want to add asset groups (for scanning and/or reporting), customize scan options set in option profiles, and customize the business risk calculation.

Publish reports with trending. Publish your trend reports to all parties involved throughout your organization.

Perform business risk analysis first. Initial business risk settings are provided so trend reports include a business risk value automatically. It’s recommended, however, that you first perform business impact analysis on assets in your organization, and then apply those findings to your asset groups and the business risk lookup table. This way the business risk calculation and resulting business risk values match your organization’s security policy.

ROLLOUT STEPS

Run reports with trending. You can run pre-defined reports and custom scan reports with user-defined settings. The pre-defined templates with trending information include the Executive Report (scan template) and remediation reports. Several pre-defined graphs can be included in scan reports. Trend graphs may be included in a scan report when the template has the scan results selection setting “Status with Trend”.

Run custom scan templates with trending. When adding a custom scan report template, select the Scan Results Selection setting “Status with Trend”. Refer to “Patch Reports” in Chapter 4 for information.
Chapter 5 — Compliance
Vulnerability Reporting and Trend Analysis

Adjust business risk setup. Adjust business risk setup settings that affect how the business risk rating is calculated for scan status reports (automatic) based on the business risk analysis you’ve performed. See “Business Risk in Scan Reports” in Chapter 4 for information.

Use Asset Search. Use the Asset Search feature to search and view current host information, and take remediation actions.

Executive Report with Trending

The Executive Report includes scan status with trend information. This report is appropriate for management, as it compares vulnerability assessment results over a period of time, giving security information in summary format. Initially the time period in this report is set to eight weeks. You may change the time period by editing the report template to select some number of days, weeks, months, or the previous two detections.

The vulnerability status is provided in the “by Status” table. This table identifies the number of new, active and re-opened vulnerabilities over the report time period. A re-opened vulnerability is a vulnerability that you previously fixed. You have the option to edit the report template to include potential vulnerabilities.

Summary of Vulnerabilities

<table>
<thead>
<tr>
<th>Status</th>
<th>Confirmed</th>
<th>Potential</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>1838</td>
<td>-</td>
<td>1838</td>
</tr>
<tr>
<td>Active</td>
<td>2930</td>
<td>-</td>
<td>2930</td>
</tr>
<tr>
<td>Re-Opened</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>4829</td>
<td>-</td>
<td>4829</td>
</tr>
</tbody>
</table>

The “Top 10 Vulnerability Categories” table illustrates the top 10 areas that need the most attention, and how much the exposure has changed over time.

<table>
<thead>
<tr>
<th>Category</th>
<th>Confirmed (Trend)</th>
<th>Potential (Trend)</th>
<th>Information Gathered</th>
<th>Total (Trend)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>857 (+433)</td>
<td>-</td>
<td>-</td>
<td>857 (+433)</td>
</tr>
<tr>
<td>Web server</td>
<td>719 (+710)</td>
<td>-</td>
<td>-</td>
<td>719 (+710)</td>
</tr>
<tr>
<td>CGI</td>
<td>568 (+659)</td>
<td>-</td>
<td>-</td>
<td>568 (+659)</td>
</tr>
<tr>
<td>General remote services</td>
<td>658 (+639)</td>
<td>-</td>
<td>-</td>
<td>658 (+639)</td>
</tr>
<tr>
<td>TOPO</td>
<td>326 (+307)</td>
<td>-</td>
<td>-</td>
<td>326 (+307)</td>
</tr>
<tr>
<td>Total</td>
<td>3229 (+3136)</td>
<td>-</td>
<td>-</td>
<td>3229 (+3136)</td>
</tr>
</tbody>
</table>

The “Vulnerabilities by Severity over Time” graph visually identifies the total number of confirmed vulnerabilities and potential vulnerabilities at each severity level.
You can modify the Executive Report template to include vulnerability details and additional graphs, and to adjust the time period that the report covers. See “Enterprise Reporting” in Chapter 4 for more information.

**Asset Search**

The Asset Search feature allows you to search and view current host information in your account. The Asset Search retrieves information on hosts that have already been scanned.

Only scanned hosts are searched and returned in the asset search results. The service searches the most recent vulnerability scan data by default. When the Compliance application is available in the user account, the service searches the most recent compliance scan data as well.

To access Asset Search, go to Assets > Asset Search. Using the Asset Search form, identify the target hosts to search for. You may specify one or more of these targets: asset groups, IP addresses/ranges, a DNS hostname, or a NetBIOS hostname. Note that hosts matching any target are returned.
Chapter 5 — Compliance
Vulnerability Reporting and Trend Analysis

Optionally, select search attributes to refine your search. For example, you may specify a host tracking method, an operating system name, open ports, running services, a vulnerability ID (QID), and last scan date. After making entries, click Search.

The Asset Search Report includes a Report Summary section at the top followed by the Results section with hosts that match your search criteria.
Each entry in the report identifies a target host, including its IP address, the DNS and NetBIOS hostname (as applicable and when available), its operating system, the asset groups to which the host belongs, the host tracking method and the last scan date. Additional information is returned when certain attributes are entered such as Open Ports, Running Services and QID.

When viewing the Asset Search Report you can take workflow actions by selecting hosts and a workflow action on the Actions menu. See “Taking Workflow Actions” (page 51) for more information. You can also view current host information by clicking the host IP address. See “Current Host Information” (page 81).
The Risk Analysis is used to analyze selected hosts for a risk due to a specific threat (a vulnerability or potential vulnerability). The service uses existing vulnerability scan data (results returned from previous scans) to determine if hosts are at risk. By running Risk Analysis you can address high risk vulnerabilities on critical assets, without waiting for the next scan opportunity.

To run Risk Analysis, go to Reports > Risk Analysis.

In the Risk Analysis form, identify the target hosts to analyze — asset groups and/or individual IPs — and select a vulnerability or potential vulnerability that you want to test. Then click Run to start the analysis.

The Risk Analysis Report includes a Report Summary section at the top followed by the Hosts Possibly Exposed section (under the Qualys ID and title). Hosts possibly exposed are listed by business impact, allowing you to readily assess the impact to your business and fix the most vulnerable hosts first.

As with other reports, you can print and download the report in multiple formats.
From the Risk Analysis Report you can take workflow actions by selecting hosts and an action on the Actions menu. See “Taking Workflow Actions” (page 51). You can view current host information by clicking the host IP address. See “Current Host Information” (page 81).

Each entry in the report identifies a target host, including its IP address, NetBIOS hostname, the asset groups to which the host belongs, and the business impact assigned to the asset group. Check marks to the right indicate the possible exposure to the vulnerability.

<table>
<thead>
<tr>
<th>QID</th>
<th>Check indicates the vulnerability (QID) has been detected on the host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Check indicates the host runs the OS related to the vulnerability.</td>
</tr>
<tr>
<td>Port</td>
<td>Check indicates the host has an open TCP or UDP port related to the vulnerability.</td>
</tr>
<tr>
<td>Service</td>
<td>Check indicates the host runs one or more services related to the vulnerability.</td>
</tr>
<tr>
<td>Results</td>
<td>Check indicates results from previous scans on this host include information related to this vulnerability.</td>
</tr>
</tbody>
</table>
Vulnerability Compliance Reports

Template based compliance reports are derived from vulnerability scan data.

To run a template based compliance report, go to Reports. From the Reports tab select New > Template based Compliance Report.

Run the Qualys Top 20 Report to see whether your network is vulnerable to the Qualys Top 20 vulnerabilities, a dynamic list of the 10 most prevalent external and internal security vulnerabilities. This list is dynamically updated by Qualys.

Run the SANS Top 20 Report to discover whether you are exposed to SANS Top 20 vulnerabilities identified by The SANS Institute as the most critical Internet security vulnerabilities. These vulnerabilities are sorted into categories, each of which may include several vulnerability checks.

Run the Payment Card Industry (PCI) Reports to identify compliance with the Payment Card Industry (PCI) Data Security Standard. The Technical Report is used to identify and prioritize remediation; it includes verified solutions for detected vulnerabilities. The PCI Executive Report is used to submit to acquiring banks as proof of compliance.
**Remediation Reporting**

Centralized reporting provides users access to current host remediation information and status based on the latest vulnerability scans. Access to current host-based remediation data is crucial to successful vulnerability management and policy compliance. These features are provided.

Remediation Reports — When Remediation Workflow is enabled, remediation reports provide security managers with a current viewpoint on remediation progress, vulnerability status and ticket trends. Qualys provides four different remediation reports appropriate for management and in-depth technical analysis with trending.

Daily Trouble Ticket Updates — When Remediation Workflow is enabled, users may choose to receive the Daily Trouble Ticket Updates email notification, reporting remediation ticket status and trends on a daily basis. This notification is a user account option that can be enabled by editing the user account. Users may enable this notification in their own accounts.
Chapter 5 — Compliance
Remediation Reporting

**BEST PRACTICES**

**Review host information and status.** Review current host information and remediation status based on the latest available scan results. To do this, use Qualys reporting features described earlier in “Remediation Reporting.” Also use the features Asset Search and Risk Analysis.

**Regularly run remediation reports.** We recommend that you run remediation reports at least monthly, with the same frequency that you run trend scan reports.

**Check first remediation reports.** Check your first remediation reports to be sure that the trending information is both meaningful and useful for your organization. It’s possible that you may want to add asset groups and make other customizations such as scan option profiles, the business risk calculation, and remediation policy.

**Publish remediation reports.** Publish your trend reports to all parties involved in the organization.

**ROLLOUT STEPS**

**Run remediation reports.** Qualys provides four pre-defined remediation reports that can be run at any time when Remediation Workflow is enabled.

**Review Daily Trouble Ticket Updates.** Select this email notification in your account.

**Run Risk Analysis.** Use the Risk Analysis feature to find out whether hosts that are likely exposed to security vulnerabilities. For hosts likely to be exposed, view current host information and take remediation actions.

**Remediation Reports**

There are four pre-defined remediation reports in all user accounts. These reports may be run when Remediation Workflow is enabled.

**Executive Report.** This report includes a ticket status table and graphical elements illustrating the total number of open and closed tickets at each severity level, ticket state changes for the past 12 weeks, and an open ticket trend for the past 12 weeks.

**Tickets per Asset Group.** This report includes a ticket status table and tickets per asset group data. All asset groups in the user account are listed. For each asset group the report shows the total number of tickets, the number of tickets in each ticket state, the average number of days for resolution on tickets, and the total number of overdue tickets.

**Tickets per User.** This report includes a ticket status table and tickets per user data. All users in the subscription are listed. For each user the report shows the total number tickets assigned, the number of tickets in each ticket state, the average number of days for resolution on tickets, and the total number of overdue tickets.
**Tickets per Vulnerability.** This report includes a ticket status table and tickets per vulnerability data. For each vulnerability the report shows the total number of tickets related to the vulnerability, the number of tickets at each ticket state, the average number of days for resolution on tickets, and the total number of overdue tickets.

To run and view a remediation report, go to Reports > Templates. From the report templates list, locate a remediation report with the template type in the Type column. Select a report row, click and then select Run from the Quick Actions menu.

All remediation reports display a Ticket Status table with current ticket status.

<table>
<thead>
<tr>
<th>Severity</th>
<th># of Tickets</th>
<th>Open</th>
<th>Resolved</th>
<th>Closed</th>
<th>Avg. Resolution</th>
<th>Overdue</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>34</td>
<td>9</td>
<td>7</td>
<td>22</td>
<td>15 days</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>13</td>
<td>0 days</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>55</td>
<td>17</td>
<td>0</td>
<td>38</td>
<td>19 days</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>6</td>
<td>0</td>
<td>8</td>
<td>5 days</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>131</strong></td>
<td><strong>35</strong></td>
<td><strong>15</strong></td>
<td><strong>81</strong></td>
<td><strong>5.2</strong></td>
<td><strong>12</strong></td>
</tr>
</tbody>
</table>

The Executive Remediation Report includes pie charts showing the total number of open tickets and total number of closed tickets by severity level. In the sample below, 40% of the total number of open tickets represent severity level 5 vulnerabilities.
PAYMENT CARD INDUSTRY (PCI) 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 Payment Card Industry 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: Perform 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: Remediation Workflow

Run the PCI Technical Report template for a completed PCI external scan to view the vulnerabilities detected by the scan and your compliance status. Go to Reports > Templates, hover over the PCI Technical Report template, and then select Run from the Quick Actions menu.

Review this report including the compliance status and risk rankings for all hosts. All hosts must have the compliance status PASS to pass the PCI DSS requirements for an external scan. If a host has the compliance status FAIL then one or more vulnerabilities must be fixed. After fixing them perform another PCI external scan (a verification scan), wait until the scan status is "Finished" and the scan processing status is "Finished", and then run another PCI scan report to review the risk rankings. Continue the remediation process until all High ranking vulnerabilities are fixed and no High ranking vulnerabilities appear in your PCI scan report.

Step 3: Share Scan with PCI

To share a PCI scan with your PCI Merchant account:

1. Go to Scans > Setup > PCI Account Links. Add another account link if you wish to share a scan with a PCI account that is not listed. A Manager can create a new PCI Merchant subscription and link to it. (Note: A Manager must be the first user to link to any PCI Merchant subscription.)

2. Now go back to the Scans tab. Click anywhere in the row for a PCI scan and click the “Share with PCI” link in the preview pane.

3. Select the PCI Merchant account that you want to share the scan with. All PCI merchant accounts that you have linked to are listed.
4 Click the “Share” button. All IPs in the scan target will be shared to Qualys PCI.
5 Complete the onscreen steps to log into the Qualys PCI app.

**Step 4: Create Your Certification Report**

Using your PCI account, you can create a PCI network report and take required actions for PCI certification:

- Review the scan results (go to Network > Scan Results).
- View the current vulnerabilities (go to Network > Vulnerabilities). If there are PCI vulnerabilities detected for the scan you must perform remediation and rescan to verify that all PCI vulnerabilities are fixed.
- View the compliance status (go to Compliance > Compliance Status) and generate PCI network reports.
- Complete report approval and submit 1) submit the report to your ASV for approval, and 2) once approved, submit the report to your acquiring banks.

**Quarterly PCI Internal Scans Workflow**

Per PCI DSS v3.0 requirement 11.2.1 and 11.2.3, the PCI Council 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.
POLICY COMPLIANCE (PC)

The Qualys Policy Compliance (PC) module provides these features:

*Compliance Scanning* extends the Qualys global scanning capabilities to audit hosts to measure compliance with corporate security policies, laws and regulations.

*Technical Controls Library* includes controls based on CIS and NIST standards and mapped to several frameworks and regulations. Like vulnerability signatures, the controls software is updated automatically on a regular basis by the service.

*Policy Compliance Reporting* provides automated exception and trend reporting to document compliance to internal and external auditors.

Policy compliance features are available when this module is enabled for the subscription. Please contact Technical Support or an Account Manager for information. Managers access these features automatically; sub-account users may be assigned access.

Auditor User Role

The Auditor user role grants the user permissions to compliance management features, including the ability to manage policies, create compliance reports, manage exceptions, manage asset groups and view user accounts.

Policy Editor

The Policy Editor provides a graphical user interface for Managers and Auditors to create and edit policies, and assign them to assets. Go to Policies and then select New > Policy. The policy may be divided into sections and can include a cover page to describe its purpose within the organization.
The application prompts you to set technologies — operating systems and applications, such as Windows XP Desktop, Windows 2003 Server, Oracle — and provide a policy title. Use the top menu bar to add controls and assign asset groups with compliance hosts. For each control, one or more checks (data points) are listed.

**Technical Controls.** Technical controls, maintained by the service, measure compliance against numerous policies and technologies.

**Technologies.** A technical control applies to one or more technologies, including operating systems and applications.

**Data Points.** These are the checks to the technologies that validate controls on the policy’s hosts. A default expected value is provided for each data point. Users can change the default value for some data points.
Policy Manager

Saved policies are saved in the Policy Manager. Over time policies may be updated to reflect new business practices, security policies and regulations. For each policy, the service tracks the user who created the policy, the date when created, the user who updated the policy and the date when last updated.

The service provides a Compliance Policy Library containing several sample policies as part of the Policy Manager, giving Auditors and Managers the ability to import them into the subscription and use them for compliance reporting. The sample policies are based on several popular compliance frameworks. Locked policies are available in the library for certification purposes, for example to certify that you are meeting all requirements outlined in a particular CIS benchmark.

To import a sample policy, go to Policies. From the Policies tab select New > Import Compliance Policy > Import from Library. The library includes multiple policies to choose from. Select a policy and then follow the workflow provided to assign asset groups to it.
Policy Compliance Reporting

These policy compliance reporting options are available: template based and interactive. These options are available from the New menu when you are in the Report section.

Running Template Based Reports

These template based compliance reports are derived from compliance scan data.

To run a report using a template, go to PC > Reports and select New > Compliance Report > Authentication report or Policy report.

Authentication Report. Identifies the authentication status for hosts in your account. Authentication to hosts is required for compliance scans. The service provides an authentication report template.

Policy Report. Identifies compliance with a specific policy that is defined in your account. (Available when the policy compliance module is enabled.) We provide the template “Policy Report Template” and we recommend this template to get started. Users may define custom policy report templates.

Running Interactive Reports

Interactive compliance reports support a dynamic workflow that allows users to update report content in iterations to view compliance status.

To run an interactive compliance report, go to PC > Reports and select New > Compliance Report > Interactive report. You’ll be prompted to select one of these reports:

Control Pass/Fail. Identifies the compliance posture (Passed or Failed) for a technical control in a particular policy.

Individual Host Compliance. Identifies the compliance status for a host in a particular policy. The controls applicable to the host are listed. For each control, the compliance posture (Passed or Failed) is listed.
Select settings for report source, display and sorting from within the report, and then run the report.

Report results appear in the same window as the report settings so you can change the settings and run the report again to find the compliance information you’re most interested in. Note: Interactive compliance reports are not saved to Report Share.

The details section of a sample Individual Host Compliance Report is below. For each control, the report identifies the expected value and actual value, as returned in the latest compliance scan results.
Exceptions Management

When viewing an interactive compliance report, users have the ability to submit exception requests for host/control pairs shown in the Results section.

Exceptions List — Go to Exceptions to view your exceptions list. All users view the status of all exception requests. Managers and Auditors approve requests. Unit Managers may be assigned this privilege for requests in their own business unit.

Submit in Single and Batch Mode — Users can submit exception requests one at a time or in batch mode. To submit a single request from the Control Pass/Fail Report, select the Request link next to a host. To submit requests in batch, select hosts using check boxes and then click the Request Exception button. The exceptions appear in the exceptions list which is available to all users.

Exception Approval — Exception requests must be accepted by an approver. Managers and Auditors are designated approvers.

Exception Timeframe — Exception requests may be approved for an explicit period of time, after which the exception expires automatically.

Exception Audit Trail — All information from the exception requestor and approver is captured and available for viewing. To view exception information, go Exceptions. From the exceptions list, select an exception row, click ➤ and then select Info from the Quick Actions menu.
POLICY COMPLIANCE — CURRENT REGULATIONS AND MANDATES

Qualys enables organizations to comply with a wide variety of government and industry regulations including:

Healthcare — HIPAA regulates the security and privacy of health data, including patient records and all individually identifiable health information.

Financial Institutions — GLBA requires IT controls to maintain the confidentiality and privacy of consumer financial information.

Online Merchants and Retailers — The Payment Card Industry mandates the protection of customer information residing with merchants, safe from attackers, viruses, and other potential security risks.

Public Companies — Sarbanes-Oxley requires effective controls and processes for validating the integrity of annual financial reports.

Government — FISMA requires that federal agencies establish risk-based information security programs to secure federal information.

California Commerce — CA 1798.92 mandates that organizations doing business in California report any cybersecurity breaches that may have compromised customer information.

Healthcare

DEFINITION: Health Insurance Portability and Accountability Act (HIPAA) regulations require organizations to enforce security controls that promote the confidentiality, integrity and availability of all personal health information.

CHALLENGE: HIPAA standards require organizations to use risk-based methods for protecting all health information. HIPAA specifies compliance guidelines for achieving a minimum security baseline in areas covering administrative and technical safeguards. HIPAA applies to any organization that processes, stores or manages personal health information electronically not just healthcare entities.

SOLUTION: Qualys is ideal for organizations looking to achieve and prove HIPAA compliance quickly and cost-effectively. The Qualys vulnerability management solution enables users to create HIPAA-specific reports to measure and document ongoing security compliance efforts.
Financial Institutions

**DEFINITION:** Gramm-Leach-Bliley Act (GLBA) regulations require organizations to protect themselves against unauthorized access, anticipated hazards and risks threatening the security or integrity of consumer financial information.

**CHALLENGE:** GLBA has introduced a great deal more rigor in how banks and credit unions have to handle, manage and secure their customers’ personal information. In today’s world much of our information is computerized making information security a major component of GLBA compliance.

The guidelines define customer information as any record containing a customer’s non-public personal information, whether in printed, electronic or other form. They require each institution to implement a written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank as well as the nature and scope of its activities.

**SOLUTION:** Qualys is ideal for organizations looking to achieve and prove GLBA compliance quickly and cost-effectively. The Qualys vulnerability management solution enables users to create GLBA-specific reports to measure and document ongoing security compliance efforts.
Online Merchants and Retailers

**DEFINITION:** The Payment Card Industry (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.

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

**CHALLENGE:** The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data, and affect all payment channels, including retail (brick-and-mortar), mail/telephone order and e-commerce.

Failure to comply with these security standards may result in fines, restrictions or permanent expulsion from card acceptance programs.

For more information on the PCI Data Security Standard, visit [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)

**SOLUTION:** As an approved PCI scanning vendor, Qualys is fully certified to help merchants and service providers to assess and achieve continuous compliance with the PCI Data Security Standard.

Public Companies

**DEFINITION:** Sarbanes-Oxley Act of 2002 (SOX) was passed to make corporate executives more responsible for their companies’ financial statements.

**CHALLENGE:** Section 404 of the Sarbanes-Oxley Act is relevant to information security as it requires management to demonstrate that they have established appropriate “internal controls” to safeguard an organization’s financial processes. The regulation’s internal controls specify that organizations safeguard financial data through the prevention and detection of security breaches that may have a material effect on financial statements.

**SOLUTION:** Qualys is ideal for publicly traded companies that need to meet compliance with Section 404 of Sarbanes-Oxley quickly and cost effectively. Qualys provides SOX-specific reports to measure, reduce and document ongoing efforts to safeguard electronic systems and data.
Chapter 5 — Compliance
Policy Compliance — Current Regulations and Mandates

Government


CHALLENGE: FISMA requires federal agencies to establish agency-wide risk-based information security programs to secure the information and information systems that support their associated operations and assets, and demonstrate how well they are meeting all of FISMA’s provisions. These provisions fall into three major categories: assessment, enforcement and compliance. Agencies that fail to comply with all FISMA mandates risk facing budget or resources cuts.

FISMA applies to any federal agencies, contractors or organizations whose information systems possess or make use of federal information.

SOLUTION: Qualys enables agencies to audit and measure their network risk, enforce security policies and document compliance with FISMA requirements. Qualys will explain each policy violation and tell you how to remediate the violation through a verified solution, for example by making a configuration change or applying a patch from a vendor.

California Commerce

DEFINITION: California Breach Disclosure Act (CA 1798.82), also known as SB 1386, requires State Agencies and private businesses to report cybersecurity breaches that may have compromised confidential information.

CHALLENGE: Organizations who fail to comply with CA 1798.82 face civil or class action lawsuits. The law covers not just California-based agencies but all private enterprises doing business in California. The law requires that California customers be notified if any unauthorized individuals have acquired their personal and/or financial information, thereby giving them the opportunity to take proactive steps to ensure that they do not become victims of identity theft.

Organizations that do not apply generally accepted security and detection best practices may be considered criminally negligent by State and Federal law. Becoming compliant with CA 1789.82 is not a one-time event, but rather a process that requires continuous measurement and management of network risks.

SOLUTION: Qualys helps organizations ensure data privacy by providing a security framework to measure, manage and mitigate network security risks. Qualys' Software-as-a-Service (SaaS) solution, Qualys, enables IT departments to eliminate network weakness through the proactive detection and remediation of security vulnerabilities.
SUCCESSFUL QUALYS ROLLOUT CASE STUDIES

As a step toward helping you understand how to succeed in your rollout of Qualys, it makes sense to provide you with actual case studies that call out practical examples and lessons learned. On the next several pages you will read summaries of choices made by some of our customers, the results of those choices emphasizing the real benefits Qualys provided to their organizations.

Case 1 — Global Online Retailer
Case 2 — Web Meeting Application Provider
Case 3 — Global Electronics Manufacturer
Case 4 — Global UK Bank
Case 5 — Large Chemical Company
Case 6 — Global Food Services Company
Case 1 — Global Online Retailer

Case Profile

**Infrastructure**
- Over 100,000 systems in 25 countries with strong presence in Asia and EMEA
- Centralized management of IT resources from corporate headquarters

**Situation before introduction of enterprise VM**
- Rapid growth caused uncertainty of network topology and system configurations
- The option was either doing no VA or building a Nessus-based system
- No ability to assess security situation and enforce security standards

**Motivation for introducing VM**
- Maintain confidence with the online marketplace that online transactions are in fact secure through their systems
- Have a tool to prove compliance to industry standards
- Need to quickly prioritize remediation when a severe new vulnerability emerges
- Reduce the costs around their patching process through automation

**Usage of VM**
- Up to 10 users (in Security Team), 12 scanning appliances in use — expanding up to 30
- Plan is to methodically introduce new geographic regions into established VM processes

**Ingredients for Success**

**#1 Obtain Executive Sponsorship for the VM program**
- Encourage highest ranking executive in your respective chain to send out an introductory email to all affected groups. The email should acknowledge that there is always uncertainty with such a program, however the benefits to the larger organization outweigh the risks.
- Exec support proves instrumental during the infrequent system failures that can occur.

**#2 Use VM to learn more about your environment first**
- Discover, understand and organize your network and the people managing the systems.
- Form Asset Groups and Business Units around the existing logical structure.
- Create a flexible solution to support a “living process” which adapts to different local operating environments while maintaining global standards and visibility

**#3 Build internal confidence — demonstrate that the technology is safe**
- Gain the trust and confidence of the operating teams and outsourcers.
- Work with Network and Operations Groups to identify the core pieces of infrastructure early and then form mapping/scanning plans around them.
Case 2 — Web Meeting Application Provider

Case Profile

**Infrastructure**
- 4,000 systems and 35 locations
- Internally managed network

**Situation before introduction of enterprise VM**
- No visibility, unknown network, patching status and exposure
- Ineffective homegrown tool

**Motivation for introducing VM**
- Reducing security risk and exposure
- Manage the lifecycle of vulnerabilities
- Gain visibility of network resources in general

**Usage of VM**
- 14 users in rollout — centralized with Corporate Security Team
- 4 appliances in two locations
- Weekly scanning and targeted remediation of all perimeter and internal systems
- Used for Access Control — new servers are put through a test before and after deployment

**Ingredients for Success**

**#1 Understand your environment prior to scanning**
- Do your homework in advance to understand your environment/network segments.
- Match your Business Units and Asset Groups accordingly to avoid what will invariably be double work.
- “Don’t want to spend time having to administer/change the configuration continually — I want to use it.”

**#2 Be conscious of how the rollout is perceived internally**
- Understand the needs of the different constituents.
- Learn when it’s best to schedule maps and scans.
- Begin with phased approach with Remediation expectations on IT (i.e. Severity Levels 4 and 5 to begin with).

**#3 Share report trending data to all involved parties**
- Trending data displaying the progress toward security posture can build confidence with internal groups.
Case 3 — Global Electronics Manufacturer

Case Profile

Infrastructure
- 20,000 systems worldwide
- Network managed by IBM in 85 locations

Situation before introduction of enterprise VM
- Relied entirely on IT group to confirm patches
- Two failed deployments of VM tools — far too difficult to manage
- Sever exposure to worms which infected significant parts of the network
- No central visibility of the network exposure

Motivation for introducing VM
- Empower local administrators to have domain knowledge and be accountable
- Protect against worms
- Ensure quality and timeliness of patching for severe vulnerabilities

Usage of VM
- 40 users in rollout
- 3 scanner appliances centrally managed
- Hold local administrators accountable to respond to regional remediation reports
- Weekly scanning of EMEA, APAC and Americas

Ingredients for Success

#1 Document the procedures around VM thoroughly
- List the steps to take should a host or system crash occur.
- Commit it to an SLA with Network Group to respond to such events.
- Set expectations clearly internally on the frequency and scope of mapping/scanning.
- Expect interesting interplays between the Network and Security Groups. There is often natural antagonism, however documentation and expectation setting aids greatly.

#2 Choose a top down approach (avoid a bottom up approach)
- Security Group may feel like they have to “yell louder” to get response from IT/Network Groups if there is not Executive sponsorship.
- Plan ahead to avoid an overreaction from IT/Network Groups to remediation efforts. Remediation policies can be very digestible if handled properly.
- IT Groups should be encouraged to display trend data on their progress.
Case 4 — Global UK Bank

Case Profile

**Infrastructure**
- 38,000 systems in 75 countries with strong presence in Asia, Middle East and Africa
- 600 applications running on a diverse infrastructure
- Systems managed by dozens of different IT teams and outside service providers

**Situation before introduction of enterprise VM**
- Network topology and system configurations unknown, spot auditing with pen-testing
- Local operating teams perform occasional scanning with various tools
- No ability to assess exposure and take corrective action

**Motivation for introducing VM**
- Have a clear picture of the exposure with common standards worldwide
- Need to quickly prioritize remediation when a severe new vulnerability emerges
- Motivate and empower outsourcing vendors to meet specific security SLA
- Reduce the cost and time of patching (“every patch costs money”)

**Usage of VM**
- Up to 200 users, 6 scanning appliances in use — expanding up to 40
- Security and Operating teams map and organize the network jointly
- Central Security team to configure the solution, setup user accounts, and create global scanning and reporting templates
- One cohesive view of the network, assets, vulnerabilities, remediation work in progress AND people engaged in the process

**Ingredients for Success**

**#1 Demonstrate that the technology is safe for your environment**
- Gain the trust and confidence of the operating teams and outsourcers

**#2 Use VM to learn more about your environment first**
- Discover, understand and organize your network AND the people managing the systems
- Allow for ongoing changes in an iterative process

**#3 Have a strong “service delivery” ownership of the process**
- Use VM as a vehicle to motivate and empower operating teams
- Develop better prioritization through more insight into your network and its assets
Case 5 — Large Chemical Company

Case Profile

Infrastructure
- 38,000 systems and 35 locations
- Network managed by up to 40 different outsourcers and IT service providers

Situation before introduction of enterprise VM
- No visibility: unknown network, patching status and exposure
- Outsourcers not compelled to maintain specific security SLAs

Motivation for introducing VM
- Understanding the network (agents too expensive and not available for some devices)
- Reduce cycle time for patching from over 30 days to 5 days across the enterprise
- Verify patches and standard builds
- Simplify IT audits via central repository vs. costly punctual audits

Usage of VM
- Up to 600 users in rollout, 20 appliances distributed worldwide, centrally managed
- Weekly scanning and remediation of all perimeter systems
- IT outsourcers ATOS Origin and IBM Global Services embedded in the process with direct access to the VM solution
- One cohesive view of the network, assets, vulnerabilities, remediation work in progress AND people engaged in the process

Ingredients for Success

#1 Forge partnership with the business
- Demonstrate the value to the operating teams and outsourcers
- Wealth of vulnerability intelligence from Qualys empowers functional groups with actionable data

#2 Be culturally sensitive in the rollout
- Don’t use VM results as a “stick” to beat up IT
- Reduce workload for everyone through automation and prioritization
- Demonstration the value-add through “quick wins”. For example:
  - scanned 256 production servers and found 22 “sasser” infections despite “patching”
  - supported SUS by identifying all Service Pack 2 installations
  - reduced the time and cost of IT audit by eliminating the need for punctual verification
    (all data can be accessed centrally)
Case 6 — Global Food Services Company

Case Profile

Infrastructure
- 313,000 employees with subsidiaries in 78 countries
- Heterogeneous and decentralized network
- 512 IP addresses, 119 domains, 6 scanner appliances

Situation before introduction of enterprise VM
- No VM solution
- Branches with wide-ranging autonomy
- No ability to centralize the supervision of the network security
- Network topology and system configurations unknown

Motivation for introducing VM
- Security supervision through the creation of a Global Security Team
- Establishment of a proactive and continuous vulnerability management policy
- Preservation of the autonomy of the various branches with tools that are easy to install and to use

Usage of VM
- Each organizational unit was given control and responsibility over its own resources
- Use Scans, Maps, Reports, Remediation & Schedules
- 74 users, 6 business units, 7 managers
- Typically 40 scheduled Scans per month, and 35 on demand Scans per month
- Typically 6 scheduled Maps per month, and 27 on demand Maps per month
### Ingredients for Success

<table>
<thead>
<tr>
<th>#1 Self-management for branches with a consistent policy throughout the enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Preservation of the decentralized organization</td>
</tr>
<tr>
<td>- A solution that is easy to implement, to use and to manage</td>
</tr>
<tr>
<td>- Ensure the people managing the systems and demonstrate Qualys value for operating team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#2 Define a strict methodology for scans and use of the collected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Define precise security rules</td>
</tr>
<tr>
<td>- Prioritize tasks and devices to be monitored</td>
</tr>
<tr>
<td>- Define realistic goals for remediation</td>
</tr>
</tbody>
</table>