



# GETTING STARTED WITH THE PCI COMPLIANCE SERVICE VERSION 5.5

December 20, 2011



Copyright 2006-2011 by Qualys, Inc. All Rights Reserved.

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

Qualys, Inc.  
1600 Bridge Parkway  
Redwood Shores, CA 94065  
1 (650) 801 6100



# Table of Contents

<b>Introducing the PCI Compliance Service.....</b>	<b>4</b>
PCI Data Security Standard .....	4
Using this Getting Started Guide.....	4
<b>First Steps .....</b>	<b>5</b>
Logging In .....	5
Change Your Login & Password (Optional) .....	6
Check Your Account Settings.....	6
Check Access to Scanner IP Addresses.....	7
Two-Factor Authentication (Optional) .....	7
<b>Network Scan .....</b>	<b>8</b>
Network Scan Workflow.....	8
Use Wizard to Add IPs and Domains to Your Account.....	8
Start New Network Scan.....	9
View Network Scan Results .....	13
Fix Vulnerabilities and Rescan.....	15
Submit False Positive Requests.....	17
View Open Services Report .....	20
View Compliance Status .....	21
<b>Network Compliance and Reports .....</b>	<b>22</b>
Network Reports Workflow .....	22
View Compliance Status .....	22
Use Wizard to Generate Network Reports.....	25
View Your Network Reports.....	26
Request ASV Review of Network Reports.....	30
Submit Network Reports .....	31
<b>Web Application Scan.....</b>	<b>32</b>
Web Application Scan Workflow .....	32
Add Web Application to Your Account .....	32
Add Authentication Records to Web Application .....	35
Start New Web Application Scan .....	37
View Web Application Scan Results .....	39
<b>Self-Assessment Questionnaire.....</b>	<b>40</b>
Questionnaire Workflow.....	40
Start New Questionnaire.....	41
Request Questionnaire Validation.....	46
Submit Your Questionnaire.....	46



# Introducing the PCI Compliance Service

Welcome to QualysGuard PCI, the on demand PCI compliance testing and reporting service from Qualys, Inc. Our company is certified as a PCI Approved Scanning Vendor (ASV) 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. To learn how to validate compliance with the PCI Data Security Standard, go [here](#).

## PCI Data Security Standard

The [PCI Security Standards Council](#) (PCI SSC) 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](#) (PCI 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. The PCI Security Standards Council released new Approved Scanning Vendor (ASV) requirements on March 16, 2010; these changes are detailed [here](#).

## Using this Getting Started Guide

This getting started guide walks you through how to complete the requirements for PCI certification as defined in the latest PCI DSS.

[First Steps](#) introduces you to the PCI Merchant user interface, your account, how to change your password and customize settings.

[Network Scan](#) covers the steps necessary to scan your Internet-facing IPs and domains that must be compliant with the PCI DSS requirements, perform remediation for vulnerabilities detected, submit false positive requests if appropriate, and rescan to verify your PCI compliance status passes all PCI DSS requirements. To get started, use the Wizard to add your in-scope IPs and domains.

[Network Compliance and Reports](#) covers how to review your PCI compliance status for all in-scope network components and then use the Wizard to review findings, perform the required attestation, and generate PCI network reports that you can later submit to your QSA or acquiring banks for PCI certification.

[Web Application Scan](#) describes meeting PCI DSS Requirement 6.6, which deals with security of web applications, by performing a web application scan.

[Self-Assessment Questionnaire](#) describes the SAQ v2.0 and how to complete this requirement.



## First Steps

All of your interactions with the PCI compliance service will be through its Security Internet Interface which you access using any standard Web browser. When you receive your registration email, follow the one-time secure link to view your login information, including your login credentials and platform URL where you log into the PCI Merchant application. Once you click this link it will no longer be active.

### Logging In

Simply open your browser and go to the platform URL for the PCI compliance service. Upon accepting the Service User Agreement you are directed to your Home page which presents your overall PCI compliance status and navigation options.

The screenshot displays the QualysGuard PCI dashboard. The header includes the QualysGuard PCI logo and the user name 'Irina Rockster' with links for 'Help' and 'Log Out'. The main content area is divided into three sections:

- Your Network Scans:** Shows a 'PASS Compliant' status. A table displays 'Total IPs' (2), 'Live IPs in Compliance' (100%), and 'Severity Count' (High: 0, Medium: 1, Low: 1). It also shows 'Last Submitted N/A' and 'Next Due N/A'.
- Self-Assessment Questionnaire:** Shows a 'PASS Completed' status. A table displays 'Questionnaire Type' (D), 'Completion Status' (100%), and 'Answer Count' (Yes: 221, No: 0, N/A: 3, CC: 1). It shows 'Last Submitted 08/29/2010' with a 'PASS' indicator and 'Next Due 08/29/2011'.
- Quick Answers:** A sidebar with frequently asked questions under categories like 'Network Scan', 'Questionnaires', and 'General'.


A left-hand navigation menu includes links for Home, Network, Compliance, Web Applications, Questionnaires, Account, Contact Support, and Resources.

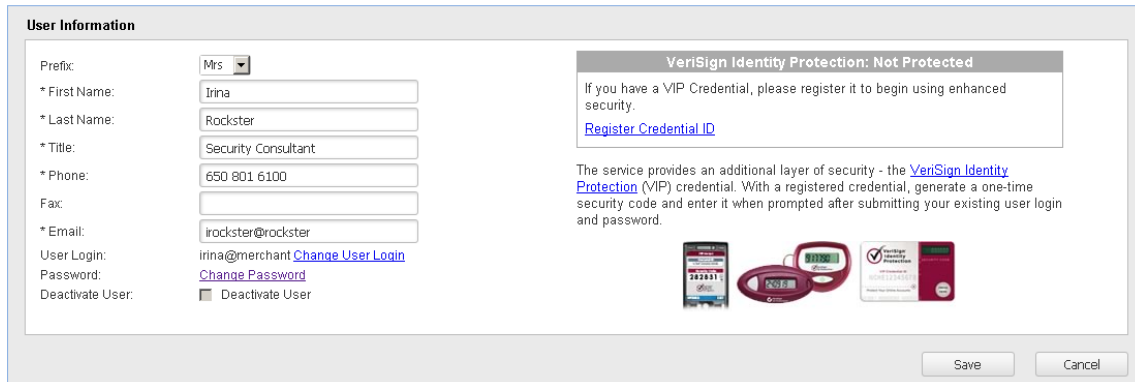
Your current compliance status is displayed for each PCI requirement, Network Scan and Self-Assessment Questionnaire, along with the details about your compliance progress. Use the links in the Quick Answers section to get help for frequently asked questions.

## First Steps

Change Your Login & Password (Optional)

# Change Your Login & Password (Optional)

At account creation time, you are assigned a user login and a randomly generated “strong” password. If you want to change your user login and/or password, you can do so at any time by editing your user account. Go to Account—>Users on the left menu. Identify your own user account (it will be in bold), and click . The Edit User page appears with User Information.



**User Information**

Prefix: Mrs

\* First Name: Irina

\* Last Name: Rockster

\* Title: Security Consultant

\* Phone: 650 801 6100

Fac:

\* Email: lrockster@rockster

User Login: irina@merchant [Change User Login](#)

Password: [Change Password](#)


Deactivate User:  Deactivate User

**VeriSign Identity Protection: Not Protected**

If you have a VIP Credential, please register it to begin using enhanced security.

[Register Credential ID](#)

The service provides an additional layer of security - the [VeriSign Identity Protection](#) (VIP) credential. With a registered credential, generate a one-time security code and enter it when prompted after submitting your existing user login and password.



Save Cancel

**Change User Login** — Select this link to change your user login. You’ll be prompted to enter your current login and a new login. Your user login must be unique and must include the @ character, such as john@company. Click “Change and Logout”. Then log in with your new user login.

**Change Password** — Select this link to change your password. Your password must be a minimum of 6 characters and must include a combination of alpha and numeric characters. Click “Change and Logout”. Then log in with your new password.

## Check Your Account Settings

The Account section is where you can display important information about your Merchant subscription, your user account, and it allows you to make custom settings.

Go to Account—>Settings to verify details about your Merchant subscription. Review your merchant information, subscription information, including the total number of IPs purchased, the total number of IPs currently in your account, and your bank information. You can edit many of these settings.

Go to Account—>IP Assets to view the IP addresses and domains in your account. These are the IP addresses for the hosts that must be compliant with the PCI requirements. You can add and remove IP addresses as needed.

Go to Account—>Web Applications to view the web applications in your account. These are the web application that you need to scan to meet PCI DSS Requirement 6.6. Customers are required to add web applications since their settings depend on each customer’s environment.

Go to Account—>Users to view your user account settings, edit these settings, and add more users if you wish. By adding users you can share the PCI scanning and reporting responsibilities. All users have the same privileges to access and manage questionnaires and network reports. See “Managing Users” in the online help for details.

## Check Access to Scanner IP Addresses

Per the PCI Council's Program Guide, it is your responsibility to confirm that the PCI network scan of your entire in-scope infrastructure can be performed without interference from intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

Only IPs that are accessible from the Internet are scanned by the service. The service automatically provides multiple scanners for external (perimeter) scanning, located at the Security Operations Center (SOC) that is hosting the PCI compliance service. Depending on your network, it may be necessary to add the scanner IPs to your list of trusted IPs, so the service can send probes to your in-scope system components.

The scanner IPs are:


62.210.136.128/25 (62.210.136.129-62.210.136.254)

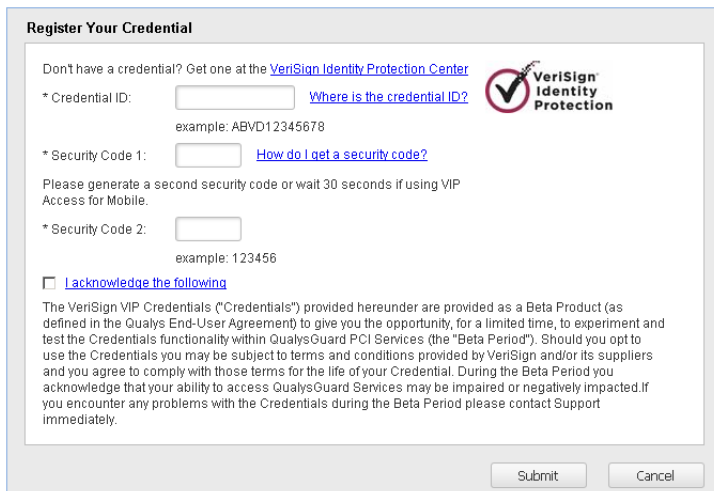
64.39.96.0/20 (64.39.96.1-64.39.111.254)

167.216.252.0/26 (167.216.252.1-167.216.252.62)

## Two-Factor Authentication (Optional)

Support for VeriSign Identity Protection (VIP) two-factor authentication is available. You can obtain a VIP Credential ID from VeriSign at: <https://idprotect.verisign.com/mainmenu.v>

To register a VIP Credential ID, go to Account—>Users on the left menu. Identify your own user account (it will be in bold), and click . Select the "Register Credential ID" link in the VeriSign Identity Protection box. The Register Your Credential form appears. Note that two security codes are required to register your VIP Credential ID.



**Register Your Credential**

Don't have a credential? Get one at the [VeriSign Identity Protection Center](#)

\* Credential ID:  [Where is the credential ID?](#)

example: ABVD12345678

\* Security Code 1:  [How do I get a security code?](#)

Please generate a second security code or wait 30 seconds if using VIP Access for Mobile.

\* Security Code 2:

example: 123456

[I acknowledge the following](#)

The VeriSign VIP Credentials ("Credentials") provided hereunder are provided as a Beta Product (as defined in the Qualys End-User Agreement) to give you the opportunity, for a limited time, to experiment and test the Credentials functionality within QualysGuard PCI Services (the "Beta Period"). Should you opt to use the Credentials you may be subject to terms and conditions provided by VeriSign and/or its suppliers and you agree to comply with those terms for the life of your Credential. During the Beta Period you acknowledge that your ability to access QualysGuard Services may be impaired or negatively impacted. If you encounter any problems with the Credentials during the Beta Period please contact Support immediately.

Submit Cancel

Once you register your VIP credential, logging in will be a two-part process. You'll enter your PCI user login and password and then you'll need to enter a new VIP security code.



# Network Scan

The PCI DSS requires all merchants and service providers to perform network security scans of their Internet facing IP addresses on a quarterly basis. To determine your network status, first add IP addresses if target IPs are not already in your account, and then scan your network for vulnerabilities.

Scan your network in segments and remediate/rescan vulnerabilities on target IP addresses until you achieve PCI compliance. Segmented scanning allows you to scan hosts that you have remediated, without having to scan your entire network. After fixing vulnerabilities required to pass PCI compliance, you are ready to generate network reports.

## Network Scan Workflow

Step 1: Use Wizard to Add IPs and Domains to Your Account

Step 2: Start New Network Scan

Step 3: View Network Scan Results

Step 4: Fix Vulnerabilities and Rescan

Step 5: Submit False Positive Requests

Step 6: View Open Services Report

Step 7: View Compliance Status

## Use Wizard to Add IPs and Domains to Your Account

The PCI service provides a System Components Wizard to assist you in configuring your account for PCI network scans. Per the PCI Council's Program Guide, you are responsible for defining the in-scope infrastructure for the PCI network scan. Your account must include all Internet-facing IP addresses and/or ranges. If you have domains that host in-scope PCI infrastructure you need to configure your account to also include these domains.

Walk through the wizard to do the following:

- Add IP addresses and/or IP ranges to your account.
- Add domains to your account, including domains that host your online payment applications, such as web servers, mail servers, virtual hosts and web applications.
- Confirm that the load balancers on your network and systems behind them are configured correctly.

To access the wizard, click the Asset Wizard button on the Home page. Then follow the online prompts to configure your account.



## Manage IP Assets in Your Account

From the IP Assets page (Account—>IP Assets), you can view the IP addresses and domains in your account, add more IP addresses to your account, remove IP addresses from your account, and perform a discovery scan to find IP addresses on your network. You can also view out of scope assets, including IP addresses that were previously in-scope but removed from the account and IP addresses that were discovered by the service as part of your in-scope infrastructure. See the online help for complete information on these options.

## Start New Network Scan

When starting a network scan, you have the option to scan all IP addresses in your account or only selected IP addresses. The underlying scan settings have been optimized to test compliance with the PCI Data Security Standard. There is one user-configurable scan performance setting - Bandwidth - which affects overall scan performance. It's recommended that you use the default bandwidth level (Medium) to get started.

You'll have the option to launch your scan immediately or schedule it to start on a future date/time.

To start a network scan, go to Network—>New Scan on the left menu. If there are no IP addresses in your account, you are prompted to enter IPs.

The New Scan page appears.

The screenshot shows a web application interface for QALYS GUARD PCI. At the top, there is a blue header with the text 'Payment Card Industry Compliance' and 'Inna Rockster | Help | Log Out'. Below the header, the main content area is titled 'New Scan'. A modal dialog box titled 'Scan Settings' is open, containing the following configuration options:

- \* Title: My First Network Scan
- \* Bandwidth: Medium (with an Info link)
- \* Target IPs:  All IPs,  Select IPs (with an empty text box below)
- \* Launch:  Launch Now,  Schedule for Later

Buttons for 'OK' and 'Cancel' are located at the bottom right of the dialog.

### Scan Settings

**Title** — A user-defined scan title. The title appears in the Scan Results list (Network—>Scan Results) and the Scan Results Report.

**Bandwidth** — Select a bandwidth level. It's recommended that you keep the default bandwidth level Medium (15 IP addresses may be scanned in parallel). Bandwidth setting options are High, Medium (the default), Medium - low HTTP impact, Low, and Lowest. Select the Info link for detailed information on the bandwidth levels.

**Target IPs** — Select the IP addresses you want to scan. You can enter IPs and IP ranges, separated by commas. If you select the All IPs option, all IPs in your account will be scanned. If you select the Select IPs option, only selected IPs in your account will be scanned. Enter the target IP addresses in the field provided or click the Select IPs link to choose IPs from a list.

### Scan Launch

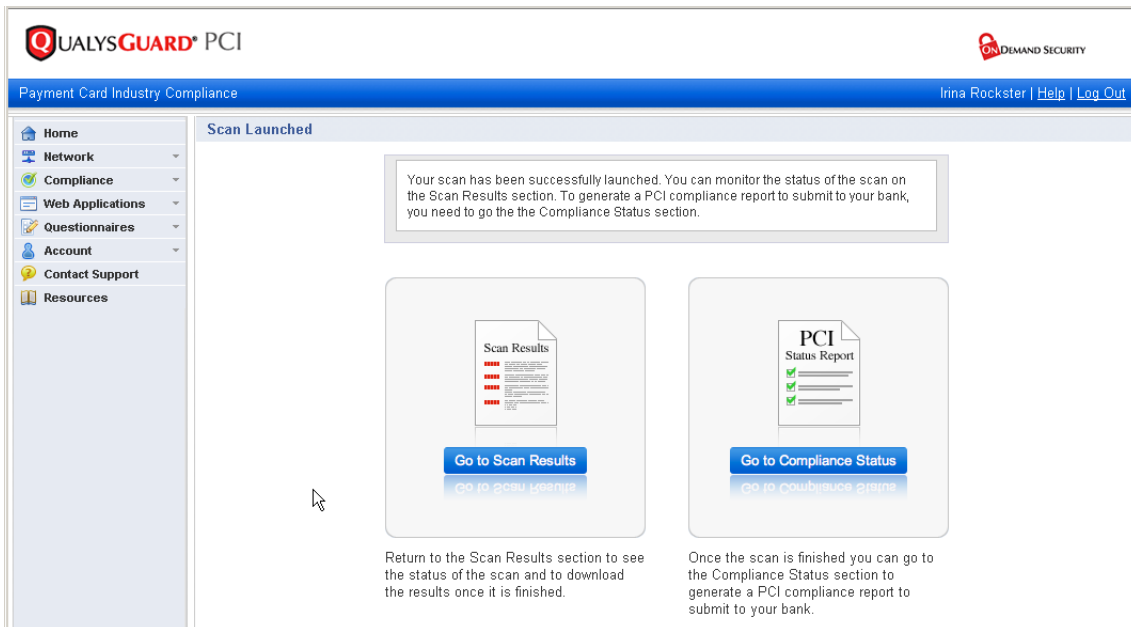
Select one of these options:

- **Launch Now** — Launch the scan immediately.
- **Schedule for Later** — Schedule the scan to start at a later time. You can also schedule a scan to repeat on a daily or weekly basis. See "Scan Scheduler."

### Save Scan

Click OK to save the scan. If you selected "Launch Now" the scan is started right away.

The Scan Launched section indicates that your scan has been successfully launched.



The scan runs in the background so you can exit the PCI web application while the scan continues, and then return to the application at a later time.

**Go to Scan Results** — Click to go to the Scan Results section to monitor the scan status and cancel the scan. When the scan has finished, you can download the Scan Results Report. This report identifies all vulnerabilities detected by the service (and cannot be submitted for PCI certification). See “View Network Scan Results.”

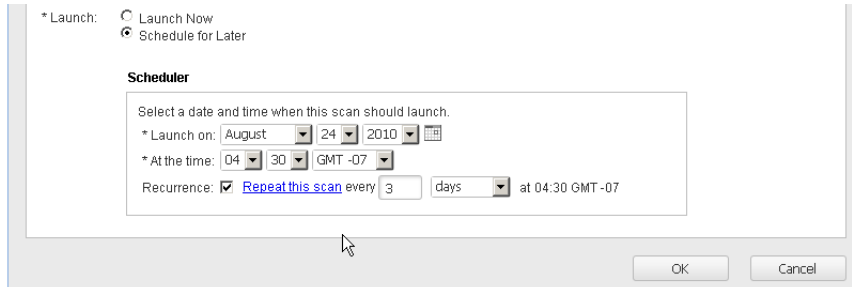
**Go to Compliance Status** — Click to go to the Compliance Status section and view the current compliance status for all hosts in your account. See “View Compliance Status.” When the scan has finished, you can generate network reports. The Report Generation Wizard assists you with generating the reports and completing all PCI reporting requirements. See “Use Wizard to Generate Network Reports.”

## Scan Summary Email

When the scan has finished, you will receive a Scan Summary email notification with a link to access the PCI Merchant application so you can log back in to view your scan results. The email includes scan details, including the scan title, launch date, name of the user who initiated the scan, the number of active hosts, and the PCI compliance status based on the scan results.

## Scan Scheduler

On the New Scan page, you have the option to schedule a one-time network scan to start at a later time or schedule a recurring scan to run on a daily or weekly basis. To do so, select the “Schedule for Later” option. You will be prompted to provide the date and time when the scan should run. Optionally, set recurrence to repeat the scan.



\* Launch:  Launch Now  Schedule for Later

**Scheduler**

Select a date and time when this scan should launch.

\* Launch on: August 24 2010

\* At the time: 04 30 GMT-07

Recurrence:  Repeat this scan every 3 days at 04:30 GMT-07

OK Cancel

**Launch on** — Select the month, day and year when this scheduled scan should launch. Use the calendar pop-up to assist you.

**At the time** — Select the time when this scheduled scan should launch. Select hours and minutes in 24 hour format. The GMT shift is set automatically based on your local system setting. You may select a different GMT shift from the menu provided.

**Recurrence** — If you want the scheduled scan to repeat on a daily or weekly basis, select the option Repeat this scan. For a daily recurrence, enter between 1-31 days to launch your scan every 1 day, 2 days, 3 days, etc. For a weekly recurrence, enter between 1-13 weeks to launch your scan every 1 week, 2 weeks, 3 weeks, etc. The scheduled recurring scan will continue to launch at the specified time unless you deactivate or delete it.

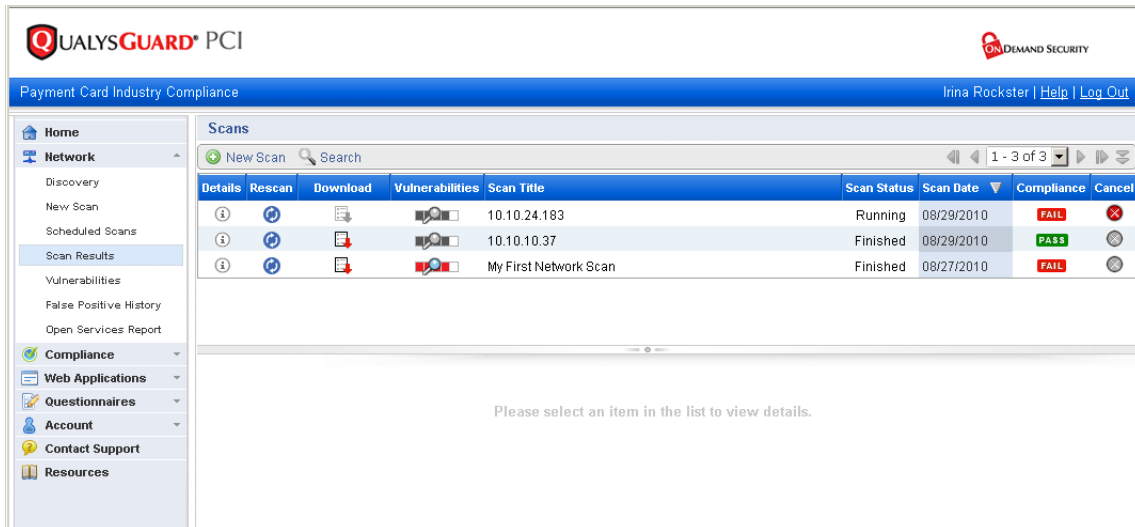
After clicking OK, your scheduled scan appears on the Scheduled Scans list (Network—> Scheduled Scans). You can return to this list at any time to view, edit or delete your pending network scans. You can also deactivate a scheduled scan if you don’t want it to launch at its scheduled time (edit the schedule and click “Deactivate this schedule”).

If the scan target includes all IP addresses in your account, then the service will scan all IP addresses in your account at the time that the scan is launched. For example, if you schedule a scan when there are 2 IPs in your account and then add 3 IPs to your account before the scan is launched, the service will scan 5 IPs.

## View Network Scan Results

The Scan Results section shows a complete history of your network scans. Return to the Scan Results section at any time for the latest scan status. To do this, go to Network—>Scan Results on the left menu. Your scans run in the background so you can exit the PCI web application while scans are in progress.

After you launch your first scan, there is only one scan in the list. Over time there will be more scans in the Scans list.



### Manage scan tasks

Cancel — Click to cancel a running scan.

New Scan — Select this link (above the scans list) to start a new scan.


Rescan — Click to start another scan using the same scan settings as a previously launched scan. The New Scan page appears with the scan settings pre-populated, including the scan bandwidth, title, and target IPs. For a scheduled scan, the start date is automatically set to the current date (other scheduler settings remain the same).

Search — Select this link to search for a particular scan in the list. You can find scans based on scan title, scan status, scan date and compliance status.

### View scan information

Details — Click to view scan details for a scan task, including the scan title, when the scan was launched, the user who launched the scan, the scan status, the target IPs, whether the scan was launched on demand or scheduled, and the scan bandwidth setting.

Download — Click to download the Scan Results Report in PDF format. The Detailed Results section of the report displays all vulnerabilities detected by the service at the time of the scan. All vulnerabilities and potential vulnerabilities with a PCI status of FAIL must be fixed to pass the PCI compliance requirements.

Vulnerabilities — Click  to see a list of all current vulnerabilities associated with the scan's target IPs. Current vulnerabilities are those vulnerabilities detected by the most recent scan of each host. For this reason, the current vulnerabilities list may have more up-to-date information than the Scan Results Report. See “Fix Vulnerabilities and Rescan.”

Compliance — Identify whether the scan is compliant with the PCI Data Security Standard. **PASS** indicates that the scan is Compliant. No vulnerabilities that fail PCI compliance were found on the target IPs. **FAIL** indicates that the scan is Not Compliant. One or more vulnerabilities that fail PCI compliance were found on the target IPs.

## PCI Pass/Fail Criteria

The calculation of the PCI pass/fail compliance status follows the PCI compliance standards set by the PCI Security Standards Council.







For each vulnerability, the PCI compliance service uses the CVSS version 2.0 base score provided by NIST to determine whether the vulnerability must be fixed to pass PCI compliance requirements. When a CVSS version 2.0 score is not available from NIST, the service provides a CVSS 2.0 score and uses that score to determine whether the vulnerability must be fixed.

**Important:** The service uses the PCI severity level and other criteria, as defined by the PCI Security Standards Council, to determine whether a detected vulnerability passes or fails the PCI compliance requirements. Please note that the PCI severity level, based on CVSS score, is not the only criteria used to calculate a vulnerability's pass/fail status. A vulnerability may pass or fail PCI compliance based on the type of exploit. For example, a denial of service vulnerability will pass PCI compliance regardless of its CVSS score.

## PCI Severity Levels

Each vulnerability is assigned a PCI severity level of High, Medium or Low, which is based on the CVSS score assigned to the vulnerability. A vulnerability with a High or Medium severity level will fail PCI compliance. A vulnerability with a Low severity level will pass PCI compliance.

See the table below for PCI severity levels based on CVSS scores.

CVSS Score	Confirmed Severity	Potential Severity	Compliance	Guidance
7.0 through 10.0			Fail	These vulnerabilities must be fixed to pass PCI compliance. Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical ones (rated 10.0), followed by those rated 9, 8, 7, etc., until all vulnerabilities rated 4.0 through 10.0 are corrected.
4.0 through 6.9			Fail	
0.0 through 3.9			Pass	These vulnerabilities are not required to be fixed to pass PCI compliance. Organizations are encouraged, however, to correct these vulnerabilities.

## Fix Vulnerabilities and Rescan

The Current Vulnerabilities list provides a list of current vulnerabilities and potential vulnerabilities detected on all IP addresses in your account. These are the vulnerabilities detected by the most recent network scan of each host in your account. All detected vulnerabilities are listed, including vulnerabilities that must be fixed to pass PCI compliance as well as vulnerabilities that we recommend that you fix. For each vulnerability you can view detailed information for remediation so that you can quickly fix and eliminate the vulnerability.

To view the Current Vulnerabilities list, go to Network—>Vulnerabilities on the left menu. The service automatically displays all current vulnerabilities and potential vulnerabilities on all IP addresses in your account. Click on any row in the list to display vulnerability details.

The screenshot displays the 'Current Vulnerabilities' dashboard. At the top, there's a search section for IP addresses and filter options for severity levels (High, Med, Low) and PCI fail vulnerabilities. An 'ACCOUNT SUMMARY' bar shows counts for HIGH (4), MED (2), and LOW (28) vulnerabilities. Below this is a table of vulnerabilities with columns for Title, Severity, and IP Address. The first row is highlighted, showing a 'Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040)' with a severity of HIGH. To the right of the table is a detailed view of this vulnerability, including its QID (90336), category (Windows), and a description of the threat and impact.

Vulnerability Title	Severity	IP Address
Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040) QID: 90336 <b>FAIL</b>	HIGH	10.10.10.216 lotus-10-216
SSL Server Has SSLv2 Enabled Vulnerability QID: 38139 <b>FAIL</b>	MED	10.10.10.216 lotus-10-216
SSL Server Supports Weak Encryption Vulnerability QID: 38140 <b>FAIL</b>	HIGH	10.10.10.216 lotus-10-216
SSL Certificate - Self-Signed Certificate QID: 38169	HIGH	10.10.10.216 lotus-10-216
SSL Certificate - Subject Common Name Does Not Match QID: 38170	LOW	10.10.10.216 lotus-10-216
SSL Certificate - Signature Verification Failed Vulnerability QID: 38173	HIGH	10.10.10.216 lotus-10-216
Anonymous Access to LDAP Server QID: 45007	MED	10.10.10.216 lotus-10-216
NetBIOS Name Accessible QID: 70000	LOW	10.10.10.216 lotus-10-216
Lotus Domino Anonymous SMTP Access Allowed QID: 74205	LOW	10.10.10.216 lotus-10-216
POP3 Server Allows Plain Text Authentication Vulnerability QID: 74224 <b>FAIL</b>	MED	10.10.10.216 lotus-10-216
ICMP Timestamp Request QID: 82003	LOW	10.10.10.216 lotus-10-216

**Vulnerability Details:**  
**Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040)**  
 10.10.10.216  
 lotus-10-216  
 QID: 90336 **FAIL** CVSS Base: 10  
 Category: Windows CVSS Temporal: 7.4  
 Port/Service: - / Windows False Positive: Requested on 08/27/2010  
 Bugtraq ID: 19409  
 CVE ID: CVE-2006-3439  
 Vendor Reference: MS06-040  
 Last Update: 09/21/2007 at 16:55:06  
 Threat:  
 An unchecked buffer in the Server service is responsible for a remote code execution vulnerability. Any anonymous user who can deliver a specially crafted message to the affected system could try to exploit this vulnerability.  
 The Server service provides RPC support, file print support and named pipe sharing over the network. The Server service allows the sharing of your local resources (such as disks and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC.  
 Impact:  
 An attacker who successfully exploits this vulnerability could take complete control of the

### Filter the list of vulnerabilities

Use the search and filter settings (at the top of the page) to only show vulnerabilities for certain IPs or vulnerabilities with certain attributes.




**Search by IP Address** — Use this field to search for vulnerabilities by IP address. Enter one or more IP addresses and/or IP ranges in the field provided (separating each IP/range with a comma) and then click Find IP Address. The current vulnerabilities list is updated to only show vulnerabilities for the IPs that you entered.

## Network Scan

Fix Vulnerabilities and Rescan

**Filter Results** — Use this field to search for vulnerabilities by QID, vulnerability title or hostname. As you type in the field, the list of vulnerabilities is dynamically updated to match your entry. For example if you type “OpenSSH”, the list is filtered to only show vulnerabilities with “OpenSSH” in the title. If you type “105” then the list is filtered to only show vulnerabilities with a QID that includes “105” such as 10579, 105236, and 43105.

**Display only PCI Vulnerabilities** — Select this option to display only vulnerabilities that must be fixed to pass PCI compliance. The PCI compliance service uses CVSS version 2.0 base scores and other criteria to determine the PCI pass/fail status. See “PCI Pass/Fail Criteria.”

**False Positives** — Search for vulnerabilities with associated false positive requests that are Requested (  ), Rejected (  ), or Expired (  ). Expired false positives were approved but expired after 90 days.

**Potential/Confirmed Severity Level** — Select each severity level you want to include in the current vulnerabilities list. See “PCI Severity Levels” for a description of each level.

**Hide Filters/Show Filters** — You can hide the filter settings to maximize the space available for the list view by clicking Hide Filters. To show the filter settings again click Show Filters.




## Account Summary Graph


The Account Summary graph displays the total number of confirmed vulnerabilities (red) and potential vulnerabilities (yellow) on all hosts in your account at each PCI severity level (High, Medium and Low).

## Current Vulnerabilities List

When no filter settings are selected, all current vulnerabilities on all IPs in your account are displayed. If filter settings are selected, the list is restricted to the vulnerabilities that match your search criteria. Click on any row in the list to see additional vulnerability details, like the CVSS scores assigned to the vulnerability, the Threat, Impact and Solution descriptions, and specific scan test results for the vulnerability instance.




The Current Vulnerabilities list includes the following information:

**Type** — Icons are used to represent the different types of vulnerabilities that may be detected during a network scan:  represents a network vulnerability,  represents a web application vulnerability, and  represents an SSL certificate vulnerability.

**Vulnerability Title** — The vulnerability title and the QID assigned by the PCI compliance service.  appears next to each vulnerability that fails PCI compliance. These vulnerabilities must be fixed to pass PCI compliance. The PCI compliance service uses CVSS version 2.0 base scores and other criteria to determine the PCI pass/fail status. See “PCI Pass/Fail Criteria.”

**Severity** — The PCI severity level: High, Medium or Low. See “PCI Severity Levels.”

**IP Address** — The IP address and hostname for the host that the vulnerability was detected on.

**Scanned** — The date the scan was started. If a false positive request was submitted for the vulnerability then one of these indicators may appear below the date:  indicates that a false positive request was submitted for approval,  indicates that the false positive request was rejected, and  indicates that the false positive request was approved but expired after 90 days. You must submit a new false positive request for this vulnerability to pass PCI compliance.

## Take actions

Use the actions bar above the Current Vulnerabilities list to take actions on your current vulnerabilities. These buttons allow you to take actions:

**Download All** — Click to download a report of your current vulnerabilities list in CSV format. Note: All current vulnerabilities detected on all hosts are included in the report, even if you've filtered the list of vulnerabilities.

**Review False Positives** — Select vulnerabilities from the list using the check boxes (in the left column) and then click the Review False Positives button to review vulnerability details and submit false positive requests, if appropriate. See "Submit False Positive Requests."

## Rescan hosts to verify fixes

After fixing the critical vulnerabilities, start another network scan. It's possible to launch a scan on selected hosts, in case you need to verify compliance status on certain hosts. Segmented scanning allows you to scan hosts that you have fixed, without scanning your entire network. The network scan analyzes your hosts for vulnerabilities again and validates that previously detected vulnerabilities have been fixed.

## Submit False Positive Requests

It's possible after fixing all vulnerabilities, as defined by the PCI DSS compliance standards, that you have an issue that doesn't seem to apply to the host. In this circumstance, you may request an exception that will be considered by us as a false positive.

Before making this request, complete all remediation steps to fix vulnerabilities by following these guidelines:

- Work with your system administrator to fix all vulnerabilities in your scan results using the recommended solutions. A custom solution is provided for each vulnerability in the vulnerability details.
- Re-scan after fixing vulnerabilities to validate that systems are not vulnerable. You can re-scan as often as necessary to track remediation progress.
- Before you submit a false positive, be sure to fix all vulnerabilities except the false positive issues. Your last re-scan should show only the false positive issues.

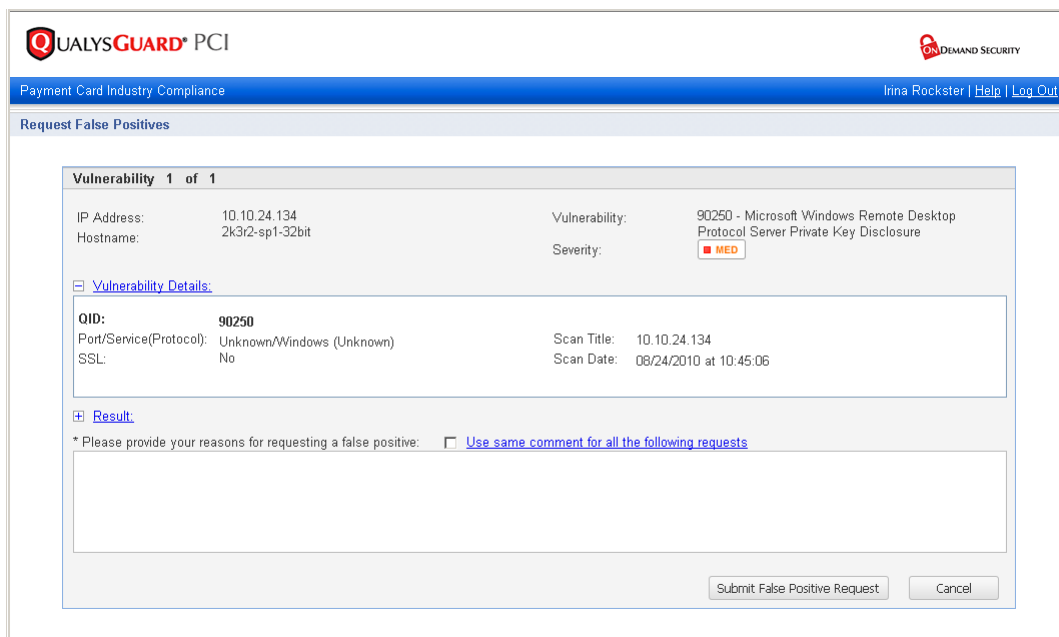
If you followed the guidelines above and believe that the PCI compliance service has identified a false positive in your scan, then use the steps below to submit a false positive request to Technical Support.

### To submit a false positive request:

- 1 Select Network—>Vulnerabilities on the left menu.
- 2 Optionally, use the search and filter options at the top of the page to find specific vulnerabilities or hosts.
- 3 Select the check box to the left of each vulnerability you want to include in your request and click the Review False Positives button. Note it's not possible to select a check box for a vulnerability that is not required to fix in order to pass PCI compliance.

- 4 On the Request False Positives page, provide a detailed explanation for each selected vulnerability as to why you believe it is a false positive. Your reason should include steps taken to validate that it is a false positive. An error will occur if you select a vulnerability without providing an explanation.

If you selected multiple vulnerabilities, you have the option to enter one reason for the requests by selecting the check box "Use same comment for all the following requests".



The screenshot shows the QALYS GUARD PCI interface for "Payment Card Industry Compliance". The user is logged in as Irina Rockster. The page title is "Request False Positives".

**Vulnerability 1 of 1**

IP Address:	10.10.24.134	Vulnerability:	90250 - Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure
Hostname:	2k3r2-sp1-32bit	Severity:	<span style="background-color: #f08080; padding: 2px;">MED</span>

[Vulnerability Details:](#)

QID:	90250	Scan Title:	10.10.24.134
Port/Service(Protocol):	Unknown/Windows (Unknown)	Scan Date:	08/24/2010 at 10:45:06
SSL:	No		

[Result:](#)

\* Please provide your reasons for requesting a false positive:  [Use same comment for all the following requests](#)

- 5 Click the Submit False Positive Request button.

When you submit the false positive request, an email is sent to Technical Support for review. A Technical Support representative will work with you to determine if the identified issue is indeed a false positive and will send you an email response.

**Approved** — If the false positive request is approved, then it is approved for 90 days. The service automatically updates vulnerability and compliance status information in these ways:

- **Scan Results Reports:** The vulnerability for the host is removed from the Scan Results Report returned by the most recent host scan. Also, the vulnerability for the host will not show up in future scan results for the host for the next 90 days.
- **Current Vulnerabilities:** The vulnerability for the host is removed from the Current Vulnerabilities list.
- **Compliance Status:** The Compliance Status section is updated to show that the vulnerability for the host will not cause you to fail PCI compliance.
- **PCI Network Reports:** The next time you generate PCI network reports from the Compliance Status section, the reports indicate that the vulnerability for the host does not cause you to fail PCI compliance. In the PCI Technical Report you'll see the vulnerability for the host listed as a false positive in the "Approved False Positives Details" appendix.

Rejected — If the false positive request is not approved, you must fix the vulnerability in order to pass PCI compliance standards. Remediation steps are provided in the Solution section of the vulnerability details.

### False Positive Expiration

Each approved false positive is valid for 90 days. After 90 days, the approved false positive will expire automatically. The next time you run a network scan after a false positive expires, if the QID is detected on the host, you will fail PCI compliance.

After the false positive expires and the vulnerability is detected in a new scan, the vulnerability will be listed on the Current Vulnerabilities list with an indicator that there is an expired false positive associated with the vulnerability. A new false positive request must be submitted and approved to pass PCI compliance.

It is best practice to track the false positive status of your approved false positives and to submit new false positive requests as needed.

### View False Positive History

To view the false positive history, go to Network—>False Positive History on the left menu. All false positive requests that have been submitted by all users are listed.

The screenshot shows the QualysGuard PCI interface. The top navigation bar includes the QualysGuard PCI logo and the Demand Security logo. The main content area is titled "False Positive Request History" and contains a table with the following data:

Details	QID	Title	IP	Requested	Reviewed	Status
<a href="#">(i)</a>	90477	Microsoft SMB Remote Code Execution Vulnerability ...	10.10.24.134	08/24/2010	08/24/2010	Approved
<a href="#">(i)</a>	90250	Microsoft Windows Remote Desktop Protocol Server P...	10.10.24.134	08/24/2010	08/25/2010	Approved

Below the table, there is a section for "[90477] - Microsoft SMB Remote Code Execution Vulnerability (MS09-001)". This section includes "General Information" and "Comment History".

**General Information**

Host IP:	10.10.24.134	Severity Level:	<span style="color: red;">HIGH</span>	Port/Service:	- / Windows
Scan Title:	10.10.24.134	Scanned:	08/24/2010	Status:	Approved

**Comment History**

- 08/24/2010 - Service Representative: This false positive request has been approved by the ASV.
- 08/24/2010 - Irina Rockster: Please consider QID 90477 for host 10.10.24.134 as a False Positive.

This information is listed for each false positive request: vulnerability ID (QID), vulnerability title, IP address of the host the vulnerability was detected on, date the request was submitted by a user, date the request was reviewed and updated by a service representative, and false positive status (Requested, Approved, Rejected or Expired).

Select ⓘ next to a request to view request details and comment history. Click the Search link to search for requests by various criteria including when false positives are set to expire.

Click the Download All button to download the list information in CSV format. The downloaded report identifies all false positive requests submitted by all users, and includes false positive details and comments for each request.

## View Approved False Positive Details in Technical Report

The appendix “Approved False Positive Details” appears in the PCI Technical Report to assist users with vulnerability management. This report appendix provides a list of vulnerabilities that were approved as false positives on the hosts in the report. The false positives list includes approvals for *current vulnerabilities* on the hosts in the report. It does not include any approvals for vulnerabilities which were not detected by the latest scan of each host.

## View Open Services Report

The Open Services Report is an interactive report provided to assist merchants with satisfying PCI DSS requirement 1.1.5. This report includes a complete list of services, protocols and ports detected by the most recent scans across all IPs on your network. Review the list of detected services and classify each service as Authorized or Unauthorized. Once you have reviewed all the services and classified them appropriately, you can download a report for auditing purposes.

To view the Open Services Report, go to Network—>Open Services Report on the left menu.

**QUALYS GUARD PCI** DEMAND SECURITY

Payment Card Industry Compliance Irina Rockster [TechPubs Shop] | Help | Log Out

**Open Services Report**

### Summary

PCI DSS requirement 1.1.5 requires documentation and business justification for use of all services, protocols and ports allowed. To meet this requirement, review the detected services below, classify each as Authorized or Unauthorized, and then generate a report.

There are **14 total** services identified by the most recent scans on all IPs.

**Authorized** 2     **Unauthorized** 1     **Unreviewed** 11

### Open Services

Classify as: [v] Download [v] Group By: IP Address Filter By: All Search [ ] Showing 1 - 10 of 14

Service	Port	Protocol	Description	Hostname	Last Detected On	Classification	Comments
IP: 10.10.10.37 (10 Services)							
ssh	22	TCP	SSH Remote Login Protocol	dhcp-37.qualys.com	03/06/2011	<input checked="" type="checkbox"/> Authorized	Irina Rockster 03/08/2011 The ssh service is authorized for this host.
unknown	2522	TCP	WinDb	dhcp-37.qualys.com	03/06/2011		
unknown	2932	TCP	unknown	dhcp-37.qualys.com	03/06/2011		
vnc	5900	TCP	vnc	dhcp-37.qualys.com	03/06/2011		
unknown	6085	TCP	unknown	dhcp-37.qualys.com	03/06/2011		
unknown	7997	TCP	unknown	dhcp-37.qualys.com	03/06/2011		
http	8500	TCP	unknown	dhcp-37.qualys.com	03/06/2011		
unknown	4000	UDP	Terabase	dhcp-37.qualys.com	03/06/2011		
http	8983	TCP	unknown	dhcp-37.qualys.com	03/06/2011		
unknown	49288	TCP	unknown	dhcp-37.qualys.com	03/06/2011	<input checked="" type="checkbox"/> Unauthorized	Irina Rockster 03/08/2011 Classifying as Unauthorized.

## **Classifying Services as Authorized or Unauthorized**

When a service is initially detected, it is classified as Unreviewed. Review each detected service and then classify the service as Authorized or Unauthorized. When you change the classification, you'll be prompted to provide a comment explaining how the service, protocol and port is necessary for your business.

To classify one or more services as "Authorized", select the check box next to each service you want to include in the action and then select Classify as—>Authorized. Similarly, to classify one or more services as "Unauthorized", select the check box next to each service you want to include in the action and then select Classify as—>Unauthorized.

You can also quickly change the classification for a single service from Authorized to Unauthorized and vice versa. Select the current classification in the Classification column and then select the new classification from the drop-down menu that appears.

The change in the classification is logged with the name of the user who made the change, the date of the change, and comments entered by the user at the time of the change. Note that changing the classification of a service does not affect your PCI compliance status.

## **Downloading a PDF or CSV Report**

Once you have reviewed all the detected services and classified them appropriately, you can generate and download a PDF or CSV report for auditing purposes. To do so, select Download—>PDF Report or Download—>CSV Report.

The report includes a summary with the total number of scanned hosts, the total number of services detected, and the number of services classified as Unreviewed, Unauthorized and Authorized. Following the summary is a complete list of all detected services grouped by classification and then by IP address. For each IP address, the following information appears: a list of services detected on the host with the port and protocol, the date when the service was last detected on the host, and the last user-provided comment.

## **View Compliance Status**

The Compliance Status section provides the current PCI compliance status for your network and its hosts. To view compliance status, go to Compliance—>Compliance Status on the left menu. When the overall compliance status is Compliant, you are ready to generate network reports.

See "Network Compliance and Reports" for information on your compliance status, generating network reports and submitting reports for PCI certification.



# Network Compliance and Reports

The Compliance section provides the current PCI compliance status for your network and its hosts. When the overall compliance status is Compliant, then you are ready to generate network reports for PCI certification.

## Network Reports Workflow

**Before You Begin:** Make sure you've already completed the "Network Scan Workflow" described in the previous chapter.

Step 1: View Compliance Status

Step 2: Use Wizard to Generate Network Reports

Step 3: View Your Network Reports

Step 4: Request ASV Review of Network Reports

Step 5: Submit Network Reports

## View Compliance Status

Your network scan compliance status appears on the Home page. You can view full compliance details on the Compliance Status page (Compliance—>Compliance Status) as shown below.

The screenshot displays the QualysGuard PCI Compliance Status page. The page header includes the QualysGuard PCI logo and the ONDEMAND SECURITY logo. The main content area is titled "Compliance Status" and features a summary table with columns for Overall Status, Hosts, Vulnerabilities, Potential Vulnerabilities, and Actions. The Overall Status is "Compliant" (indicated by a green checkmark). The Hosts table lists three hosts with their IP addresses, hostnames, operating systems, and compliance levels. A "Generate" button is present in the Actions column.

Overall Status	Hosts	Vulnerabilities	Potential Vulnerabilities	Actions
	In Account: 4 Not Live: 1 Compliant: 1 Not Compliant: 2 Not Current: <a href="#">[+]</a> 0	3 3 5	0 1 1	 <a href="#">Generate</a>

Details	IP	Hostname	Operating System	Compliance	Vulnerabilities	Scan Date
<input type="checkbox"/>	<a href="#">10.10.10.37</a>	dhcp-37.qualys.com	MacOS X		6	03/08/2011
<input type="checkbox"/>	<a href="#">10.10.24.134</a>	2k3r2-sp1-32bit	Windows 2003 R2 Service Pack 1		5	03/08/2011
<input type="checkbox"/>	<a href="#">10.10.24.183</a>		FreeBSD		2	03/08/2011

Please select an item in the list to view details.

## Overall Status

Identifies whether the network is compliant with the PCI Data Security Standard. The network consists of all the IP addresses in your account. A check mark (✔) indicates that the network is Compliant. A dash (⊖) indicates that the network is Not Compliant.

## Hosts

Host status indicators provide information about the hosts in your account.

**In Account** — The total number of hosts in your account.

**Not Live** — The total number of hosts in your account that were not found to be alive during scan processing. These IPs were specified as target IPs for scans that were launched in your account. The service was not able to find the host during host discovery, the first phase of the scan. Check to be sure that your hosts are properly connected to your network and have Internet access.

Hosts that are not live will not cause you to fail PCI compliance. Note, however, these hosts will be identified in the PCI network reports that you submit to your acquiring banks to demonstrate compliance, since the PCI compliance service could not determine whether these hosts passed PCI compliance requirements.

**Compliant** — The total number of hosts in your account that are Compliant with PCI security standards.

**Not Compliant** — The total number of hosts in your account that are Not Compliant with PCI security standards.

**Not Current** — Total number of hosts in your account that are Not Current. A host in your account is considered Not Current if it was scanned more than 30 days ago or has never been scanned. The PCI compliance service defines the best practice scanning period to be 30 days prior to today. In order for a host to receive Compliant status you must scan the host during the best practice scanning period and there can be no PCI vulnerabilities found for that scan.

## Vulnerabilities and Potential Vulnerabilities

The total number of current vulnerabilities and potential vulnerabilities, at each PCI severity level, that have been detected on the network. These include vulnerabilities that failed PCI compliance and must be fixed, as well as vulnerabilities that we recommend you fix. See “PCI Severity Levels” for a description of each severity level.

## Actions

Click the Generate button to generate PCI network reports based on the current vulnerability data for your network. See “Use Wizard to Generate Network Reports.”

## Compliance Status for each Host

All live hosts are displayed by default. For each host, the service lists host information (IP address, hostname, operating system, etc) and the host compliance status, which indicates whether the host is compliant with PCI compliance standards.

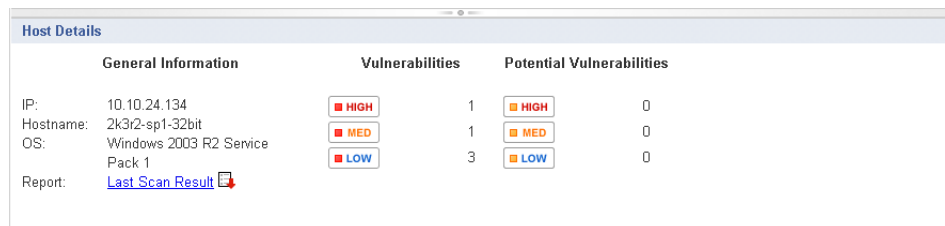
**Compliance** — A check mark (✔) indicates that the host is Compliant. No vulnerabilities, which must be fixed to pass PCI compliance, were found on the host. A dash (⊖) indicates that the host is Not Compliant. One or more vulnerabilities, which must be fixed to pass PCI compliance, were found on the host.

**Vulnerabilities** — The total number of current vulnerabilities and potential vulnerabilities that have been detected on the host. These include vulnerabilities that failed PCI compliance and must be fixed, as well as vulnerabilities that we recommend that you fix.

**Scan Date** — The start date of the most recent scan. Place your cursor over the date to see also see the start time.

### Host Details

Click on any IP address in the list to display host details in the preview pane, including a link to the last Scan Results Report for the host and the current number of vulnerabilities and potential vulnerabilities on the host.



General Information		Vulnerabilities	Potential Vulnerabilities
IP:	10.10.24.134	<span>HIGH</span> 1	<span>HIGH</span> 0
Hostname:	2k3r2-sp1-32bit	<span>MED</span> 1	<span>MED</span> 0
OS:	Windows 2003 R2 Service Pack 1	<span>LOW</span> 3	<span>LOW</span> 0
Report:	<a href="#">Last Scan Result</a>		

### Select Hosts to Display

All live hosts are displayed by default. Click one of these buttons to display certain hosts:

**All Live Hosts** — Click to display all hosts that were found to be alive (up and running, and connected to the Internet) when they were last scanned.

**Hosts not Live** — Click to display hosts that were not found alive when they were last scanned. When you display hosts that are not live, you have the option to launch a scan on those hosts by clicking the Scan Now button.

**Hosts not Current** — Click to display hosts that are not current. A host in your account is considered Not Current if it was scanned more than 30 days ago or has never been scanned. When you display hosts that are not current, you have the option to launch a scan on those hosts by clicking the Scan Now button. You can also remove those hosts by clicking the Remove Hosts button.

### Take Actions on Hosts

When you display all live hosts, an actions bar appears above the list enabling you to perform actions on one or more hosts in the list. Select hosts using the check boxes (in the far left column), and then select an action. If no hosts are selected in the list, then the action applies to all hosts.

**Scan** — Click to start a new network scan.

**View Vulnerabilities** — Click to view the Current Vulnerabilities list.

**Download Report** — Click to download the Current Vulnerabilities Report in PDF format.

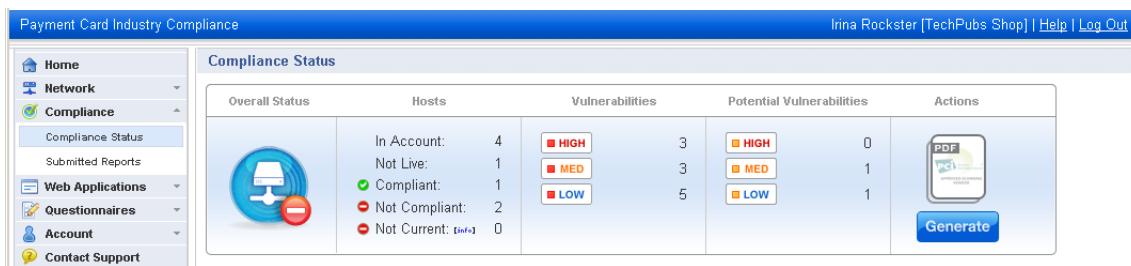
The Current Vulnerabilities Report displays all current vulnerabilities detected by the most recent network scans on the selected hosts. All vulnerabilities and potential vulnerabilities with a PCI status of FAIL must be fixed to pass the PCI compliance requirements.

## Use Wizard to Generate Network Reports

The service provides these network reports: PCI Executive Report and PCI Technical Report. The network reports include current vulnerability data returned from the most recent scans on your network, including all IP addresses in your account.

Once all vulnerabilities have been fixed and verified by another scan, then you are ready to generate PCI network reports. The service provides a Report Generation Wizard to assist you in generating your network reports and completing all PCI reporting requirements specified by the PCI Council. The wizard will guide you through the report generation process including reviewing scan findings and performing the required attestation.

To generate network reports, go to Compliance—>Compliance Status on the left menu and then click the Generate button (in the upper right corner of the page).



The Report Generation Wizard appears. For each step in the wizard, provide the information requested and click Next to go to the next screen.

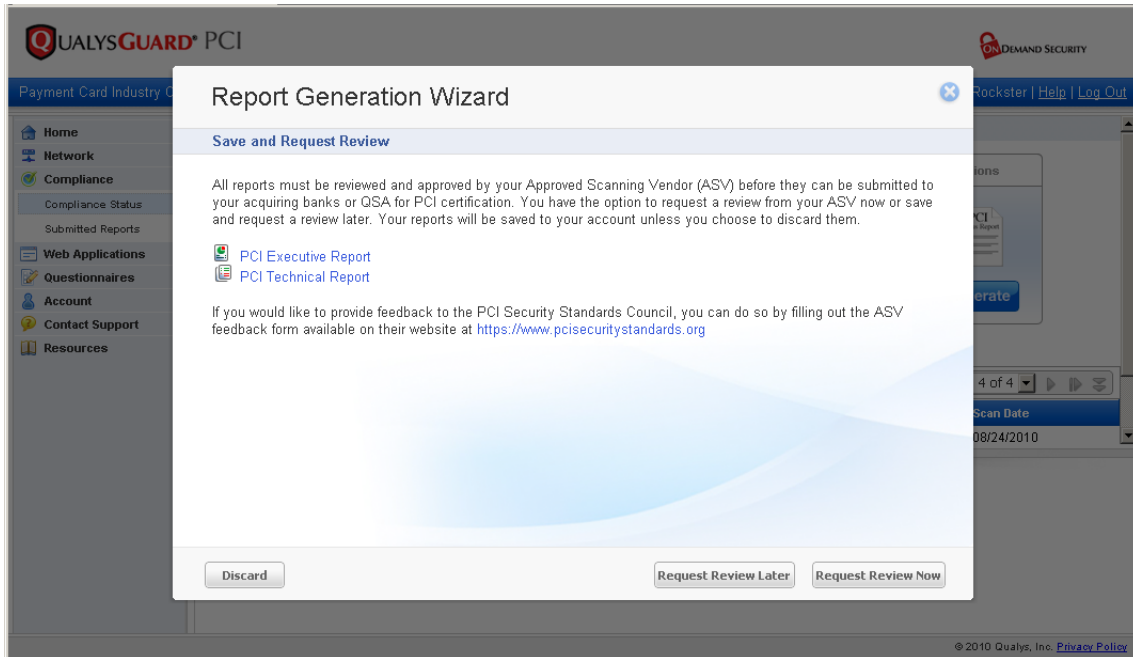


On the Summary page (the last page in the wizard), enter a submission title for the report for easy identification. Then click Generate Report to generate the PCI Executive Report and the PCI Technical Report.

## Network Compliance and Reports

### View Your Network Reports

Note: If you close the wizard or your browser, the reports will continue running in the background. You can view the status of your reports in progress from the Submitted Reports list (Compliance—>Submitted Reports).



A message appears when report generation is complete. Click Next and then select from these options:

**View Your Reports** — Click the PCI Executive Report link or the PCI Technical Report link to view the report online in PDF format.

**Request Review Later** — Click to exit the wizard without sending your reports to the ASV for review. Your reports are saved automatically on the Submitted Reports list with the report status Generated. You can request an ASV review at a later time from the Submitted Reports list.

**Request Review Now** — Click to immediately send the reports to your ASV for review. The ASV is notified of your request and the report status appears as Pending Review on the Submitted Reports list. You will be notified by email when the review is complete.



**Discard** — Click to exit the workflow without saving your reports.

## View Your Network Reports

You'll notice that there are two PCI network reports generated: PCI Executive Report and PCI Technical Report. These reports provide similar information suitable for different workflows. The PCI Executive Report provides summary level information only. The PCI Technical Report includes a Detailed Results section with technical details about detected vulnerabilities to assist you with remediation. Both reports must be submitted to your Approved Scanning Vendor for review and approval. Then once attested (approved) by the ASV, your report can be downloaded and sent to your acquiring banks or QSA for PCI certification.

**Sample PCI Executive Report**

The first page of the report includes the “Attestation of Scan Compliance” with an overall summary that shows whether your infrastructure received a passing scan and met the scan validation requirement.

### ASV Scan Report Attestation of Scan Compliance

Scan Customer Information				Approved Scanning Vendor Information			
Company:	Rockster Corp			Company:	Qualys		
Contact:	Irina Rockster	Title:	Security Consultant	Contact:	Patrick Slimmer	Title:	Technical Support Engineer
Telephone:	650 801 6100	Email:	ttrujillo@qualys.com	Telephone:	650 801 6100	Email:	pslimmer@qualys.com
Business Address:	1600 Bridge Parkway,			Business Address:	1600 Bridge Parkway, Suite 101		
City:	Redwood Shores	State/Province:	California	City:	Redwood Shores	State/Province:	California
ZIP:	94065	URL:		ZIP:	94065	URL:	http://www.qualys.com

---

**Scan Status**

- \* Compliance Status : PASS
- \* Number of unique components scanned: 2
- \* Number of identified failing vulnerabilities: 0
- \* Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 1
- \* Date scan completed: 08/27/2010
- \* Scan expiration date (90 days from date scan completed): 11/25/2010

---

**Scan Customer Attestation**

Rockster Corp attests on 2010-08-29 19:54:00 that this scan includes all components\* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. Rockster Corp also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicated whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

---

**ASV Attestation**

This scan and report was prepared and conducted by Qualys under certificate number 3728-01-05, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

Qualys, Inc. attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by Patrick Slimmer

---

The second page of the report is the “Executive Summary” with a list of the IP addresses that were scanned and the PASS or FAIL compliance status for each IP. This section also includes a list of the vulnerabilities noted for each IP address.

ASV Scan Report Executive Summary					
<b>Part 1. Scan Information</b>					
Scan Customer Company:	Rockster Corp	ASV Company:	Qualys		
Date scan was completed:	08/27/2010	Scan expiration date:	11/25/2010		
<b>Part 2. Component Compliance Summary</b>					
IP Address: 10.10.10.37					<b>PASS</b>
IP Address: 10.10.24.183					<b>PASS</b>
<b>Part 2. Component Compliance Summary - (Hosts Not Current)</b>					
<b>Part 3a. Vulnerabilities Noted for each IP Address</b>					
IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls
10.10.24.183	82054 - TCP Sequence Number Approximation Based Denial of Service_CVE-2004-0230	<b>MED</b>	5	<b>PASS</b>	
10.10.24.183	82003 - ICMP Timestamp Request CVE-1999-0524	<b>LOW</b>	0	<b>PASS</b>	
Consolidated Solution/Correction Plan for 10.10.10.37		-			
<b>Part 3b. Special Notes by IP Address</b>					
IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software	
-	-	-	-	-	

The PCI Executive Report and the PCI Technical Report include the sections above as well as these sections: Report Summary, Summary of Vulnerabilities and Appendices.

The PCI Technical Report also includes a Detailed Results section listing all detected vulnerabilities, potential vulnerabilities and information gathered for each scanned host.

See “PCI Report Details” in the online help for complete information for both reports.

## Submitted Reports List

To view the Submitted Reports list, go to Compliance—>Submitted Reports on the left menu. All PCI network reports generated in your account are saved automatically on the Submitted Reports list. From this list you can view report status and take action on generated reports like requesting an ASV review and submitting attested reports to your acquiring banks.

Details	Executive	Technical	Status	Next Action	Title	Date	Compliance
			Attested	<a href="#">Submit</a>	PCI Network Reports - Jan 2011	01/21/2011	PASS
			Generated	<a href="#">Request Review</a>		11/30/2010	FAIL

The Submitted Reports list provides these options:

**Details** — Click to view compliance details for the report and report status information. If the report was submitted to acquiring banks using the current version of the PCI web application, then a list of banks with access to the report is also shown.

**Executive / Technical** — Click to download the PCI Executive Report or click to download the PCI Technical Report.

**Status** — The current status of the PCI network report:

- Report Generating. Report generation is in progress.
- Generated. The report was generated and saved to your account.
- Pending Review. The report was sent to your ASV for review and the review is pending.
- Attested. The report was reviewed and attested by your ASV. You can now download this report and mail it to your acquiring banks for PCI certification.
- Rejected. The report was reviewed and rejected by your ASV. Work with your ASV to resolve open issues and then request another review.
- Submitted. (Only applicable if you have banks defined in your account.) The report was submitted to your acquiring banks through the web application.

Next Action — Your next action based on the current status of the PCI network report:

- Request Review. Select this link to request a review of the report from your ASV.
- Resubmit for Review. Select this link to request another ASV review of the report.
- Submit. (Only applicable if you have banks defined in your account.) Select this link to make your report available to your acquiring banks through the web application.

Title — The user-defined report submission title, if provided during report generation.

Date — The date when the PCI network reports were generated. Place your cursor over the date to see the time.

Compliance — Identifies whether the reports are compliant with the PCI requirements.

**PASS** indicates that the report is Compliant. No vulnerabilities, which must be fixed to pass PCI compliance, were found on your network. **FAIL** indicates that the report is Not Compliant. One or more vulnerabilities, which must be fixed to pass PCI compliance, were found on your network.

## Request ASV Review of Network Reports

All PCI network reports must be reviewed and attested by your Approved Scanning Vendor (ASV) before they can be submitted to your acquiring banks or QSA for PCI certification.

You can request a review of your network reports from within the report generation wizard or from the Submitted Reports list (see below).

### Request review of network reports:

- 1 Go to Compliance—>Submitted Reports on the left menu.
- 2 Identify the reports you want to send to the ASV for review and click the Request Review link in the Next Action column.
- 3 In the window that appears, click the Request Review Now button to confirm the action.

The ASV is notified of your request for review and the status changes to Pending Review in the Status column on the Submitted Reports list. You are notified by email once the review is complete.

### Attested:

Once the ASV has attested (approved) the report, then the report status changes to Attested. At this point, you can download the network report and send it to your acquiring banks for PCI certification. The Last Submitted date on the Home page for Your Network Scan reflects the report generation date of your last ASV attested report. The Next Due date is 90 days from the last submitted date.

If you have banks defined in your account, then a Submit link appears in the Next Action column allowing you to submit the report to your banks through the web application. See “Submit Network Reports.”

**Rejected:**

If the ASV rejects the report, then the report status changes to Rejected. Work directly with the ASV to resolve open issues and then request another review by clicking the Resubmit for Review link in the Next Action column. Repeat this process until the report is attested by the ASV.

## **Submit Network Reports**

Note: This procedure only applies if you have banks defined in your account.

Once your PCI network reports have been reviewed and attested by the ASV (Approved Scanning Vendor), you are ready to submit them to your acquiring banks for PCI certification. You submit reports to your banks from the Submitted Reports list. The banks defined in your account can then log into the PCI compliance service to view the PCI network reports that you have submitted. Note that your banks do not have online access to reports that have not been submitted.

**Submit network reports:**

- 1** Go to Compliance—>Submitted Reports on the left menu.
- 2** Identify the report you want to submit to your acquiring banks and click the Submit link in the Next Action column. (Note this link only appears for reports with a status of Attested.)

A confirmation window appears listing the banks defined for your account.

- 3** Click Submit in the confirmation window to confirm the action and submit your report to your acquiring banks.



# Web Application Scan

The PCI compliance service provides Web Application Scanning (WAS) to assist customers with meeting PCI DSS Requirement 6.6, which deals with security of web applications. The requirement calls for securing web applications using a variety of options. Until June 30, 2008 this was a best practice but has been made a requirement since that date.

The PCI Council published a clarification document on the topic of Requirement 6.6 in April 2008 titled *PCI DSS: Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified*. This document is published at the PCI Security Standards Council's web site at:

[https://www.pcisecuritystandards.org/security\\_standards/documents.php](https://www.pcisecuritystandards.org/security_standards/documents.php)

The PCI compliance service provides an automated WAS module that allows users to crawl web applications, detect cross-site scripting and SQL injection vulnerabilities, and conduct authenticated and non-authenticated scanning to capture the perspective of both authorized and unauthorized users. The WAS solution automates the techniques used to identify most web vulnerabilities such as those in the OWASP Top 10 and WASC-TC, including SQL Injection and Cross-Site Scripting. The WAS module combines pattern recognition and observed behaviors to accurately identify and verify vulnerabilities.

Web application scanning is available in your account only when the Web Application Scanning (WAS) module is enabled for your subscription. The WAS module may be enabled for a trial period. If you would like to enable this feature, please contact Technical Support.

## Web Application Scan Workflow

Step 1: Add Web Application to Your Account

Step 2: Start New Web Application Scan

Step 3: View Web Application Scan Results

## Add Web Application to Your Account

You have the ability to add web applications to your account up to the maximum number of applications permitted in your account settings. Other users in the same subscription have the same privilege. Note your account manager cannot add applications to your account. (To remove a web application, please submit a request to Technical Support.)

It is your responsibility to ensure that you are providing all of your applications for scanning.

The maximum number of web applications you can add to your account is equal to the number of applications purchased for your subscription. To view the total applications purchased, go to Account—>Settings on the left menu.

To add a new web application to your account:

- 1 Go to Account—>Web Applications on the left menu. When there are no applications in your account, the Web Applications list is empty as shown below.
- 2 Click the New link above the Web Applications list. The New Web Application page appears.

Note: When you add a web application, the service does not verify whether the web application you've entered is accessible from the Internet. This occurs after you've launched a scan. Only web applications that are accessible from the Internet are scanned by the service.

The screenshot shows the 'New Web Application' page in the QualysGuard PCI interface. The page has a blue header with the QualysGuard PCI logo and the text 'Payment Card Industry Compliance'. On the right side of the header, there is a 'DEMAND SECURITY' logo and the user name 'Irina Rockster' with links for 'Help' and 'Log Out'. The main content area is titled 'New Web Application' and contains a form for 'Web Application Details'. The form has four fields: '\* Title' with the value 'phpBB Application', '\* Site' with the value '10.10.25.16', '\* Port' with the value '80', and '\* Starting URI' with the value '/'. Below the form is a yellow message box that says 'You must save the new web application before you can add authentication records. Edit the web application to add records.' and two buttons: 'Save' and 'Cancel'. At the bottom right of the page, there is a copyright notice: '© 2010 Qualys, Inc. Privacy Policy'.

## Web Application Details

**Title** — A user-defined title for the web application.

**Site** — The starting host from which to start web crawling. Enter an IP address or host name (FQDN) to start web crawling under. The web application can consist of a single physical host or multiple identical hosts behind a single load-balanced IP address. The Port field allows you to limit the web crawling to a specific port number. The Starting URI field allows you to limit the crawling to a specific path.

The protocol may be entered with the starting site, either “https://” or “http://”. If entered, the service automatically removes the protocol when the web application is saved.

**Port** — The port number from which to start web crawling.

**Starting URI** — The starting path from which to start web crawling. By default the crawling starts at the web application root directory. To start web crawling from a subdirectory, enter the path to the starting directory starting with “/”. For example: /services/app1

## **Web Application Scan**

Add Web Application to Your Account

**Blacklist** — Important! Automated web application scanning has the potential of causing data loss. Use this feature to avoid data loss.

For a production web application, it's best practice to blacklist pages with certain functionality that if executed would have undesirable results, such as possibly sending out too many emails, potentially submitting a "delete all" button, or disabling/deleting accounts.

This feature prevents the web crawler from making requests for certain links in your web application. The blacklist consists of one or more strings identifying links in the web application that should not be visited. For each string specified, the crawler performs a string match against each link it encounters. When a match is found, the crawler does not submit a request for the link.

Click the Blacklist link and enter a list of URLs in the field provided. A maximum of 100 URLs may be entered.

Enter each URL on a separate line (separated by a return character). The URL is interpreted as a regular expression. Therefore, a question mark that is used as a query string delimiter (for example `/page.cgi?a=1`) should be escaped with a back slash (for example `/page.cgi\?a=1`). Use `.*` (dot asterisk) for wildcards.

The web crawler automatically follows links it encounters in forms. To do this, the web crawler makes requests to the web server just like the web application makes itself when users take certain actions. For example, when a crawler encounters a button in a form, the crawler submits a request for the button URI to the web server. This action made by the web crawler could cause an undesirable effect. For example, if the button is designed to "delete all" data, like accounts, configurations, etc. then all data would be deleted. In an administrator web application, an administrator may click a button to change the authentication type for the subscription account, changing the authentication behavior for all users of the web application.


## **Save Application**

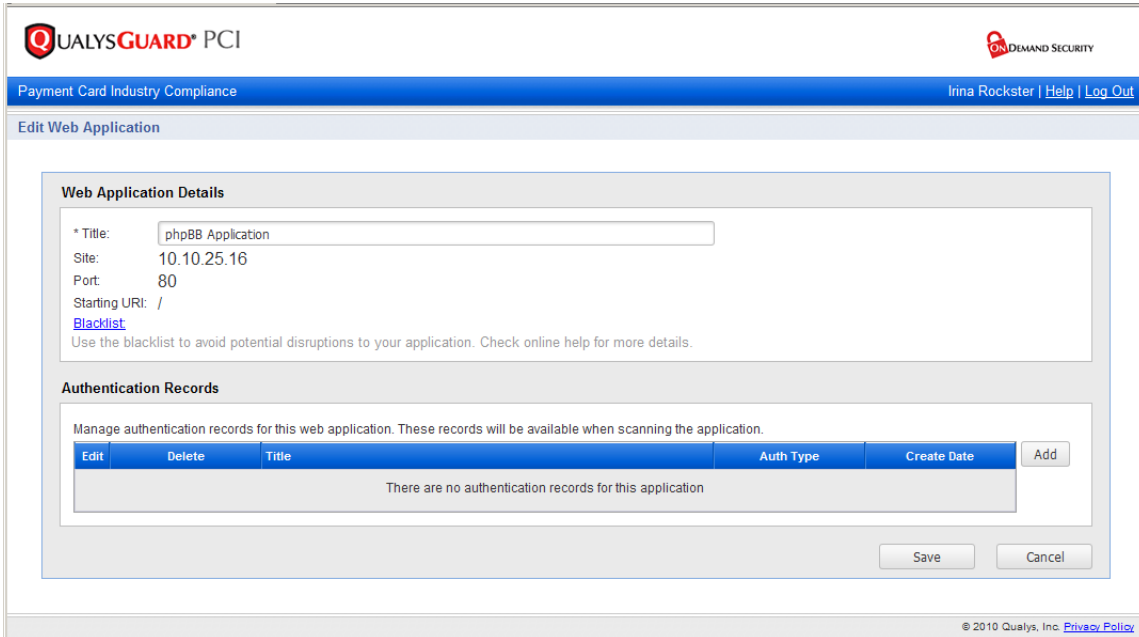
Click Save to save the web application to your Web Applications list.

## Add Authentication Records to Web Application

One or more authentication records may be added to a web application when authentication is desired. Each record includes credentials (user name and password) to be used for authentication when the web crawler encounters a login form.

You add authentication records to a web application that's already in your Web Applications list. Note: You must first create a web application before adding authentication records to it.

To add an authentication record, go to Account—>Web Applications. Identify the application you want to add the record to, and click . The Edit Web Application page appears. When there are no records defined, this list is empty as shown below.



QUALYS GUARD<sup>®</sup> PCI DEMAND SECURITY

Payment Card Industry Compliance Irina Rockster | [Help](#) | [Log Out](#)

### Edit Web Application

**Web Application Details**

\* Title:   
Site: 10.10.25.16  
Port: 80  
Starting URI: /  
[Blacklist](#)  
Use the blacklist to avoid potential disruptions to your application. Check online help for more details.

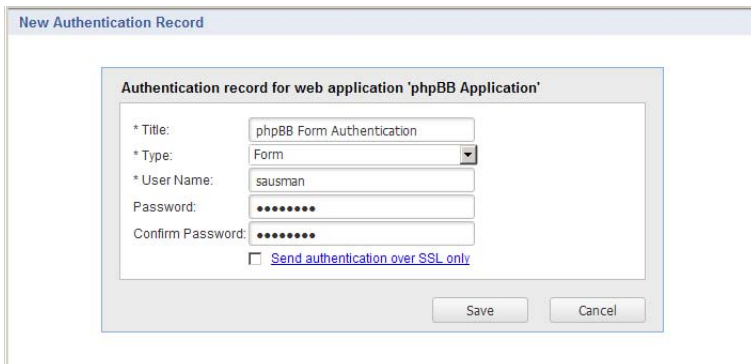
**Authentication Records**

Manage authentication records for this web application. These records will be available when scanning the application.

Edit	Delete	Title	Auth Type	Create Date	Add
There are no authentication records for this application					

© 2010 Qualys, Inc. [Privacy Policy](#)

To add a new record, click the Add button to the right of the Authentication Records list area.



New Authentication Record

**Authentication record for web application 'phpBB Application'**

\* Title:   
\* Type:   
\* User Name:   
Password:   
Confirm Password:   
 [Send authentication over SSL only](#)

## Web Application Scan

Add Authentication Records to Web Application

### Authentication Record Details

Title — A user-defined title for the authentication record.

Authentication Type — Select one of these options:

- Form
- Server: HTTP Basic

Two-factor authentication and one-time authentication are not supported at this time, but a workaround may be possible using header injection to replay session cookies. See the Header Injection scan setting described in the next section “Start New Web Application Scan.”

SSL option — Select “Send authentication over SSL only” if you want the service to attempt authentication only when the form being authenticated to will be sent over SSL. When selected, authentication is attempted only when the form is submitted via a link that uses SSL (link URI <https://...>).

User Name/Password — Credentials to be used for authentication in an authentication record. Users may wish to scan the same web application with different credentials. For example, it may be necessary to distinguish scans that were executed with different credentials. To do this, you can define multiple records and provide an authentication record title for each with information related to the privilege level like “Anonymous”, “User”, “Admin”. For example a “User” record may find 300 links and 10 vulnerabilities, whereas an “Anonymous” record may find only 100 links and no vulnerabilities.

Realm — For authentication type Server: HTTP Basic, enter the name of a protected realm. When specified, authentication is attempted only to the protected realm.

### Save Authentication Record

Click Save to save the authentication record. The new record will appear in the Authentication Records list for the web application you are editing.

The screenshot displays the 'Edit Web Application' interface in the QALYS GUARD PCI application. The top navigation bar includes the QALYS GUARD PCI logo and 'Payment Card Industry Compliance'. The user 'Irina Rockster' is logged in, with 'Help' and 'Log Out' links. The main content area is titled 'Edit Web Application' and contains two sections: 'Web Application Details' and 'Authentication Records'. The 'Web Application Details' section has a form with the following fields: Title (phpBB Application), Site (10.10.25.16), Port (80), and Starting URI (/). A 'Blacklist' link is present below the Starting URI field. The 'Authentication Records' section features a table with columns for Edit, Delete, Title, Auth Type, Create Date, and an Add button. Two records are listed: 'phpBB HTML Basic Authentication' and 'phpBB Form Authentication', both using 'Form' authentication type and created on 08/24/2010. A 'Save' button is located at the bottom right of the table area.

Edit	Delete	Title	Auth Type	Create Date	Add
		phpBB HTML Basic Authentication	Form	08/24/2010	
		phpBB Form Authentication	Form	08/24/2010	

## Start New Web Application Scan

The web crawler crawls a web application under a single host name or IP address as defined in the web application settings. The web application can consist of a single physical host or multiple identical hosts behind a single load-balanced IP address. It's possible to launch a web application scan on a target application if a scan is not already running on the same application.

To start a web application scan, go to Web Applications—>New Scan on the left menu. The New Web Application Scan page appears.

The screenshot shows the 'New Web Application Scan' dialog box. At the top, it displays the QualysGuard PCI logo and 'ON DEMAND SECURITY'. Below the header, there's a blue bar with 'Payment Card Industry Compliance' and user information 'Irina Rockster | Help | Log Out'. The main title is 'New Web Application Scan'. The 'Scan Settings' section includes: '\* Title: My Web Application Scan'; '\* Application: Demo Web Application (with a '+New' link); 'Authentication Record: Demo App - Form Authentication'; '\* Form Submission: Disallow Forms'; 'Maximum links to crawl: 300'; 'Bandwidth: Medium (with an 'Info' link)'; and two unchecked checkboxes: 'Limit crawling to starting URI' and 'Crawl Only (do not conduct web vulnerability tests)'. There is a link for 'Advanced Options'. The 'Scan Date' section has 'Launch Now' selected and 'Schedule for Later' as an option. At the bottom right are 'OK' and 'Cancel' buttons. The footer contains '© 2010 Qualys, Inc. Privacy Policy'.

### Scan Settings

**Title** — A user-defined scan title.

**Application** — Select the web application that you want to scan. The web crawler crawls a web application under a single host name or IP address, as defined in the application settings.

**Authentication Record** — Select an authentication record to apply to the scan if authentication is desired. By default, no authentication record is selected.

**Form Submission** — Select the method to be used by the web crawler to submit requests to forms. The web crawler follows links to form actions that it encounters when the form method attribute, as defined in each target form, matches the Form Submission setting you select.

Select one of these Form Submission options:

- **Disallow Forms (default)** — No requests to forms will be submitted unless application authentication is requested, in which case only the login form will be tested.
- **GET & POST** — The web crawler submits requests to all forms. When authentication is desired, this option is recommended best practice to ensure maximum vulnerability analysis and the most comprehensive scan results.

## Web Application Scan

Start New Web Application Scan

- GET Only — Limits web crawling to GET forms.
- POST Only — Limits web crawling to POST forms.

Maximum links to crawl — The maximum number of links to crawl during the scan. Default is 300. Maximum is 5,000.

Limit crawling to starting URI — Select this option to limit crawling to the starting URI defined for the web application. When selected, the web crawler follows links down the web site branch in the same directory as the starting URI. It will not follow links across the web site branch to pages parallel to the starting URI.

Bandwidth — Select a bandwidth level. It's recommended that you keep the default bandwidth level of Medium. Bandwidth options are High, Medium (the default), Low, and Lowest. Select the Info link for more information on the bandwidth levels.

Crawl Only (do not conduct web vulnerability tests) — Select this option to perform a web crawl without running vulnerability tests. We strongly recommend that you use the Crawl Only option for your first scan. This is a good way to understand where the scan will go and whether there are URIs you should blacklist.

Advanced Options— Click this link to enter a value for header injection. This may be desirable for complex authentication schemes (inject session cookie) or to impersonate a web browser.

Select one of these options: Launch Now or Schedule for Later (see “Scan Scheduler” below).

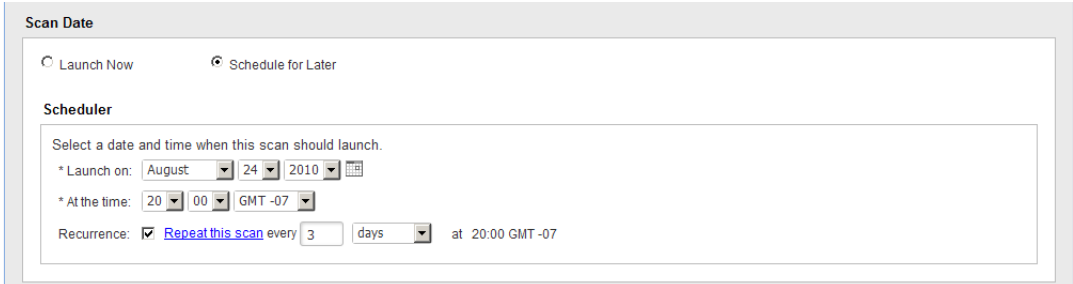
Click OK to save the scan. If you selected “Launch Now” the scan is started right away.

### Scan Summary Email

When the scan has finished, you will receive a Scan Summary email notification. Use the link in the email to log back into the PCI Merchant application to view the full scan results.

### Scan Scheduler

On the New Web Application Scan page, you have the option to schedule a one-time web application scan to start at a later time or schedule a recurring scan to run on a daily or weekly basis. To do so, select the “Schedule for Later” option. You will be prompted to provide the date and time when the scan should run. Optionally, set recurrence to repeat the scan.



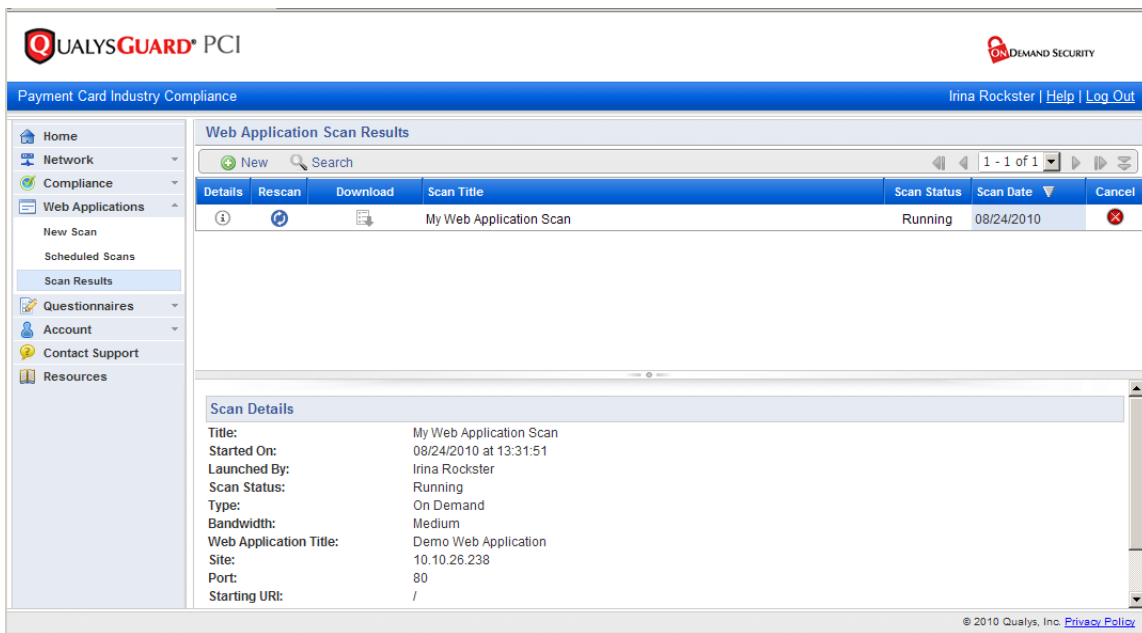
The screenshot shows a 'Scan Date' section with two radio buttons: 'Launch Now' (unselected) and 'Schedule for Later' (selected). Below this is a 'Scheduler' section with the instruction 'Select a date and time when this scan should launch.' It includes three rows of input fields: '\* Launch on:' with dropdowns for 'August', '24', and '2010'; '\* At the time:' with dropdowns for '20', '00', and 'GMT -07'; and 'Recurrence:' with a checked box, a link 'Repeat this scan', a text input '3', a dropdown 'days', and the text 'at 20:00 GMT -07'.

When the scan starts (at the time you've specified), then it will appear in the Scan Results section (Web Applications—>Scan Results) where you can view the scan status. As with scans launched immediately, you will receive a Scan Summary email notification when the scan completes.

## View Web Application Scan Results

Return to the Scan Results section at any time for the latest scan status for your web application scans. To do this, go to Web Applications—>Scan Results on the left menu. Your scans run in the background so you can exit the PCI application while scans are in progress.

The Web Application Scan Results section shows a complete history of your web application scans. Return to this section at any time for the latest scan status. To do this, go to Web Applications—>Scan Results on the left menu. Your scans run in the background so you can exit the PCI web application while scans are in progress.



### View Scan Information

**Details** — Click to view scan details for a scan task, including the scan title, when the scan was launched, the user who launched the scan, the scan status, whether the scan was launched on demand or scheduled, the target web application, user-defined scan settings.

**Download** — Click to download the Web Application Scan Results Report in PDF format for a completed scan. The detailed results section shows all detected web application vulnerabilities.

### Web Application Vulnerability Checks

The vulnerability checks (QIDs) performed by the scanning engine for a web application scan allow the user to examine web applications with an eye toward discovering common vulnerability types. WAS vulnerability checks are performed for web application scans only (not network scans). These include: Cross-site Scripting Vulnerabilities (Persistent, Reflected, Header, Browser-Specific) and SQL Injection Vulnerabilities (Regular and Blind).

Additional vulnerability checks identify information gathered about the web application during the scan process, such as the links crawled, the external links discovered, external form actions discovered, host information, and scan diagnostics.



# Self-Assessment Questionnaire

The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) is a validation tool to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS). Merchants are required to submit a PCI self-assessment questionnaire every 12 months.

The PCI compliance service supports SAQ v2.0 based on the PCI DSS v2.0 standard. The PCI Council requires that all assessments started after December 31, 2011 use version 2.0.

## Questionnaire Versions (A-D)

There are multiple PCI self-assessment questionnaire (SAQ) versions available (A, B, C, C-VT and D). You must select the appropriate questionnaire version for your organization to validate compliance with the PCI Data Security Standard.

The QualysGuard PCI provides an online SAQ wizard to help you select the questionnaire version that is appropriate for your organization. The SAQ wizard is based on the guidelines of the PCI Security Standards Council. These guidelines are available on the PCI Security Standards Council's web site at:

[https://www.pcisecuritystandards.org/merchants/self\\_assessment\\_form.php](https://www.pcisecuritystandards.org/merchants/self_assessment_form.php)

## Questionnaire Access Privileges

Your account may have questionnaire access privileges defined by your account manager. One or both of these privileges may be defined:

**Questionnaire Type Access** — Limits you to only one questionnaire type (A, B, C, etc). In this case, when you start a new questionnaire, the questionnaire type available for your account appears automatically.

**Questionnaire Only Access** — Limits you to questionnaire access privileges only. In this case, you have access to questionnaire functionality; access to other functionality like launching scans and submitting network reports is not permitted.

## Questionnaire Workflow

Step 1: Start New Questionnaire

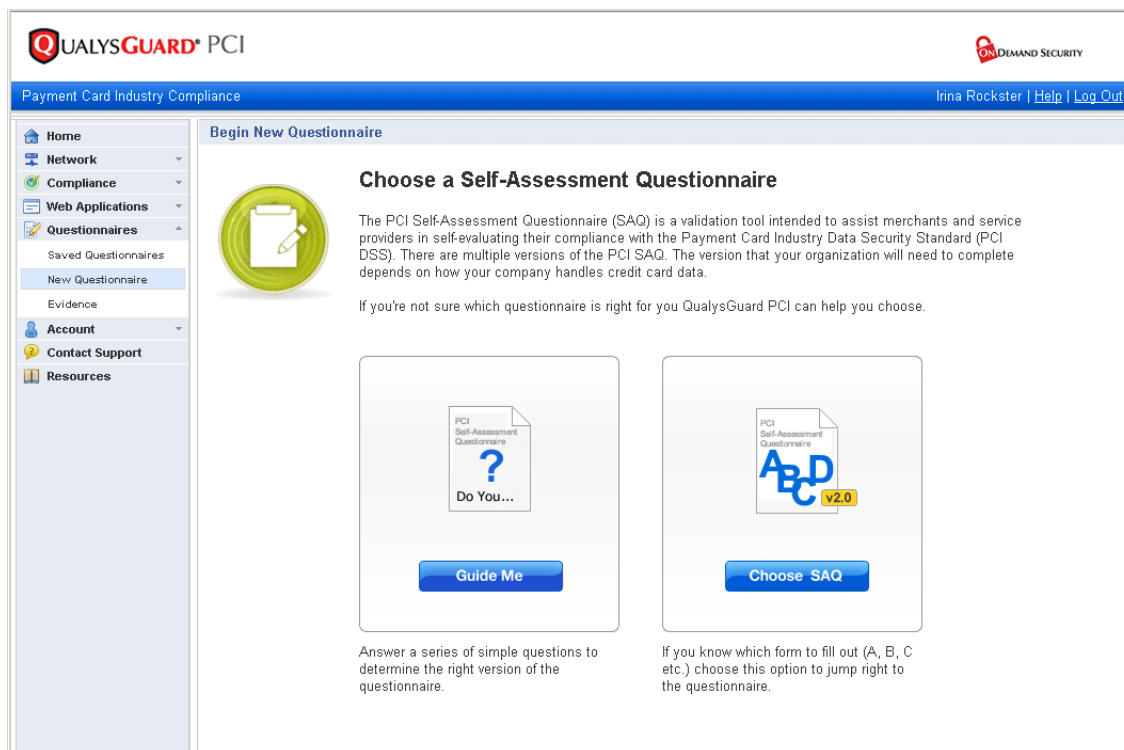
Step 2: Request Questionnaire Validation (if appropriate)

Step 3: Submit Your Questionnaire

## Start New Questionnaire

Go to Questionnaires—>New Questionnaire on the left menu. You will be prompted to select a questionnaire version. There are multiple versions of the PCI SAQ. The version appropriate for your organization depends on how your company handles credit card data.

Select **Guide Me** or **Choose SAQ**. If you select Guide Me, the PCI service asks you simple questions to determine the right version of the questionnaire.



The first page of the questionnaire is a cover page where you can provide a title and organization information.

### Title (Optional)

Enter a unique title for the questionnaire in the Questionnaire Title field. This title will appear on the cover page of your submitted questionnaire. The title is also shown on the Saved Questionnaires list for easy identification.

### Organization Information (Optional)

The text fields are pre-populated with organization information saved in your account settings, and the Contact Name displayed is the primary contact defined for your account.

You can make changes to the text fields and choose another user to be the contact person for the questionnaire. To overwrite account settings with your changes, select the check box “Update Account Information with changes made above” before saving the questionnaire. Your account settings are updated and the user selected in the Contact Name menu becomes the new primary contact.

## Filling Out the Questionnaire

To be compliant with the self-assessment portion of the PCI DSS, you must respond to all questions with “Yes” or “N/A” or “Compensating Controls”. If you respond to any question with “No”, the questionnaire is not considered compliant. The PCI Security Standards Council provides guidelines and instructions when requirements are deemed not applicable to your environment, and when using compensating controls. See “Responding with N/A or Compensating Controls” for more information.

The screenshot displays the QualysGuard PCI Self-Assessment Questionnaire D interface. The top navigation bar includes the QualysGuard PCI logo and the Demand Security logo. The main header shows the title "Payment Card Industry Self-Assessment Questionnaire D" and the date "08/24/2010". The left sidebar contains a "Table of Contents" with a list of requirements (Requirement 1 to Requirement 12) and their completion percentages. Below this is a "Prioritized Approach" section with checkboxes for Milestones 1 through 6. The main content area displays "Requirement 1: Install and maintain a firewall configuration to protect data" and lists three sub-questions (1.1.2, 1.1.3, and 1.1.5) with response options (Yes, No, N/A, Compensating Controls) and links for "More Information", "Comments", and "Evidence".

Questionnaire features (labeled 1-8) are described below.

### 1 Table of Contents

This section lists the requirements of the questionnaire based on the requirements outlined in the PCI DSS. The number of requirements in the questionnaire depends on the questionnaire version (A-D) you have selected to complete. Each requirement includes one or more questions. Click a requirement to display its questions. Note that the percent complete for each requirement is dynamically updated as you complete the questionnaire.

### 2 Prioritized Approach

You have the option to prioritize questions according to milestones. Questions are assigned color coded milestones based on compliance goals established by the PCI Security Standards Council. When your questionnaire is displayed, all milestones that apply to your questionnaire are selected. You can clear the check box for any milestone you don't want to address, and the questions matching that milestone will no longer appear.

As you complete the questionnaire, the compliance percentage for each milestone is dynamically updated, so you can easily track your compliance progress. Learn more about the prioritized approach at the PCI Security Standards Council's web site at:

[https://www.pcisecuritystandards.org/security\\_standards/prioritized.php](https://www.pcisecuritystandards.org/security_standards/prioritized.php)

### **3 More Information**

Select to view additional information for a specific question. This additional information may assist you when determining a response to a question.

### **4 Comments**

Select to enter notes explaining your response to a specific question. Comments are optional for any question with a "Yes" response. Comments are required for any question with a "No", "N/A" or "Compensating Controls" response. Your comments will appear in the submitted questionnaire. See "Compensating Controls."

### **5 Evidence**

Select to upload files to the questionnaire as evidence of compliance with a specific requirement or question. When you submit the questionnaire to your acquiring banks, you have the option to include the evidence files. Once a file is successfully uploaded, it is stored securely in the PCI application and made available to all users in the subscription. To see a complete list of uploaded evidence files, go to Questionnaires—>Evidence on the left menu. See "Evidence Files" for more information.

### **6 View a list of third party vendors**

This link appears below any question (or sub-question) where at least one third party vendor has been identified as having a product that can assist you in complying with the requirement. One or more vendors may be listed.

### **7 QualysGuard PCI Connect Recommendation**

This option appears next to each requirement/question that was included in an imported QualysGuard PCI Connect Summary Report (see 8 below). Click the link to see the vendor's recommendation and other details from the vendor's report.

### **8 Import QualysGuard PCI Connect XML**

When available, select to import a QualysGuard PCI Connect Summary Report (in XML format) to the questionnaire. Note that this option is available only to certain merchant accounts. QualysGuard PCI Connect Summary Reports are available to merchants from PCI solution vendors who support PCI Connect.

The QualysGuard PCI Connect Summary Report is a report provided to you by a PCI solution vendor who has performed their own assessment of your compliance with one or more requirements. For each requirement included in the report, the vendor provides a recommendation (Pass or Fail) and a summary of their assessment, including the number of assets analyzed, the number of assets that are not compliant, and a list of violations, if any. Once imported to the questionnaire, you can view the information in the vendor's report and use that information to determine the best response to each question.

## Save Questionnaire

When editing a questionnaire there are save options at the bottom of the questionnaire window.

**Save Draft** — Click at any time while completing the questionnaire to save the work you've done. When you're ready to proceed with the questionnaire, go to Questionnaires—>Saved Questionnaires on the left menu. See "Saved Questionnaires" below.

**Submit Final** — Click Submit Final to save the questionnaire and submit it to your acquiring banks. The Submit Questionnaire window appears, prompting you to review the questionnaire status and supply comments, if you wish, before submitting (see "Submit Your Questionnaire" to view a sample Submit Questionnaire window). The submit workflow saves the questionnaire on the Saved Questionnaires list where you can download the questionnaire in PDF format. When your account settings lists your acquiring banks, the final questionnaire is submitted automatically to your banks. When there is no acquiring bank in your account, then you need to download the PDF report and submit it manually.

**Request Validation** — This option only appears if the questionnaire validation feature is enabled for your account. Click Request Validation to submit the completed questionnaire to your QSA (Qualified Security Assessor) for approval. See "Request Questionnaire Validation" for more information.

## Responding with N/A or Compensating Controls

The PCI Security Standards Council provides guidelines when responding to questions with N/A (non-applicability and exclusions) or Compensating Controls. When you use these options, then you are required to provide specific information in the "Comments" field.

### Guidance for Non-Applicability and Exclusions

N/A may be selected in your questionnaire when a requirement is deemed not applicable to your environment or you are excluded from the requirement.

**Exclusions** — The PCI Council states that certain, specific exceptions may be considered when completing questionnaires C and D. Possible exceptions are outlined in the document *PCI DSS: Self-Assessment Questionnaire: Instructions and Guidelines Version 2.0* (dated October 2010), in the section "Guidance for Non-Applicability of Certain, Specific Requirements." This document is published on the PCI Security Standards Council's web site at:

[https://www.pcisecuritystandards.org/merchants/self\\_assessment\\_form.php](https://www.pcisecuritystandards.org/merchants/self_assessment_form.php)

**Non-Applicability** — When completing any of the questionnaires, if a requirement is deemed not applicable to your environment, select the response N/A. Then provide your explanation of non-applicability in the "Comments" field.

### Compensating Controls

Compensating Controls may be selected in your questionnaire when you cannot meet a requirement explicitly as stated. For a definition of Compensating Controls, refer to the document *PCI DSS and PA-DSS: Glossary of Terms, Abbreviations, and Acronyms Version 2.0* (dated October 2010). This document is published on the PCI Security Standards Council's web site at:

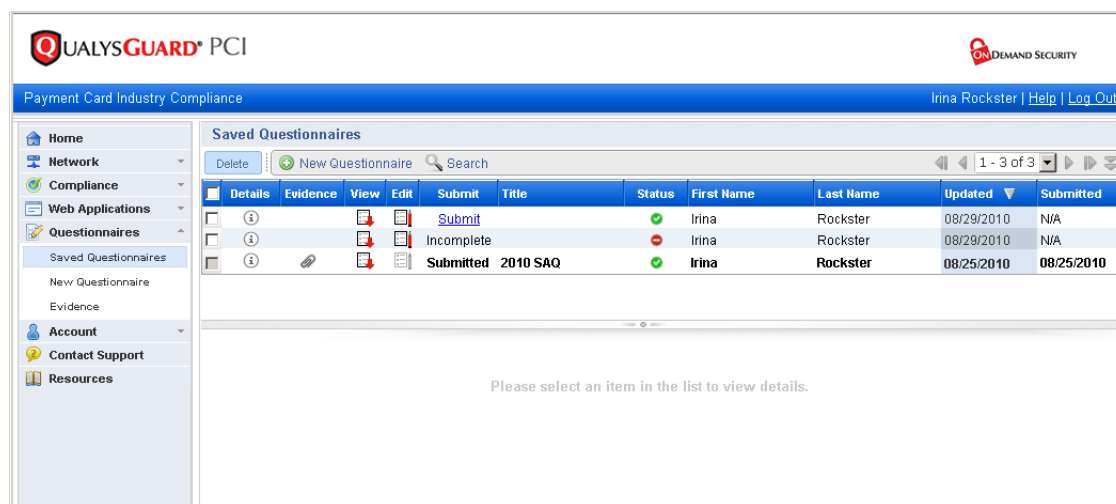
[https://www.pcisecuritystandards.org/security\\_standards/documents.php](https://www.pcisecuritystandards.org/security_standards/documents.php)

The PCI Council requires additional information when compensating controls are used. Enter additional information in the “Comments” field when you select “Compensating Controls” for a requirement. Refer to “Appendix C: Compensating Controls Worksheet” which is available in each of the questionnaires from the PCI Security Standards web site at:

[https://www.pcisecuritystandards.org/merchants/self\\_assessment\\_form.php](https://www.pcisecuritystandards.org/merchants/self_assessment_form.php)

## Saved Questionnaires

The service provides a complete list of questionnaires for your subscription, including draft questionnaires, completed questionnaires and submitted questionnaires. To view the list, go to Questionnaires—>Saved Questionnaires on the left menu. The Saved Questionnaires list is empty until you (or another user in your subscription) creates and saves a questionnaire. A sample Saved Questionnaires list is shown below.



The screenshot shows the QALYS GUARD PCI interface. The top navigation bar includes the logo, "Payment Card Industry Compliance", and the user name "Irina Rockster" with links for "Help" and "Log Out". A left-hand navigation menu lists various sections: Home, Network, Compliance, Web Applications, Questionnaires (with sub-items for Saved Questionnaires, New Questionnaire, Evidence, and Account), Contact Support, and Resources. The main content area is titled "Saved Questionnaires" and features a table with columns for Details, Evidence, View, Edit, Submit, Title, Status, First Name, Last Name, Updated, and Submitted. The table contains three rows: a "Submit" button, an "Incomplete" questionnaire by Irina Rockster (updated 08/29/2010), and a "Submitted 2010 SAQ" questionnaire by Irina Rockster (updated and submitted 08/25/2010). Below the table, a message reads "Please select an item in the list to view details."

## Manage questionnaires in the list

Select ⓘ next to any questionnaire to view questionnaire details in the preview pane. The option “Allow my acquiring banks to view evidence files” appears in the preview pane for submitted questionnaires. When selected, your banks have online access to the evidence files. When cleared, your banks do not have online access to the evidence files.

Click 📎 to view and download evidence files attached to the questionnaire, if applicable.

Click 📄 to download the questionnaire in PDF format.

Click 📝 to edit a questionnaire that has not yet been submitted.

## Evidence Files

Each subscription is allocated a certain amount of disk space for storing evidence files. Go to Account—>Settings on the left menu and scroll down to the Subscription Information section to view storage details for the subscription.

The service provides a complete list of all evidence files that have been uploaded by users in the subscription. To view the list, go to Questionnaires—>Evidence on the left menu. From this list, you can download evidence files and delete evidence files from the subscription.

Click ⓘ next to any file in the Evidence list to view file details in the preview pane.

## Request Questionnaire Validation

If the questionnaire validation feature is enabled for your account, then you have the option to request validation for each completed questionnaire. When you request validation, the questionnaire is submitted to a QSA (Qualified Security Assessor) for approval. The questionnaire must then be approved by the QSA before it can be submitted to acquiring banks.

### To request validation:

- 1 Go to Questionnaires—>Saved Questionnaires on the left menu.
- 2 Identify the completed questionnaire you want to have validated, and click the Request Validation link in the Submit column. (Note this link only appears when questionnaire validation is enabled for your account.)
- 3 Click Yes to confirm the action in the confirmation window that appears.

The QSA is notified of your request and the questionnaire status changes to Pending Validation on the Saved Questionnaires list. You are notified by email once the questionnaire is validated.

**Approved:** If the validation status is Approved, a Submit link appears in the Submit column on the Saved Questionnaires list so you can submit the approved questionnaire to your acquiring banks. See “Submit Your Questionnaire” below for information on the submit questionnaire workflow. (Note that you cannot edit a questionnaire that has already been approved.)

**Rejected:** If the validation status is Rejected, you should work directly with the QSA to make corrections to the questionnaire, and then request validation again. Repeat this process until the questionnaire is approved.

## Submit Your Questionnaire

Once all questions in a questionnaire have been answered, then you are ready to submit the questionnaire to your acquiring banks. You can submit the questionnaire when editing the questionnaire or when viewing the Saved Questionnaires list.

### To submit a questionnaire:

- 1 Go to Questionnaires—>Saved Questionnaires on the left menu.
- 2 Identify the questionnaire you want to submit and click the Submit link in the Submit column. The Submit Questionnaire page appears.
- 3 Review the questionnaire status on the screen, provide section comments, and review the list of banks in your account.
- 4 Click Submit.

The questionnaire is submitted to your banks, as defined in your account. (When there is no acquiring bank you must download and submit the PDF report manually.)