

GETTING STARTED WITH THE PCI COMPLIANCE SERVICE

VERSION 2.3

May 1, 2008



Copyright 2006-2008 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

Introducing the PCI Compliance Service.....	4
Your Home Page	6
PCI Scan Workflow	7
First Steps	10
Logging In	10
Change Your User Login & Password (Optional).....	11
Add Additional Users (Optional).....	12
Add IPs for Scanning.....	12
Check Access to Scanner IP Addresses.....	14
Your Account Settings.....	14
Getting Help While You Work.....	15
PCI Network Scans.....	16
Before You Begin.....	16
PCI Scan Process.....	16
Start a Network Scan	17
Schedule a Network Scan.....	18
View Scan Summary Email	19
View Scan Results	20
About Vulnerability Classification	21
Fix Vulnerabilities and Re-scan.....	22
PCI Network Compliance.....	24
View Current Vulnerabilities	24
View Compliance Status	26
Submit Network Reports	29
Submit False Positive Requests.....	32
View False Positive History.....	33
PCI Network Reports	34
View PCI Network Reports	34
PCI Report Details.....	35
PCI Questionnaires.....	41
New PCI DSS Self-Assessment Questionnaire (SAQ v1.1).....	41
Questionnaire Versions (A-D).....	42
Complete a New Questionnaire.....	42
Questionnaire D Guidance	45
Manage Questionnaires.....	48
Submit Your Questionnaire.....	48



Introducing the PCI Compliance Service

The PCI compliance service is an on demand PCI compliance testing and reporting service. Our company is certified as 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.

The PCI Security Standards Council requires banks, 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.

PCI Data Security Standard

The PCI Data Security Standard 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.

Those affected by this regulation are required to perform quarterly network security scans on their external facing networks and demonstrate compliance with their acquiring banks by submitting a report from an approved scanning vendor to prove that their infrastructure is secure and is 100% free of any vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council. Failure to comply with these security standards may result in fines, restrictions or permanent expulsion from card acceptance programs.

PCI Data Security Requirements

To comply with the PCI Data Security Standard, merchants and MSPs must demonstrate compliance to their respective acquirer(s) by completing the following security evaluation steps:

- 1** On an annual basis, conduct an Onsite Audit or complete the PCI Self-Assessment Questionnaire. Most levels of merchants and service providers must complete an annual questionnaire based on the PCI DSS requirements. The self-assessment questionnaire is available through our PCI compliance service. See “PCI Questionnaires” for details.
- 2** On a quarterly basis, use an approved scanning vendor to measure and eliminate security threats associated with electronic commerce, and provide acquiring banks with a report demonstrating compliance status. The scanning must be run against a merchant's entire Internet facing networks and systems by a PCI approved scanning vendor (ASV) like the PCI compliance service. See “PCI Network Scans” and “PCI Network Compliance” for details.

Canadian Visa Customers: Visa customers in Canada need to use a PCI approved scanning vendor (ASV) like US customers, as described above. For the questionnaire, customers must send their compliant questionnaire to a PCI qualified security assessor (QSA) for validation before submitting the questionnaire to acquiring banks.

PCI Merchant Levels

The PCI levels are described below. Note that network security scanning is a compliance component for each level as follows:

Merchant Level	Criteria / Requirements	Compliance Validation Date
Level 1	<p>Criteria:</p> <ul style="list-style-type: none"> - All merchants, including electronic commerce merchants, processing more than 6,000,000 transactions per year - All merchants that experienced an account compromise - All merchants that meet the Level 1 transaction criteria as set forth in the PCI framework <p>Requirements:</p> <ul style="list-style-type: none"> - Annual Onsite Review - Quarterly Network Security Scan 	<p>MasterCard: June 30, 2005</p> <p>Visa: September 30, 2004*</p> <p>*New Level 1 merchants have up to one year from identification to validate.</p>
Level 2	<p>Criteria:</p> <ul style="list-style-type: none"> - All merchants processing 1,000,000 to 6,000,000 e-commerce transactions per year - All merchants that meet the Level 2 transaction criteria as set forth in the PCI framework <p>Requirements:</p> <ul style="list-style-type: none"> - Annual Self Assessment Questionnaire - Quarterly Network Security Scan 	<p>MasterCard: December 31, 2008</p> <p>Visa: New Level 2 merchants: September 30, 2007</p>
Level 3	<p>Criteria:</p> <ul style="list-style-type: none"> - All merchants processing 20,000 to 1,000,000 e-commerce transactions per year - All merchants that meet the Level 3 transaction criteria as set forth in the PCI framework <p>Requirements:</p> <ul style="list-style-type: none"> - Annual Self Assessment Questionnaire - Quarterly Network Security Scan 	<p>MasterCard: June 30, 2005</p> <p>Visa: June 30, 2005</p>
Level 4	<p>Criteria:</p> <ul style="list-style-type: none"> - All other merchants <p>Requirements:</p> <ul style="list-style-type: none"> - Annual Self Assessment Questionnaire - Quarterly Network Security Scan 	Consult Acquirer

For Level 1 merchants, the annual onsite review may be conducted by either the merchant's internal auditor or a Qualified Security Assessor.

To fulfill the network scanning requirement, all merchants must conduct scans on a quarterly basis using an Approved Scanning Vendor.

Level 4 Merchants are required to comply with the PCI Data Security Standard. Level 4 Merchants should consult their acquirer to determine if compliance validation is also required.

Your Home Page

To be compliant with the PCI Data Security Standard, you must have a compliant self-assessment questionnaire and compliant network scan. The Home page shows your current compliance status for each of these components. A check mark (✔) indicates that you are compliant. A dash (✖) indicates that you are not compliant. These compliance status indicators identify the compliance status for the most recently submitted questionnaire and network scan. The compliance status indicators are kept up-to-date over time.

The following options appear on the Home page so you can quickly fulfill compliance requirements and download compliance reports.



Network Scan

You must run network security scans on your Internet facing networks and systems every 90 days. To start a scan, click the **Start a Scan** link. Then provide a scan title, select a bandwidth level, specify target IPs and click OK. You'll receive an email notification when the scan results are available.

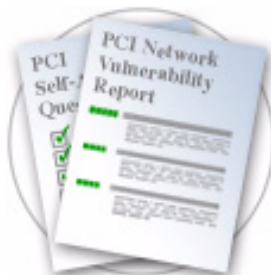
See "PCI Network Scans" to learn more.



Questionnaire

A self-assessment questionnaire must be completed every 12 months and submitted to your acquiring banks. To start a new questionnaire, simply click the **Complete a Questionnaire** link.

See "PCI Questionnaires" to learn more.



Download & Submit

Submit a compliant questionnaire and PCI network reports to your acquiring banks to demonstrate compliance with the PCI Data Security Standard. Then download the latest questionnaire and network reports for your records.

See "PCI Network Compliance" and "PCI Network Reports" to learn more.

In a new account, no compliance status indicators are displayed for the questionnaire and network scan until you submit these components to your acquiring banks using the workflows in the application. There is a separate workflow for generating network reports, called the PCI Executive Report and the PCI Technical Report, and the questionnaire. Each workflow generates

the component report in PDF, for the network or questionnaire, and saves it in your account so you can download it as needed. When your account settings include acquiring banks (see “Your Account Settings”), the service also submits the PDF reports to your banks automatically as a part of the workflow. When there is no acquiring bank on file, you need to download the PDF for the network reports and questionnaire from your account and submit them manually to your acquiring banks.

For a component that passed compliance and was submitted to acquiring banks, when the component becomes overdue for the next compliance period the component is shown as not compliant and the dash (—) is displayed.

PCI Scan Workflow


The following steps outline the PCI scan process from starting a PCI scan to submitting your network reports demonstrating your compliance with the PCI standards.


Step 1: Start a PCI Scan

Scan your entire external network on a quarterly basis. Underlying scan settings are optimized to test compliance with the PCI Data Security Standard requirements. The scan analyzes all hosts in your account to identify open vulnerabilities that must be fixed to pass PCI compliance. See “PCI Network Scans” to learn more.

Step 2: View Results and Fix Vulnerabilities

When your PCI scan completes, you can view the vulnerabilities detected by the scan from the Scans list (go to Network—>Scan Results on the left menu). The service indicates which vulnerabilities must be fixed to pass PCI compliance requirements. Review the vulnerability details for each detected vulnerability to quickly eliminate vulnerabilities that prevent you from passing PCI compliance requirements. A verified solution is provided for each vulnerability.

Select  next to the scan to download the Scan Results report to PDF format. The Detailed Results section of the report shows all vulnerabilities detected during the scan, sorted by host. All vulnerabilities and potential vulnerabilities marked as PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked PCI FAILED display vulnerabilities that the PCI compliance service found on the hosts during the scan. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

Select  next to the scan to view the Current Vulnerabilities list. The Current Vulnerabilities list provides a list of current vulnerabilities that were detected on the scan's target IPs by the most recent network scans. 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. It's possible that updated vulnerability data is available on the Current Vulnerabilities list in comparison to the vulnerability data in the Scan Results report.

View the host compliance status and current vulnerabilities per host. Go to Network—>Compliance Status on the left menu. On the Compliance Status page, the Host Status list shows compliance status per host. Click the View Vulnerabilities button to view all current vulnerabilities on all hosts. Click the Download Report button to download the Current Vulnerabilities Report in PDF format. To view the current vulnerabilities for a particular host,

select the check box to the left of the host and then click View Vulnerabilities or Download Report. See “Host Compliance Status” for more information and to learn about other host display options.

Step 3: Remediation Workflow

After fixing vulnerabilities, launch another PCI scan and check your network's compliance status. It's possible to launch a PCI scan on selected hosts, in case you need to verify compliance status on certain hosts. The PCI scan analyzes the target hosts for vulnerabilities again and validates that previously detected vulnerabilities have been fixed.

Scan your network in segments and remediate/re-scan vulnerabilities on target IPs until you achieve PCI compliance. Segmented scanning allows you to scan hosts that you have remediated, without having to scan your entire network. Compliance reporting summarizes your compliance on each of your network IPs.

Use the compliance reporting features to assist with the remediation process.

The Current Vulnerabilities list provides a list of current vulnerabilities that were detected on IPs in your account by the most recent network scans. To view this list, go to Network—> Vulnerabilities on the left menu.

The Compliance Status page provides the current PCI compliance status for your network and its hosts. To view Compliance Status, go to Network—>Compliance Status on the left menu. As you are in the process of fixing vulnerabilities, refer to the Compliance Status for information on remediation progress and the overall compliance status of your network. You can download a Current Vulnerabilities Report for one or more hosts to view vulnerability details in PDF format. See “View Compliance Status” for more information.

You may need to repeat Steps 1 through 3 until vulnerabilities are verified as fixed. Be sure to refer to the Compliance Status page to confirm your overall compliance status and host compliance status. An overall PCI compliance status of Compliant is returned when all hosts in the report passed the PCI compliance requirements. A compliance status of Compliant for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards, were detected on the host.

Step 4: Submit Network Reports to Your Acquiring Banks

Once all vulnerabilities have been fixed and verified by another PCI scan, then you are ready to submit your PCI network reports. The report generation workflow includes a Save & Submit option to allow you to save your network reports and submit them to your acquiring banks electronically, when your acquiring banks are listed in your account settings. The submitted reports are good for 90 days from the last submitted date.

To generate your network reports, go to Network—>Compliance Status on the left menu, click the Generate icon (in the upper right section) and follow the prompts to generate network reports. The message “Report Generation is complete” appears and you are prompted to review the reports in PDF format:

PCI Executive Report — This report documents compliance with PCI DSS and is suitable for submission to your acquiring banks to demonstrate PCI compliance. This report lists your overall PCI compliance status, the compliance status for each host, and the scan configuration settings

used. An overall PCI compliance status of PASSED is required to be compliant with the PCI DSS compliance standards. This status is returned when all hosts in the report passed the PCI compliance requirements.

PCI Technical Report — This report assists with remediation and tracking overall compliance status. This report lists your overall PCI compliance status and PCI compliance status by host, like the PCI Executive Report, and includes Detailed Results. The Detailed Results section identifies all detected vulnerabilities. For each vulnerability, many details are provided including a description of the threat, the impact if exploited, and a verified solution to fix the issue.

After reviewing the reports, click the Save & Submit button. The service saves your network reports on the Submitted Reports list where you can download them in PDF format at any time. The service also submits your network reports to your banks automatically when your acquiring banks are listed in your account settings. See “Your Acquiring Banks” to learn how to verify whether your banks are participating. For other banks, download and print the network reports from the Submitted Reports list and then send them manually via mail.



First Steps

All of your interactions with the PCI compliance service will be through its Secure Internet Interface which you can access using any standard Web browser. After registration, you will receive a registration email with a secure link to a user login and password for your account. This is a one-time-only link. Once you click the link to access your login credentials, the link will no longer be active. The email also identifies the platform URL for the PCI compliance service, where you log into the PCI Merchant application.

Logging In

With your login and password, you can now gain access to the PCI compliance service. Simply open your browser and go to the platform URL for the PCI compliance service. Enter your login and password and select “Login”.

First time users will be presented with a window to review the Service User Agreement. Upon accepting the Service User Agreement, you are directed to your Home page. On this page, the service provides an overall compliance status and a starting point for completing PCI compliance requirements.

QUALYSGUARD® PCI ONDEMAND SECURITY

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

Home

- Network**
 - New Scan
 - Scheduled Scans
 - Scan Results
 - Vulnerabilities
 - Compliance Status
 - Submitted Reports
 - False Positive History
- Questionnaires**
 - Saved Questionnaires
 - New Questionnaire
- Account**
 - Settings
 - IP Assets
 - Users
- Contact Support Resources**

Network Scan

Scan
[Start a Scan](#)
[Schedule a Scan](#)
[View Scan History](#)
[View Network Status](#)
[View Vulnerabilities](#)

Last Submitted: 12/05/2007
Next Due: 03/04/2008

Scanning Your Network
All merchants and service providers are required to perform quarterly external network security scans.
To determine your network status, first [add IPs](#) and then [scan your network](#) for vulnerabilities. For more information about scanning your network see the [Qualys PCI FAQ](#).

Questionnaire

Start
[Complete a Questionnaire](#)
[View Past Questionnaire](#)

Last Submitted: 04/30/2008
Next Due: 04/30/2009

Self-Assessment Questionnaire
Merchants and service providers are required to complete a self-assessment questionnaire to document their security status.
The document must be completed and submitted annually to your acquiring [banks](#).

Download & Submit

Submit
[Questionnaire](#)
[Network Reports](#)

Download Latest
[Questionnaire](#)
[Executive Report](#)
[Technical Report](#)

Submitting Your Score
You may submit your PCI compliance score to the acquiring banks either electronically or via mail.
To submit via the mail download your self-assessment [Questionnaire](#), your latest [Executive Report](#) and [Technical Report](#).


© 2008 Qualys, Inc. [Privacy Policy](#)

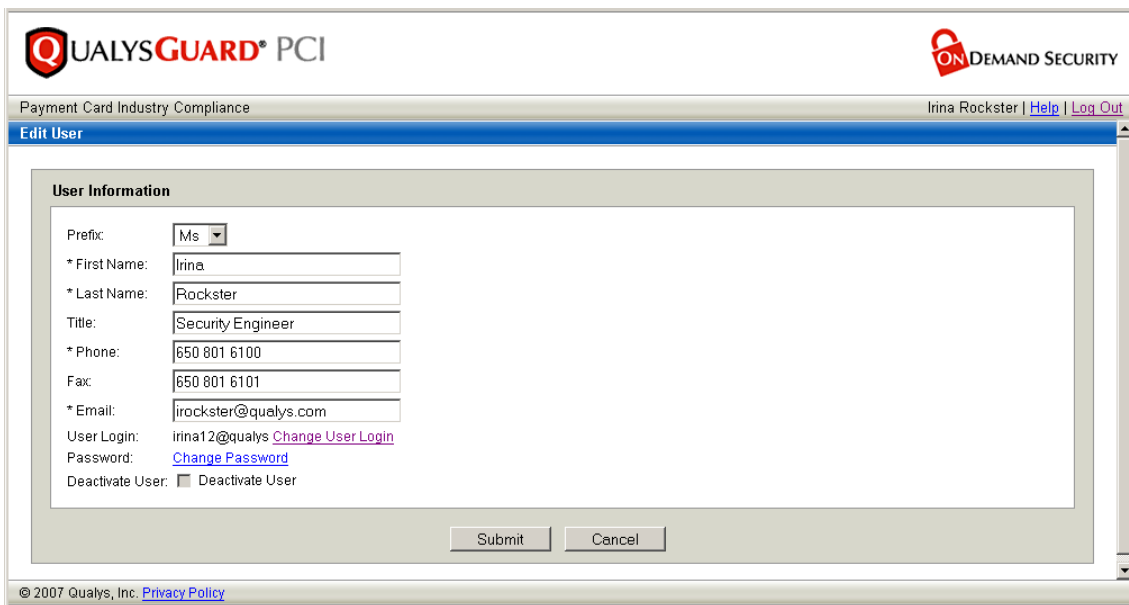
The center section provides quick links to common tasks and the compliance status of your network scan and questionnaire. Note that when you log in for the first time, the Last Submitted date appears as “Never” because you have not yet submitted reports proving compliance to your acquiring banks.

Change Your User 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. After changing your login credentials, you will be required to log back into the service using your new credentials.

To edit your 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.



The screenshot shows the 'Edit User' page in the QualysGuard PCI interface. The page header includes the QualysGuard PCI logo and the Demand Security logo. The breadcrumb trail is 'Payment Card Industry Compliance > Irina Rockster | Help | Log Out'. The main content area is titled 'Edit User' and contains a 'User Information' form. The form fields are: Prefix (Ms), * First Name (Irina), * Last Name (Rockster), Title (Security Engineer), * Phone (650 801 6100), Fax (650 801 6101), * Email (irrockster@qualys.com), User Login (irina12@qualys) with a 'Change User Login' link, Password (Change Password) with a 'Change Password' link, and a 'Deactivate User' checkbox. At the bottom of the form are 'Submit' and 'Cancel' buttons. The footer of the page is '© 2007 Qualys, Inc. Privacy Policy'.

To change your user login, select the “Change User Login” link. Enter your current login in the field provided. Then enter a new login in the New User Login field. Note that your user login must be unique and must include the @ character, such as john@company.

To change your password, select the “Change Password” link. Enter your current password in the field provided. Then enter a new password in the New Password field, following the strong password tips on the screen. Your password must be a minimum of 6 characters and must include a mixture of alpha and numeric characters.

After saving your new user login and/or password, log back into the service using your new login information.

First Steps

Add Additional Users (Optional)

Add Additional Users (Optional)

The PCI compliance service supports multiple users. You can add users to share the PCI scanning and reporting responsibilities. All users have the same privileges to access and manage questionnaires and network reports.

To add users, go to Account—>Users on the left menu. Then click the New link at the top of the Users list. On the New User page that appears, provide user contact information.

Email — The user's email address must be properly formatted (such as john_doe@company.com). Make sure the email address is current and submitted correctly.

User Login — The user login must be unique and must include the @ character, such as john@company. This is the login the user will use to connect to the service. Note that only ASCII characters are supported.

Once you've added user information, click Submit.

The new user will receive an email with instructions on how to log into the PCI compliance service. The email includes a secure link to an online registration form containing the URL to the service, the user's login, and an automatically generated "strong" password. The user can change the login credentials after logging in.

Add IPs for Scanning

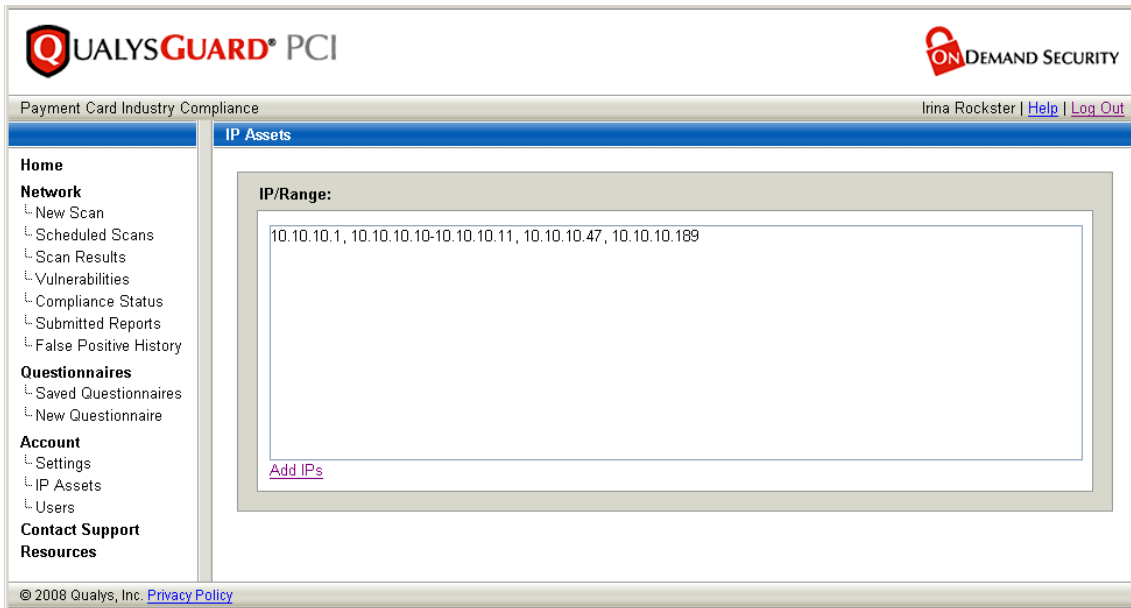
To meet compliance with the PCI Data Security Standard, PCI scans must be run against all of your Internet facing networks and systems on a quarterly basis. It is your responsibility to ensure that you are providing all of your IP addresses for scanning.

You can add IPs to your account for scanning and testing PCI compliance. Note that you cannot remove IPs from your account once they've been added. Contact Customer Support if you wish to remove IPs. To do this, select Contact Support from the left menu. On the page provided, you may send an email request to our support team.

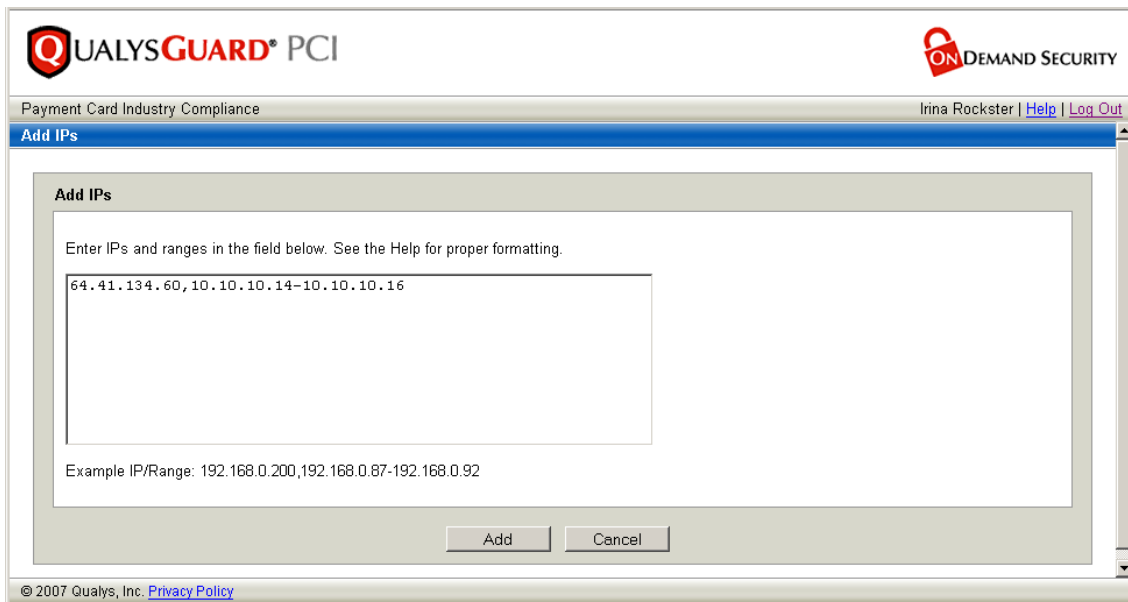
The maximum number of IPs you can add to your account is equal to the number of IPs purchased for your subscription. To view the total IPs purchased, go to Account—>Settings on the left menu. On the Settings page, scroll down to the section titled Subscription Information. You will see the fields Total IPs Purchased and Total IPs in Account.

Before adding new IPs to the account, verify the IPs already in your account. To do so, go to Account—>IP Assets on the left menu.

The IP Assets page appears with a list of the IPs in your account, if any. To add more IPs for scanning, click the Add IPs link.



The Add IPs page appears where you can add IPs for scanning.



In the field provided, enter the IP addresses and/or IP address ranges to add to the account. Separate each IP or range with a comma. Then click Add.

When adding IPs, the service does not verify whether the IP addresses you've entered are accessible from the Internet. This occurs after you've launched a scan. Only IPs that are accessible from the Internet are scanned by the service.

First Steps

Check Access to Scanner IP Addresses

Check Access to Scanner IP Addresses

Important! 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. The scanner IP addresses are below:

167.216.252.1 - 167.216.252.63

62.210.136.129-62.210.136.254

62.26.78.1-62.26.78.254

64.39.104.1-64.39.104.254

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 the IP addresses in your account during scan processing. Your network protection systems should be configured to not interfere with the vulnerability scanning, as described in the document *PCI DSS Security Scanning Procedures Version 1.1*, in the section "Scanning Procedures." This document is published at the PCI Security Standards Council's web site at:

https://www.pcisecuritystandards.org/tech/supporting_documents.htm

Your Account Settings

The service displays important information about your subscription and acquiring banks, including the bank name and your assigned merchant accounts for various credit card types.

To verify account information, go to Account—>Settings on the left menu. Review the information displayed on the Settings page and update any fields that are not correct. Note that you can also view the total number of IPs purchased, the total number of IPs currently in your account, and the Service User Agreement under Subscription Information.

Your Acquiring Banks

The PCI compliance service enables banks to view submitted PCI compliance documents and track PCI compliance status for their merchants through the PCI Bank application. To see a list of participating banks, go to Account—>Settings on the left menu and then scroll down to the Bank Information section. Click the "Edit" link and look at the banks listed in the Bank Name menu. These are participating banks.

If your acquiring bank is a participating bank, then be sure to select it in the Bank Name menu so that the bank can view your submitted documents and track your PCI compliance status through the PCI Bank application. You can add 5 banks to your account. As you submit questionnaires and network reports, they become immediately available for viewing by your banks.

If your acquiring bank is not a participating bank, then it will not appear in the Bank Name menu. Scroll down to the Other Banks section and enter the bank name in the field provided. If your account settings do not include any participating banks, then no bank has direct access to your submitted questionnaires and network reports. If this is the case, you must download your submitted documents in PDF format and send them to your banks using a method outside of the PCI compliance web application.

Getting Help While You Work

Online Help — Online help is accessible throughout the user interface by selecting the “Help” link in the top-right corner of the screen. From within the help, use the Contents, Index, and Search buttons to quickly find the information you need.

Contact Support — We welcome any comments, suggestions, or questions you might have. Go to Contact Support on the left menu to send an email message directly to our support team.

Resources — View resources to assist with passing PCI compliance requirements and follow the links for more information. To view the resources section, go to Resources on the left menu.

- Read the PCI FAQ provided by the service to learn more about the PCI compliance service and how to achieve compliance using the service.
- Visit the PCI Security Standards Council website for the latest information on the PCI Council and PCI Data Security Standard (PCI DSS).
- Visit the individual payment brand websites for information on their PCI compliance programs and security requirements.

You're Now Ready

At this point, you should have successfully obtained authorization, logged in, added IPs for scanning, and verified your account information. You are now ready to begin taking steps towards meeting compliance with the PCI Data Security Standard.

The sections to follow walk you through submitting compliant PCI questionnaires, running PCI vulnerability scans and submitting PCI scan reports to demonstrate compliance with the PCI Data Security Standard.



PCI Network Scans

The PCI Data Security Standard requires merchants and service providers to perform quarterly network security scans and eliminate security threats associated with electronic commerce. A report demonstrating compliance must be provided to your acquiring banks.

Before you begin, be sure there are IPs in your account. If there are no IPs in your account, you are prompted to enter IPs. See “Add IPs for Scanning” to learn how to add IPs to your account.

Before You Begin

Before getting started, please review the following information about PCI network scans.

Scan Target — You may launch a PCI scan on all IP addresses in your account or on selected IPs only. To achieve network status compliance, you must scan all IPs in your account during the best practice scanning period and there can be no PCI vulnerabilities found on all hosts. See “View Compliance Status” for more information on the best practice scanning period and the network compliance requirements.

Scan Settings — Underlying scan settings have been optimized to test compliance with the PCI Data Security Standard. There is one user-configurable scan performance setting - Bandwidth Level - which affects the overall scan performance. Several bandwidth levels are provided, and each level represents multiple settings. It's recommended that you use the default bandwidth level (Medium) to get started. You can make another selection at the time you launch the scan.

Scan Events — There are several events that take place during the scanning process, including host discovery, port scanning, OS detection, service discovery and vulnerability assessment. These events are described in detail in the online help provided with the PCI compliance service.

Scan Results — At the completion of your PCI scan, a Scan Summary email is sent to you with an overview of your results. Follow the link provided in this email to log back into the web application and go to Network—>Scan Results to view your scan results. A complete list of the vulnerabilities detected during the scan and instructions for remediation are provided. See “Fix Vulnerabilities and Re-scan” for further information.

PCI Scan Process

The following steps outline the PCI scan process.

Step 1: Start a Network Scan

Step 2: View Scan Summary Email

Step 3: View Scan Results

Step 4: Fix Vulnerabilities and Re-scan

Start a Network Scan

When starting a new PCI network scan, you have the option to scan all IPs in your account or only selected IPs. 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 Level - which affects overall scan performance. It's recommended that you use the default bandwidth level (Medium) to get started. You have the option to select another bandwidth level at the time you launch the scan.

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. (Or click Start a Scan on the Home page.)

The New Scan page appears.

The screenshot shows a 'New Scan' dialog box with the following fields and options:

- Scan Settings:**
 - * Title: My scan
 - Bandwidth: Medium (with an Info link)
 - Target IPs: All IPs, Select IPs
 - Target IP list: 10.10.10.1 (with a Select IPs link below)
- Scan Date:**
 - Launch Now, Schedule for Later
- Buttons: OK, Cancel

Supply a title for your scan in the Title field. The title appears in the Scans list and in PCI reports.

Select a bandwidth level. It's recommended that you keep the default bandwidth level of Medium (15 IP addresses may be scanned in parallel). Other bandwidth options are Low, Medium - low HTTP impact, Medium (the default), and High. Click the "Info" link for further information on the bandwidth levels.

Select the IPs you want to scan in the Target IPs section. 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 IPs in the field provided or click the Select IPs link to choose IPs from a list.

To start the scan right away, click the "Launch Now" option under Scan Date.

Click OK.

Your scan appears on the Scans list where you can view the scan status. The scan runs in the background so you can exit the PCI web application while the scan continues. You can return to the Scans list at any time for updated status. To do this, go to Network—>Scan Results on the left menu (or click View Scan History on the Home page).

Schedule a Network Scan

You have the option to schedule the PCI scan to start at a later time. To do so, select the “Schedule for Later” option on the New Scan page. Scheduler options appear, as shown below.

The screenshot shows a 'New Scan' dialog box with the following sections:

- Scan Settings:**
 - * Title:
 - Bandwidth: [Info](#)
 - Target IPs: All IPs Select IPs
 -
 - [Select IPs](#)
- Scan Date:**
 - Launch Now Schedule for Later
- Scheduler:**
 - Start Date:
 - Start Time:

Buttons:

Provide a start date (month, day and year) and start time (hours and minutes). The GMT shift is set automatically based on your local system setting. You may select a different GMT shift from the menu provided. After clicking OK, your scheduled scan appears on the Scheduled Scans list.

If you've selected All IPs for your scan target, then the service scans all IPs 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.

When the scan starts (at the time you've specified), then it will appear on the Scans list 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 Scan Summary Email

When the scan is complete, you will receive a Scan Summary email notification with a link to access the PCI Merchant application so you can easily log back in to view your scan results.

The email notification includes details about your scan, including the scan title, launch date, name of the user who initiated the scan, the number of active hosts scanned and the PCI compliance status based on the scan results.

From: QualysGuard PCI Support
To: Irina Rockster
Cc:
Subject: QualysGuard PCI -- Scan Summary

Email scan summary by QualysGuard PCI.

Scan Title: My scan
Start Date: 11/19/2007 at 11:23:43 (GMT -08)
Duration: 00:06:43

Target Hosts: 1
Active Hosts: 1

Launched By: Irina Rockster (irina12@qualys)
Company: Acme Sports
Launch Type: On Demand
Scan Status: Finished

PCI Status: Not Compliant

To view your detailed scan results, access the QualysGuard PCI Web application using the following link:

<https://pci.qualys.com/merchant/>

For more information, please email Qualys Support:
<mailto:support@qualys.com>

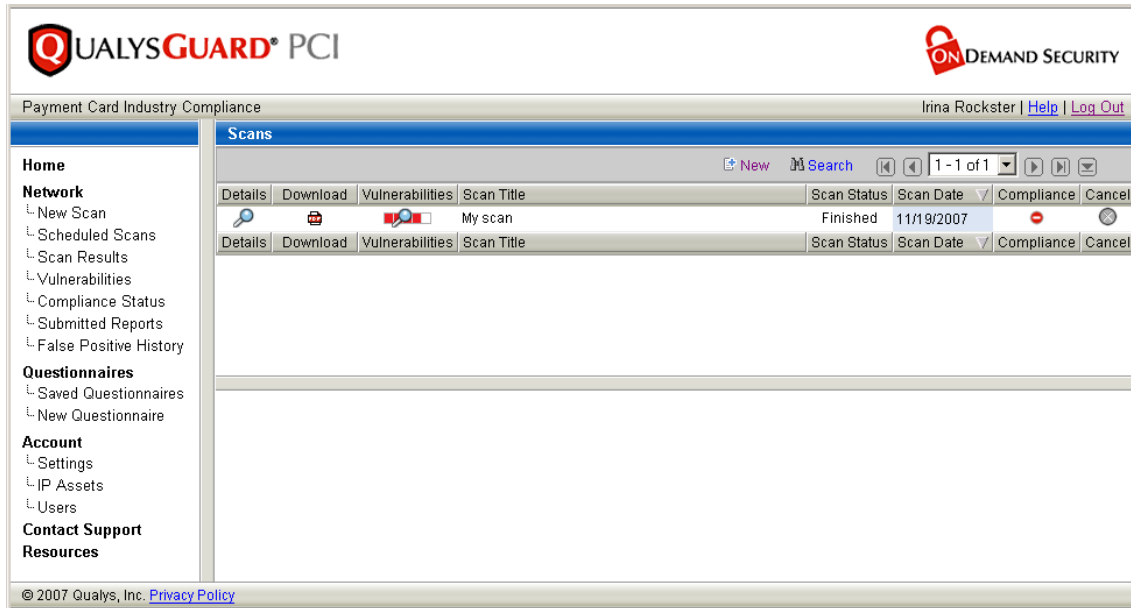
(c) Copyright 2006-2007 Qualys, Inc. All rights reserved.
<http://www.qualys.com>

This sample Scan Summary email indicates that the PCI Status is “Not Compliant”. This means that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected by the scan. Use the link in the email to log back into the PCI Merchant application to view the full scan results.

View Scan Results

The service provides a complete list of running and completed scans. From this list, you can view and download PCI scan results, view detected vulnerabilities and cancel running scans.


To see the Scans list, select Network—>Scan Results on the left menu (or click View Scan History on the Home page).





From the Scans list, you can search and view scan tasks, view scan task details, view the scan status (such as Running or Finished), cancel running scans, view detected vulnerabilities that must be fixed to achieve PCI compliance, and download the scan results. In the Scan Results report, the Detailed Results section shows all vulnerabilities detected by the service (not limited to vulnerabilities that must be fixed to achieve PCI compliance).

At the top of the list are some navigation options. To search for a particular scan, click the “Search” link. You can find scans based on scan title, scan status, scan date and compliance status. To start a new scan, click the “New” link.

For each scan the scan title, status and scan date are provided. You can take the following actions:

Details — Select  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 — Select  to download the Scan Results 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 marked PCI FAILED must be fixed to pass the PCI compliance requirements. See “PCI Network Reports” for a detailed description of the data presented in the Scan Results report.

Vulnerabilities — Select  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 scans. For this reason, the current vulnerabilities list may have more up-to-date information than the Scan Results. If this image is grayed out, then the target IPs for the scan are compliant with PCI security standards. See “Fix Vulnerabilities and Re-scan” for more information.

Compliance — Identifies whether the scan is compliant with the PCI Data Security Standard. A check mark (✔) indicates that the scan is Compliant. No vulnerabilities, which must be fixed to pass PCI compliance, were found on the target IPs. A dash (—) indicates that the scan is Not Compliant. One or more vulnerabilities, which must be fixed to pass PCI compliance, were found on the target IPs. To view overall network compliance status and compliance status per host, go to Network—>Compliance Status on the left menu. We will discuss compliance status in detail in the next chapter “PCI Network Compliance.”

About Vulnerability Classification

The calculation of the PCI pass/fail compliance status follows the PCI compliance standards set by the PCI Council. The criteria for calculation of the PCI pass/fail compliance status implemented by the PCI compliance service is calculated based on criteria listed at this URL:

http://www.qualys.com/products/pci/qgpci/pass_fail_criteria/

Important! The PCI Security Standards Council provided all Approved Scanning Vendors (ASVs) a deadline of **July 1st, 2008** to use NIST’s Common Vulnerability Scoring System (CVSS) version 2.0. Beginning **May 1st, 2008** the PCI compliance service will calculate PCI pass/fail criteria based on CVSS version 2.0 scores. In previous releases available through **April 30th, 2008** the service calculated PCI pass/fail criteria based on CVSS version 1.0 scores.

The PCI compliance service classifies vulnerabilities by vulnerability level and severity level as follows:

Vulnerability Level	Description (Severity Level)
Vulnerability	A design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. (Severity Level 1 to 5)
Potential Vulnerability	A vulnerability that we cannot confirm with 100% certainty that it exists. At least one necessary condition for the vulnerability was detected. It's recommended that you investigate these vulnerabilities further. (Severity Level 1 to 5)
Information Gathered	A vulnerability that includes visible information about the network related to the host, such as traceroute information, Information Service Provider (ISP), a list of reachable hosts, detected firewalls, SMTP banners, open services. (Severity Level 1 to 3)

To view definitions of severity levels while viewing your report, scroll down to the Appendices section and open the Report Legend.

Fix Vulnerabilities and Re-scan

The Vulnerabilities section provides a list of all current vulnerabilities that were detected by the most recent network scans. All detected vulnerabilities are listed, including vulnerabilities that must be fixed to pass PCI compliance and 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.

The workflow for fixing vulnerabilities and running verification scans is described below.

View current vulnerabilities:

Select Network—>Vulnerabilities on the left menu (or select View Vulnerabilities on the Home page). The Current Vulnerabilities list displays current vulnerabilities that were detected on hosts from the most recent scans.

The screenshot shows the QualysGuard PCI interface. The top navigation bar includes the QualysGuard PCI logo, the ON DEMAND SECURITY logo, and the text "Payment Card Industry Compliance" and "Irina Rockster | Help | Log Out". The left sidebar contains a navigation menu with categories: Home, Network (New Scan, Scheduled Scans, Scan Results, Vulnerabilities, Compliance Status, Submitted Reports, False Positive History), Questionnaires (Saved Questionnaires, New Questionnaire), Account (Settings, IP Assets, Users), and Contact Support Resources.

The main content area is titled "Vulnerability Report Settings" and includes a search section with "Find:" (QID, beginning with), "IPs/Ranges: Select IPs", and "Severity Levels: Confirmed: 5 4 3 2 1, Potential: 5 4 3 2 1". There is a "Run" button and a checkbox for "Display only PCI vulnerabilities". Below this is the "Current Vulnerabilities" section, which has a table with columns: Details, PCI, QID, Vuln Title, Severity, IP Address, Hostname, Scanned, and False Positive. The table lists several vulnerabilities, including ISC BIND Pre 9.2.2 Multiple Possible Vulnerabilities, DNS Server Allows Remote Clients to Snoop the DNS, ISC BIND Multiple Remote Denial of Service Vulnerabilities, ISC BIND Remote Cache Poisoning Vulnerability, and DNS Zone Transfer.


Details	PCI	QID	Vuln Title	Severity	IP Address	Hostname	Scanned	False Positive
<input type="checkbox"/>	<input checked="" type="checkbox"/>	15031	ISC BIND Pre 9.2.2 Multiple Possible Vulnerabilities	4	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	
<input type="checkbox"/>	<input type="checkbox"/>	15035	DNS Server Allows Remote Clients to Snoop the DNS	2	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	
<input type="checkbox"/>	<input type="checkbox"/>	15052	ISC BIND Multiple Remote Denial of Service Vulnerabilities	3	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	15053	ISC BIND Remote Cache Poisoning Vulnerability	3	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	
<input type="checkbox"/>	<input type="checkbox"/>	15018	DNS Zone Transfer	3	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	15018	DNS Zone Transfer	3	10.10.10.1	bart.vuln.qa.qualys.com	02/06/2008	

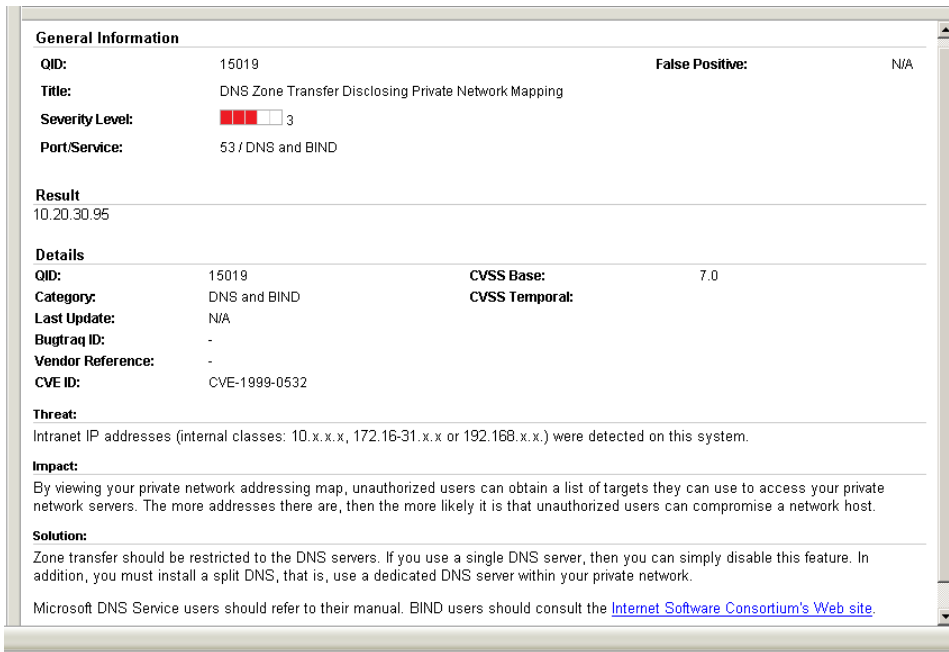
Optionally, use the search options in the Vulnerability Report Settings section to search for vulnerabilities. You may search for vulnerabilities by QID, vulnerability title, vulnerability severity levels, target IPs, and vulnerabilities with associated false positive requests. To perform a search, select report settings and then click Run.

In the Current Vulnerabilities list, you will notice the PCI column indicates whether the vulnerability must be fixed to pass PCI compliance requirements. A dash (⊖) indicates that the vulnerability must be fixed to pass PCI compliance.

You can choose to display only vulnerabilities that must be fixed to pass PCI compliance in the Current Vulnerabilities list. To do this, click the check box "Display only PCI vulnerabilities" in the Vulnerability Report Settings section. Then click the Run button.

View vulnerability details:

Select  next to a vulnerability to see vulnerability details, including the specific scan test results for the vulnerability on the particular host, a description of the threat, the possible consequences that may occur if the vulnerability is exploited and a recommended solution to fix the vulnerability.



The screenshot displays a window titled "General Information" for a vulnerability. The "Title" is "DNS Zone Transfer Disclosing Private Network Mapping". The "Severity Level" is shown as three red squares followed by a white square and the number 3. The "Port/Service" is "53 / DNS and BIND". The "Result" is "10.20.30.95". The "Details" section includes "QID: 15019", "Category: DNS and BIND", "CVSS Base: 7.0", "CVSS Temporal: ", "Last Update: N/A", "Bugtraq ID: -", "Vendor Reference: -", and "CVE ID: CVE-1999-0532". The "Threat" section states: "Intranet IP addresses (internal classes: 10.x.x.x, 172.16-31.x.x or 192.168.x.x.) were detected on this system." The "Impact" section states: "By viewing your private network addressing map, unauthorized users can obtain a list of targets they can use to access your private network servers. The more addresses there are, then the more likely it is that unauthorized users can compromise a network host." The "Solution" section states: "Zone transfer should be restricted to the DNS servers. If you use a single DNS server, then you can simply disable this feature. In addition, you must install a split DNS, that is, use a dedicated DNS server within your private network." A note at the bottom says: "Microsoft DNS Service users should refer to their manual. BIND users should consult the [Internet Software Consortium's Web site](#)."

Re-scan hosts to verify fixes:

After fixing the critical vulnerabilities, start another PCI 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 PCI scan analyzes your hosts for vulnerabilities again and validates that previously detected vulnerabilities have been fixed.

Check compliance status:

View host compliance status and current vulnerabilities per host. To do this, go to Network—>Compliance Status on the left menu.

See the next section "PCI Network Compliance" for further information on viewing compliance status, including the overall compliance status for your entire network and the host compliance status for each host.



PCI Network Compliance

The PCI compliance service makes current network compliance status available at all times to assist with the remediation process. After fixing vulnerabilities, check your compliance status based on the most recent scan results. By scanning your network in segments, you can remediate and then re-scan target IPs until you achieve PCI compliance. Segmented scanning allows you to scan hosts that you have fixed, without having to scan your entire network. Compliance reporting summarizes your compliance on each of your network IPs.

Compliance Reporting provides workflows to assist with achieving PCI network compliance:

View Current Vulnerabilities — The Current Vulnerabilities list provides a list of current vulnerabilities that were detected on IPs in your account by the most recent network scans.

View Compliance Status — The Compliance Status page provides the current PCI compliance status for your network and its hosts.

Submit Network Reports — Once all vulnerabilities have been fixed and verified by another PCI scan, then you are ready to generate PCI network reports (PCI Executive Report and PCI Technical Report) and submit them to your acquiring banks. The submitted reports are good for 90 days from the last submitted date.

Submit False Positive Requests — In special circumstances, you may request an exception for a vulnerability/IP pair that will be considered by us as a false positive. If the request is approved, the vulnerability/IP instance will not appear in PCI reports.

View False Positive History — Review all false positive requests submitted by all users over time. For each request, view current status, request details and comment history.

Important! The PCI Security Standards Council provided all Approved Scanning Vendors (ASVs) a deadline of **July 1st, 2008** to use NIST's Common Vulnerability Scoring System (CVSS) version 2.0. Beginning **May 1st, 2008** the PCI compliance service will calculate PCI pass/fail criteria based on CVSS version 2.0 scores. In previous releases available through **April 30th, 2008** the service calculated PCI pass/fail criteria based on CVSS version 1.0 scores.

View Current Vulnerabilities

The Current Vulnerabilities list provides a list of current vulnerabilities and potential vulnerabilities that were detected on IPs in your account by the most recent network scans. 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 IPs in your account by default. You may select vulnerability attributes to limit the list displayed.

The screenshot shows the QualysGuard PCI interface. At the top, there are logos for QualysGuard PCI and Demand Security. Below the logos, the user is logged in as Irina Rockster. The main content area is divided into two sections: 'Vulnerability Report Settings' and 'Current Vulnerabilities'.

Vulnerability Report Settings:

- Find:** A search box with a dropdown menu set to 'beginning with' and a text input field.
- IPs/Ranges:** A text input field with a 'Select IPs' link.
- Severity Levels:** A grid of checkboxes for severity levels 1 through 5, with 'Confirmed' and 'Potential' categories. 'Confirmed' has checkboxes for 5, 4, 3, 2, 1. 'Potential' has checkboxes for 5, 4, 3, 2, 1.
- False Positives:** Checkboxes for 'Requested' and 'Rejected'.
- Run:** A button to execute the search.
- Display only PCI vulnerabilities:** A checkbox.

Current Vulnerabilities:

A table listing vulnerabilities with columns: Details, PCI, QID, Vuln Title, Severity, IP Address, Hostname, Scanned, and False Positive. The table shows several vulnerabilities, including 'Std Format Bug Vulnerability', 'SSH Protocol Version 1 Supported', 'OpenSSH Multiple Memory Management Vulnerabilities', 'DNS Zone Transfer Disclosing Private Network Mappi...', and 'DNS Zone Transfer AT&T WinVNC Server Buffer'.


Vulnerability Report Settings

The Vulnerability Report Settings section appears above the vulnerabilities list area. This section displays several settings, giving you many ways to search your current vulnerabilities. To perform a search, select report settings and then click the Run button (to the right of the settings).

There are several methods for searching current vulnerabilities. You may search for vulnerabilities by vulnerability ID (QID), vulnerability title, vulnerability severity levels, target IPs, and vulnerabilities with false positive requests - in the requested or rejected state. Select the check box "Display only PCI vulnerabilities" to display only vulnerabilities that must be fixed to pass PCI compliance.

Current Vulnerabilities List

The Current Vulnerabilities list displays current vulnerabilities and potential vulnerabilities detected on the IPs in your account by the most recent network scans. When no report settings are selected, all current vulnerabilities on all IPs in your account are displayed. If report settings are selected, the list is restricted to the vulnerabilities that match your search criteria.

For each vulnerability, the service lists this information from the most recent scan: vulnerability ID (QID), vulnerability title, severity level, IP address, hostname, the date when the scan was started. A dash (⊖) in the PCI column indicates that the vulnerability must be fixed to pass PCI compliance. The False Positive column indicates the state of a false positive request (Requested or Rejected), if any. Select  next to a vulnerability to see vulnerability details.

False positive requests can be reviewed and managed from the Current Vulnerabilities list (view the False Positive column, view vulnerability details, search for vulnerabilities matching a false positive state) and from the False Positive History section - see "View False Positive History."

Taking 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 Report.** 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 selected settings in Vulnerability Report Settings and/or vulnerabilities in the list area (using check boxes).
- **Submit False Positive Requests.** 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."

View Compliance Status

The Compliance Status page provides the current PCI compliance status for your network and its hosts. The overall network status is Compliant when all hosts are Compliant. In order for a host to receive the Compliant status, you must scan the host during the best practice scanning period and there can be no PCI vulnerabilities found for that scan. PCI vulnerabilities are vulnerabilities that must be fixed to pass PCI compliance. The PCI compliance service defines the best practice scanning period to be 30 days prior to today.

To view compliance status, go to Network—>Compliance Status on the left menu. (Or click View Network Status on the Home page.) On the Compliance Status page, you'll notice the Compliance Status chart and the Host Status list.

Overall Compliance Status

The Compliance Status chart at the top of the page displays the current compliance status of your entire network, including all hosts.

QUALYS GUARD® PCI **ON DEMAND SECURITY**

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

Compliance Status

Overall Status: Not Compliant

In Account:	5	Level 5	0	Level 5	0
Not Live:	0	Level 4	0	Level 4	0
Compliant:	1	Level 3	2	Level 3	1
Not Compliant:	1	Level 2	1	Level 2	0
Not Current:	3	Level 1	0	Level 1	0

Actions: [Generate](#)

Host Status

All Live Hosts

IP	Hostname	Operating System	Compliance	Vulnerabilities	Scan Date
10.10.10.1	bart.vuln.qa.qualys.com	Linux 2.4-2.6	Not Compliant	4	03/21/2008
10.10.10.47	dhcp-47.vuln.qa.qualys.com	Operating System	Compliant	0	03/21/2008

Overall Status — Identifies whether the network is compliant with the PCI Data Security Standard. The network consists of all the IPs 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 giving the status of the hosts in your account.

Host Status	Description
In Account	Total number of hosts in your account. This is the total number of hosts in your network.
Not Live	Total number of IPs 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	Total number of hosts in your account that are Compliant with PCI security standards.
Not Compliant	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	The total number of current vulnerabilities, at each 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 that you fix.
Potential Vulnerabilities	The total number of current potential vulnerabilities, at each severity level, that have been detected on the network. These include potential vulnerabilities that failed PCI compliance and must be fixed, as well as potential vulnerabilities that we recommend that you fix.
Actions	Click the Generate icon to generate PCI network reports based on the current vulnerability data for your network. See "Submit Network Reports" for instructions on using the workflow to generate, save and submit network reports.

Host Compliance Status

The Host Status list provides the current compliance status for hosts in your account. The interactive list allows you to display certain hosts in the list, display host details for hosts in the list, and perform actions on hosts, such as launch a scan, view current vulnerabilities, and download reports. Current information about hosts is provided based on the most recent network scans.

All live hosts in your account are displayed in the Host Status List by default. Use the Display menu to display hosts not alive or hosts not current. For each host, the service lists the host IP address, hostname, operating system, the total number of vulnerabilities and potential vulnerabilities, the last scan date, and the host compliance status, which indicates whether the host is compliant with PCI compliance standards. A check mark (✔) indicates that the host is Compliant. A dash (⊖) indicates that the host is Not Compliant.

The screenshot shows a web interface for host management. On the left is a navigation menu with sections: Questionnaires, Account, Contact Support, and Resources. The main area is titled 'Host Status' and includes a dropdown menu set to 'All Live Hosts' and a 'Display' button. Below this is a table with columns: IP, Hostname, Operating System, Compliance, Vulnerabilities, and Scan Date. Two hosts are listed: 10.10.10.1 (Not Compliant, 4 vulnerabilities) and 10.10.10.47 (Compliant, 0 vulnerabilities). Below the table is a 'Host Details' section for IP 10.10.10.1, showing OS (Linux 2.4-2.6), a 'Last Scan Result' link, and a grid of vulnerability counts for Levels 1-5. The grid shows 0 Level 5, 0 Level 4, 2 Level 3, 1 Level 2, and 0 Level 1 vulnerabilities. At the bottom left, there is a copyright notice: © 2008 Qualys, Inc. Privacy Policy.

Display Options

The Display menu allows you to select certain hosts in your account to be displayed in the Host Status list. Your options are:

- **All Live Hosts.** Select to display all hosts that were found to be alive when they were last scanned.
- **Hosts not Live.** Select to display hosts that were not found alive (up and running, and connected to the Internet) when they were last scanned.
- **Hosts not Current.** Select 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.

Click an IP address in the Host Status list to display host details in the preview pane, under the Host Status list.

Taking Actions

Use the actions bar above the Host Status list to perform actions on one or more hosts in the list. Select hosts using the check boxes (in the left column of the list), and then select an action. These buttons allow you to take actions:

- **Scan.** Click to start a 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. The Detailed Results section of the report displays all current vulnerabilities, potential vulnerabilities and information gathered. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be fixed to pass the PCI compliance requirements. See “PCI Network Reports” for a detailed description of the data presented in the Current Vulnerabilities Report.

Submit Network Reports

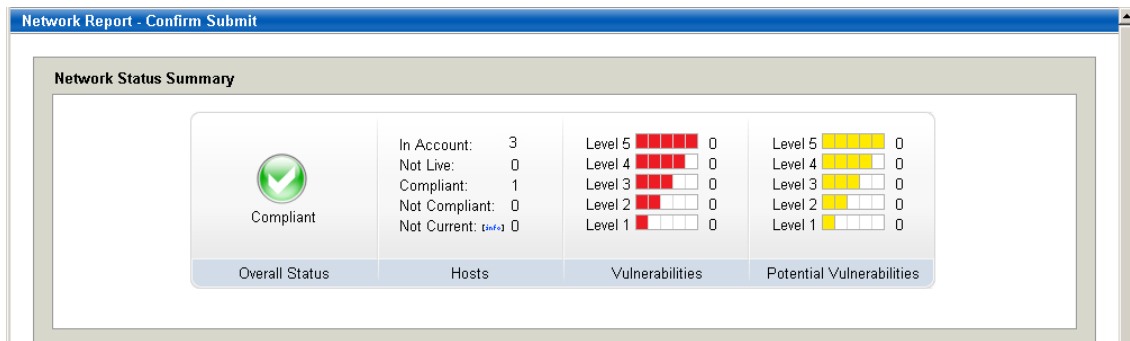
The service provides these network reports: PCI Executive Report and PCI Technical Report. The network reports include current vulnerability data returned from the most recent scans on your network, including all IPs in your account. See “PCI Network Reports” for general information about these reports.

Once all vulnerabilities have been fixed and verified by another scan, then you are ready to generate your network reports and either submit them to your acquiring banks automatically or submit them manually. The report generation workflow generates the network reports in PDF format and saves them in your account. When there are acquiring banks in your account (see “Your Account Settings”), the workflow submits the network reports to your banks automatically. If there are no banks on file, you need to download the reports and submit them manually to your banks. Submitted reports are good for 90 days from the last submitted date.

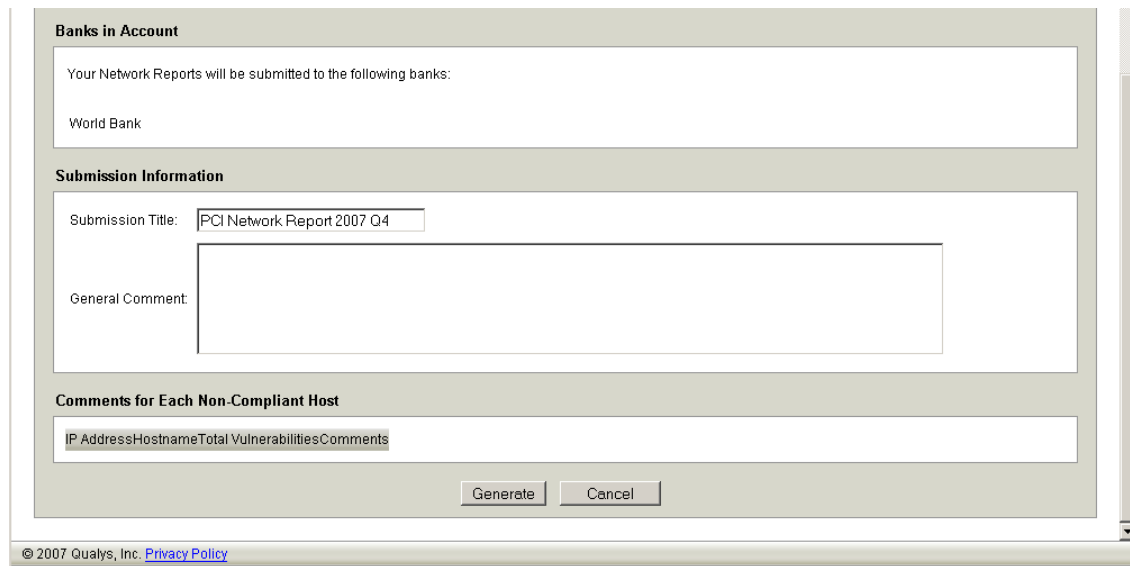
The workflow to generate, save and submit network reports is described below.

Generate network reports:

- 1 Go to Network—>Compliance Status on the left menu. (Or click View Network Status on the Home page.)
- 2 Check your overall network status. At the top of the page, the Overall Status appears with a check mark (✔) when your network is compliant and there are no vulnerabilities that must be fixed to pass PCI compliance.
- 3 Click the Generate icon (in the upper right corner of the chart). The pop-up window “Network Report - Confirm Submit” opens showing your network status summary.



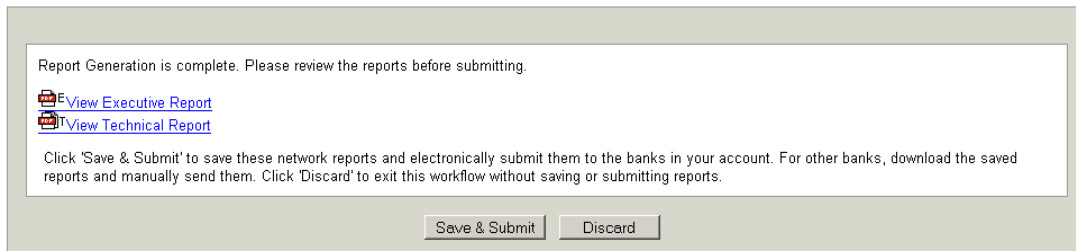
- 4 Scroll down and enter report information to be submitted to your acquiring banks, including a title and comments for tracking purposes. If you have non-compliant hosts, then you are prompted to supply comments for each host.



- 5 Click the Generate button.
- 6 During report generation, a pop-up window is displayed with status messages. The message “Launching Report” appears followed by “Generation Complete”. Important: During report generation, do not exit or cancel this page. If you leave this page, reports are not generated and cannot be saved in your account.

Review network reports:

After the network reports have been generated, the service displays the message: “Report Generation is complete. Please review the reports before submitting.”



Select the View Executive Report link to view the PCI Executive Report. Select the View Technical Report link to view the PCI Technical Report. You may choose to download these reports to your local filesystem and share them with other users.

These reports display the current vulnerability data returned from the most recent scans on your network. In both reports, the current vulnerability data for all IPs in your account is included.

Save & Submit:

Save & Submit — Click to save the PCI network reports in your account and submit them electronically to the banks in your account. The PCI Executive Report and the PCI Technical Report will be submitted to your banks if electronic submission through the service is enabled for your banks. For other banks, download and print the network reports and then send them manually via mail.

Discard — Click to exit the workflow without saving or submitting reports.

Saved PCI network reports appear on the Submitted Reports list in your account where you can view and download them as needed. To view this list, go to Network—>Submitted Reports.

Submit options:

You have the option to submit network reports electronically or manually.

If your acquiring banks are participating banks and defined for your account, then the bank can log into the PCI compliance service to view PCI network reports that you submit. Note that acquiring banks do not have access to reports that have not been submitted.

If your acquiring banks are not participating banks, then you must download the network reports in PDF format and send them to the bank using mail, outside of the application.

See “Your Acquiring Banks” to learn how to verify whether your banks are participating.

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 options in the Vulnerability Report Settings section to search for vulnerabilities.
- 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.

Details	PCI	QID	Vuln Title	Severity	IP Address	Hostname	Scanned	False Positive
<input type="checkbox"/>		15031	ISC BIND Pre 9.2.2 Multiple Possible Vulnerabili...	4	10.10.10.1	bart.vuln.qa.qualys.com	11/19/2007	<input type="checkbox"/>
<input checked="" type="checkbox"/>		15053	ISC BIND Remote Cache Poisoning Vulnerability	3	10.10.10.1	bart.vuln.qa.qualys.com	11/19/2007	<input checked="" type="checkbox"/>
<input type="checkbox"/>		15052	ISC BIND Multiple Remote Denial of Service Vulnera...	3	10.10.10.1	bart.vuln.qa.qualys.com	11/19/2007	<input type="checkbox"/>

- 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 (see screen below). 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".

Request False Positives

Vulnerability 1 of 1

IP Address: 10.10.10.1 Vulnerability: 15053 - ISC BIND Remote Cache Poisoning Vulnerability
 Hostname: bart.vuln.qa.qualys.com Severity: 3

[+ Vulnerability Details:](#)
[+ Result:](#)

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


© 2007 Qualys, Inc. [Privacy Policy](#)





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.

- If the false positive request is approved, then the vulnerability will no longer be reported for the specific host.
- If the false positive request is not approved, then you must fix the vulnerability in order to pass PCI compliance standards.

View False Positive History

The False Positive Request History page allows you to review and manage false positive requests. 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. 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, or Rejected). Select  next to a request to view request details and comment history.

False Positive Request History							
Search <input type="text" value=""/> 11 - 20 of 163							
	Details	QID	Title	IP	Requested	Reviewed	Status
		90086	Microsoft SQL Server Multiple Vulnerabilities	10.10.10.207	09/25/2006	09/25/2006	Approved
		90278	Microsoft Plug and Play Remote Code Execution and ...	10.10.10.207	09/25/2006	09/25/2006	Rejected
		90267	Windows Plug and Play Remote Code Execution (MS05-...	10.10.10.207	09/25/2006	11/21/2006	Approved
		90108	Multiple Microsoft Windows Vulnerabilities (MS04-0...	10.10.10.193	11/20/2006	09/28/2006	Requested

The list of false positive requests can be easily sorted and searched. To sort the list, select a column and click the column title. Click the Search link (in the upper right) to search for requests by vulnerability ID (QID), vulnerability title, request status and/or host IP address.

You can review and manage false positive requests from the Current Vulnerabilities list, described earlier in the section “View Current Vulnerabilities.”



PCI Network Reports

You are required to submit PCI network reports demonstrating compliance with PCI standards on a quarterly basis. See “Submit Network Reports” for further information. Once submitted, the PCI network reports are available for download from your Home page and from the Submitted Reports list.

The PCI Executive Report is appropriate for submission to your acquiring banks to demonstrate compliance with the PCI Data Security Standard. This report includes your overall compliance status, the compliance status for each scanned host, and the scan configuration settings used. An overall PCI compliance status of PASSED is required to pass PCI compliance. This status is returned in the PCI network report when all hosts in the report passed the PCI compliance requirements.

The PCI Technical Report includes the same PCI compliance status as the PCI Executive Report plus a Detailed Results section. This section provides detailed vulnerability information sorted by host, so you can quickly find and eliminate network security vulnerabilities.



These additional reports are provided by the PCI compliance service: Scan Results Report (see “View Scan Results”) and Current Vulnerabilities Report (see “View Compliance Status”). These reports provide detailed results on scans and current vulnerabilities in your account.

View PCI Network Reports

To view PCI network reports from the Home page:

- 1 Select Home from the left menu.
- 2 Scroll down to the Download & Submit section.
- 3 Under Download Latest, click the links Executive Report and Technical Report.

To view PCI network reports from Submitted Reports list:

- 1 Select Network—>Submitted Reports from the left menu. The Submitted Reports list appears.
- 2 Identify the submitted report you're interested in, and select one of the following:
 - Select  E to view the PCI Executive Report.
 - Select  T to view the PCI Technical Report.
- 3 Open or download the selected report in PDF format.

Each report includes a cover page with your company name and contact information, an executive summary, your PCI compliance status and report appendices with additional information.

PCI Report Details


The PCI reports provided by the PCI compliance service include similar sections. Note, however, that not all sections appear in all reports.


The PCI Executive Report and the PCI Technical Report include these sections: Executive Summary and PCI Status.

Executive Summary

This section appears in these reports: PCI Executive Report and PCI Technical Report.

The Executive Summary shows the SDP/PCI vendor certificate number assigned to the approved scanning vendor (ASV), the IP addresses that were scanned and the scan settings used. The summary also provides the date and time when the scan was initiated and the scan duration.





Payment Card Industry (PCI) Executive Report

12/06/2007

Executive Summary

This report was generated by the SDP compliant scanning vendor Qualys, under certificate number 3728-01-02 in the framework of the PCI data security initiative.

IP Addresses

10.10.10.1
10.10.10.10
10.10.10.47

The scan option profile used includes:

Scan Settings		Advanced Settings	
Scanned TCP Ports	Full	Host Discovery	TCP Standard Scan
Scanned UDP Ports	Standard Scan		UDP Standard Scan
Scan Dead Hosts	Off		ICMP On
Load Balancer Detection	Off	Ignore RST packets	Off
Password Brute Forcing	Standard	Ignore firewall-generated SYN-ACK packets	Off
Vulnerability Detection	Complete	ACK/SYN-ACK packets during discovery	Send
Windows Authentication	Disabled		
SSH Authentication	Disabled		
Oracle Authentication	Disabled		
SNMP Authentication	Disabled		
Perform 3-way Handshake	Off		

PCI Status

This section appears in these reports: PCI Executive Report and PCI Technical Report.

The PCI Status section shows overall PCI compliance status and PCI compliance status per host.

Overall PCI Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance requirements. An overall PCI compliance status of FAILED indicates that at least one host in the report failed the PCI compliance requirements.

Host PCI Status

Each scanned host is listed by IP address. The host's security risk rating is equal to the highest severity level detected on the host, which determines whether the host passed or failed.

A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards, were detected on the host. A PCI compliance status of FAILED indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards, was detected on the host.

The sample PCI Status section below shows Overall PCI Status of PASSED.

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status.

Overall PCI Status		PASSED
--------------------	--	--------

Live IP Addresses Scanned	Security Risk Rating	PCI Status
10.10.10.47	0.0	PASSED

The sample PCI Status section below shows Overall PCI Status of FAILED.

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status.

Overall PCI Status		FAILED
--------------------	--	--------

Live IP Addresses Scanned	Security Risk Rating	PCI Status
10.10.10.1	4.0	FAILED
10.10.10.47	0.0	PASSED

IP Addresses Not Scanned	Security Risk Rating	PCI Status
10.10.10.10	Unknown	FAILED

A host is listed under “IP Addresses Not Scanned” when the current host status is Not Live or Not Current.

Not Live — A host is considered Not Live when it was specified as a target IP for a scan and it was not scanned because the service did not discover the host to be alive. The host may not be up and running and/or properly configured on the network with Internet access.

Not Current — A host is considered Not Current if it was not scanned during the best practice scanning period defined by the PCI compliance service.

See “Overall Compliance Status” for further explanation of these host status indicators.

Report Summary

This section appears in these reports: Scan Results Report, PCI Executive Report and PCI Technical Report.

A sample Report Summary for the Scan Results Report is shown below.

Report Summary	
Company:	Acme Sports
User:	Irina Rockster
Template Title:	Scan Results
Active Hosts:	1
Total Hosts:	1
Scan Type:	On Demand
Scan Status:	Finished
Scan Title:	My scan
Scan Date:	11/19/2007 at 19:23:43 (GMT)
Reference:	scan/1195500548.22214
Scanner Appliance:	10.10.21.23 (Scanner 4.8.41-1, Web 5.2.39-1, Vulnerability Signatures 1.18.106-1)
Duration:	00:06:43
Options:	Payment Card Industry (PCI) Options
Target:	10.10.10.1

The Report Summary for the PCI Executive Report and the PCI Technical Report are similar. A sample Report Summary for the PCI Executive Report is shown below.

Report Summary	
Company:	Acme Sports
Hosts In Account:	3
Hosts Scanned:	2
Hosts Active:	2
Report Date:	12/06/2007 at 00:37:42 (GMT)
Report Title:	
Template Title:	Payment Card Industry (PCI) Executive Report

Summary of Vulnerabilities

This section appears in all PCI reports.

The Summary of Vulnerabilities provides an overview of all vulnerabilities detected. The summary displays the total number of vulnerabilities detected for all scanned hosts, the average security risk and the number of vulnerabilities detected by severity level (1-5). Note the complete list of current vulnerabilities is included in the PCI Technical Report under Detailed Results.

Two bar graphs are also included to show the number of vulnerabilities and potential vulnerabilities detected by severity level.



Detailed Results

This section appears in these reports: Scan Results Report, Current Vulnerabilities Report, and PCI Technical Report.

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. Each scanned host is identified by its IP address and registered DNS hostname. For each host, a list of vulnerabilities (red), potential vulnerabilities (yellow) and information gathered (blue) appears.

The vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. The vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI compliance service found on the hosts. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

For each vulnerability detected, the service provides a description of the threat, the possible consequences if the vulnerability is exploited, and a verified solution to remediate the issue. Other details include the vulnerability severity level, category and industry reference numbers like CVE ID and Bugtraq ID as appropriate.

The following sample shows the start of the Detailed Results section. There were a total of 19 vulnerabilities detected on host IP 10.10.10.1. The first vulnerability shown in the list is QID 15019, which is classified as severity level 3 and CVSS Base score 7.0. This vulnerability is marked PCI FAILED and must be fixed to pass PCI compliance requirements.

Detailed Results

10.10.10.1 (bart.vuln.qa.qualys.com,-) Linux 2.4-2.6

Vulnerabilities Total	19	Security Risk	<div style="display: flex; justify-content: space-between;"> </div>	4.0	Compliance Status	❌ FAILED
-----------------------	----	---------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----	-------------------	--------------------------------------------------------------

Vulnerabilities (6)

■ ■ ■ □ 3 **DNS Zone Transfer Disclosing Private Network Mapping** port 53/top

QID: 15019 CVSS Base: 7.0 PCI FAILED ❌

Category: DNS and BIND CVSS Temporal: -

CVE ID: CVE-1999-0532

Vendor Reference: -

Bugtraq ID: -

Last Update: -

THREAT:
Intranet IP addresses (internal classes: 10.x.x.x, 172.16-31.x.x or 192.168.x.x.) were detected on this system.

IMPACT:
By viewing your private network addressing map, unauthorized users can obtain a list of targets they can use to access your private network servers. The more addresses there are, then the more likely it is that unauthorized users can compromise a network host.

SOLUTION:
Zone transfer should be restricted to the DNS servers. If you use a single DNS server, then you can simply disable this feature. In addition, you must install a split DNS, that is, use a dedicated DNS server within your private network.

Microsoft DNS Service users should refer to their manual. BIND users should consult the Internet Software Consortium's Web site.

RESULT:
10.20.30.95

■ ■ ■ □ 3 **DNS Zone Transfer** port 53/top

QID: 15018 CVSS Base: 7 PCI FAILED ❌

Category: DNS and BIND CVSS Temporal: 6.3

CVE ID: CVE-1999-0532

Appendices

This section appears in all PCI reports.

Several appendices are included at the end of your report to provide additional information like which hosts were scanned and not scanned, scan settings used and a report legend. The top portion of the Appendices section is shown below.

Appendices	
Hosts Scanned	
10.10.10.1, 10.10.10.47	
Option Profile	
Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off
Advanced	
Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Hosts Scanned

This appendix lists hosts that were successfully scanned.

Hosts Not Scanned

This appendix lists hosts that were not scanned because hosts were not “alive” at the time of the scan, meaning that they did not respond to probes sent by the scanning engine.

Option Profile

This appendix lists scan options and advanced options defined in the PCI option profile. Scan options affect how the service gathers information about target hosts during network security analysis, and how it performs vulnerability assessment. Advanced options affect how the service performs host discovery and how the service interacts with your firewall/IDS configuration.

Report Legend

Please review the Report Legend appendix in your report for detailed descriptions of the criteria used to determine the PCI status as well as the vulnerability severity levels, including vulnerabilities, potential vulnerabilities and information gathered.



PCI Questionnaires

The PCI Data Security Standard Self-Assessment Questionnaire 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).

The PCI DSS requires merchants to complete a PCI self-assessment questionnaire every 12 months. The due date is 12 months since the last submission date. The PCI self-assessment questionnaire is organized into sections based on the requirements outlined in the PCI Data Security Standard. Each section focuses on a specific area of security.

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”. Note the options “N/A” and “Compensating Controls” apply to questionnaire D only. If you respond to any question with “No”, then the questionnaire is not considered compliant.

New PCI DSS Self-Assessment Questionnaire (SAQ v1.1)

The PCI Security Standards Council recently introduced PCI DSS Self-Assessment Questionnaire version 1.1 with new guidelines and instructions. The new SAQ v1.1 defines 4 questionnaire versions for multiple SAQ validation types, as defined by the PCI DSS standards.

At this time, the PCI compliance service supports the new SAQ v1.1 concurrently with the SAQ v1.0 to prepare customers for the planned migration to the new SAQ v1.1.

Beginning **May 1st, 2008** the PCI compliance service requires merchants to manage questionnaires using the SAQ v1.1 standard. This means merchant users can create, edit and submit questionnaires following the SAQ v1.1 standard only. Any questionnaires stored in your account following the SAQ v1.0 standard are available for viewing in PDF format from the Saved Questionnaires list. See “Manage Questionnaires.”

To understand the PCI DSS Self-Assessment Questionnaire and compliance requirements for your organization, refer to the document *PCI DSS: Self-Assessment Questionnaire: Instructions and Guidelines Version 1.1* (dated February 2008). This document is published on the PCI Security Standards Council’s web site at:

<https://www.pcisecuritystandards.org/tech/saq.htm>

Questionnaire Versions (A-D)

The PCI Security Standards Council recently introduced PCI DSS Self-Assessment Questionnaire version 1.1 with new guidelines and instructions. There are now 4 PCI self-assessment questionnaire (SAQ) versions available, labeled A-D. You must select the appropriate questionnaire version for your organization to validate compliance with the PCI Data Security Standard.

Questionnaire D includes every requirement in the PCI Data Security Standard. Questionnaires A, B and C are shorter versions that only include requirements which are relevant to a particular type of organization, determined by how the organization stores, processes and transmits cardholder data. You must meet certain criteria to be eligible to complete one of the shorter versions of the questionnaire.

The Begin New Questionnaire page displays eligibility criteria for each questionnaire for your information. It's recommended that you refer to the PCI standards and documentation for guidance on selecting the appropriate questionnaire for your organization.

Complete information on eligibility for each questionnaire is available in the document *PCI DSS: Self-Assessment Questionnaire: Instructions and Guidelines Version 1.1* (dated February 2008), in the section "Selecting the SAQ and Attestation that Best Apply to Your Organization." This document is published on the PCI Security Standards Council's web site at:

<https://www.pcisecuritystandards.org/tech/saq.htm>

Complete a New Questionnaire

Go to Questionnaires—>New Questionnaire on the left menu. (Or click Complete a Questionnaire on the Home page.) The Begin New Questionnaire page appears.

Select the appropriate questionnaire version by clicking a questionnaire icon. See "Questionnaire Versions (A-D)" (above) for information on the questionnaire versions.

Your selected questionnaire appears online. The first page is a cover page where you can provide a title and organization information. The cover page is followed by the requirements from the PCI Data Security Standard that are relevant to the selected questionnaire. Each requirement includes one or more questions on a specific area of security. You must select a response for each question.

QUALYS GUARD® PCI

ON DEMAND SECURITY

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

Payment Card Industry Self-Assessment Questionnaire B 03/24/2008
Started: 03/24/2008 Last Edited: 03/24/2008 Due Date: 03/19/2009

Requirement 3
Requirement 4
Requirement 7
Requirement 9
Requirement 12

Title

Questionnaire Title: Acme Sports Questionnaire

Organization Information

DBA(s): Josh Stilles

Contact Name: Irina Rockster

Approximate number of transactions/accounts handled per year:

Brief Description of Business & Locations:

Third Party Service Providers

Save Draft Submit Final Cancel

© 2008 Qualys, Inc. [Privacy Policy](#)

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)

Review organization information and modify if needed. The text fields are pre-populated with organization information saved in your account settings, and the Contact Name menu shows 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. When you submit the questionnaire to acquiring banks, the organization information fields and the contact name appear on page 2 of the submitted questionnaire. (Note that the primary contact defined for the account appears on the cover page of the questionnaire.)

To overwrite account settings with your changes, select the check box “Update Account Information with changes made above” before saving the questionnaire. All organization information fields are updated in your account settings, and the user selected in the Contact Name menu becomes the new primary contact for the account.

Requirement Sections 1-12

The questionnaire is organized into multiple sections 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. 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”. Note the options “N/A” and “Compensating Controls” apply to questionnaire D only. If you respond to any question with “No”, then the questionnaire is not considered compliant. See “Compensating Controls Definition” for more information.

The PCI Security Standards Council provides guidance and instructions for meeting compliance with questionnaire D. See “Questionnaire D Guidance” for information on exceptions and using compensating controls. For requirement 3.4, see “Compensating Controls for Requirement 3.4” for guidance on using compensating controls for this particular requirement, as provided by the PCI Council.

QUALYS GUARD® PCI

ON DEMAND SECURITY

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

Payment Card Industry Self-Assessment Questionnaire B **03/24/2008**

Started: 03/24/2008 Last Edited: 03/24/2008 Due Date: 03/19/2009

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Description	Response
3.2 Do all systems adhere to the following requirements regarding storage of sensitive authentication data? More Information Comments	<input type="radio"/> Yes <input type="radio"/> No
3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i> More Information Comments	<input type="radio"/> Yes <input type="radio"/> No

[Save Draft](#) [Submit Final](#) [Cancel](#)

© 2008 Qualys, Inc. [Privacy Policy](#)

More Information

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

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.

Specific information is required in the comments section when “Compensating Controls” is selected in questionnaire D. See “Compensating Controls Comments” for a description of required comments.

Save Questionnaire

When editing a questionnaire there are 2 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 "Manage 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.

Questionnaire D Guidance

The PCI Security Standards Council provides the following guidance and instructions for meeting compliance using questionnaire D:

- Guidance for Exclusions
- Compensating Controls Definition
- Compensating Controls for Requirement 3.4
- Compensating Controls Comments

Guidance for Exclusions

The PCI Council provides this guidance for exclusions.

"If you are required to answer SAQ D to validate your PCI DSS compliance, the following exceptions may be considered:

- *The questions specific to wireless only need to be answered if wireless is present anywhere in your network (Requirements 1.3.8, 2.1.1, and 4.1.1). Note that Requirement 11.1 (use of wireless analyzer) must still be answered even if wireless is not in your network, since the analyzer detects any rogue or unauthorized devices that may have been added without the merchant's knowledge.*
- *The questions specific to custom applications and code (Requirements 6.3-6.5) only need to be answered if your organization writes its own custom web applications.*
- *The questions specific to data centers (Requirements 9.1-9.4), only need to be answered if you have a dedicated data center or server room. A data center is defined by PCI SSC as a dedicated, physically secure room or structure where information technology infrastructure (application servers, database servers, web servers, and/or network devices) is centrally housed, whose main purpose is to store, process, or transmit cardholder data. "Data center" may be synonymous with server room, network operations center (NOC), and co-location facilities at an ISP or hosting provider."*

The excerpt above is from the PCI Council in the document *PCI DSS: Self-Assessment Questionnaire D and Attestation of Compliance Version 1.1* (dated February 2008) This document is available for download from the PCI Security Standards web site at:

<https://www.pcisecuritystandards.org/tech/instructions.htm>

Click D in the summary table for SAQ D. Then go to the section “Guidance for Exclusion of Certain, Specific Requirements.”

Compensating Controls Definition

Compensating Controls may be selected in responses to questionnaire D.

The PCI Security Standards Council defines Compensating Controls as follows.

“Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.”

The definition above is from the document *PCI DSS: Glossary, Abbreviations and Acronyms*. This document is published on the PCI Security Standards Council's web site at:

https://www.pcisecuritystandards.org/tech/supporting_documents.htm

Additional information on using compensating controls is available in the document *PCI DSS: Self-Assessment Questionnaire: Instructions and Guidelines Version 1.1* (dated February 2008), in the section “General Tips and Strategies to Prepare for Compliance Validation.” This document is published on the PCI Security Standards Council's web site at:

<https://www.pcisecuritystandards.org/tech/saq.htm>

Compensating Controls for Requirement 3.4

The PCI Council provides the following guidance for using compensating controls when companies are unable to render cardholder data unreadable per questionnaire D requirement 3.4.

“For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the “Compensating Controls” definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet all of the following conditions:

- 1 *Provide additional segmentation/abstraction (for example, at the network-layer).*
- 2 *Provide ability to restrict access to cardholder data or databases based on the following criteria: IP address/Mac address, application/service, user accounts/groups, data type (packet filtering).*
- 3 *Restrict logical access to the database. Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP).*
- 4 *Prevent/detect common application or database attacks (for example, SQL injection)."*

The excerpt above is from the PCI Council in the document *PCI DSS: Self-Assessment Questionnaire D and Attestation of Compliance Version 1.1* (dated February 2008). This document is available for download from the PCI Security Standards web site at:

<https://www.pcisecuritystandards.org/tech/instructions.htm>

Click D in the summary table for SAQ D. Then go to the section "Compensating Controls for Requirement 3.4."

Compensating Controls Comments

The PCI Council requires additional information when compensating controls are used. This information must be supplied in the "Comments" field when you select "Compensating Controls" for a requirement in questionnaire D.

- 1 *Constraints: List constraints precluding compliance with the original document.*
- 2 *Objective: Define the objective of the original control; identify the objective met by the compensating control.*
- 3 *Identified Risk: Identify any additional risk posed by the lack of the original control.*
- 4 *Definition of Compensating Controls: Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.*

The requirements above are excerpted from the PCI Council in the document *PCI DSS: Self-Assessment Questionnaire D and Attestation of Compliance Version 1.1* (dated February 2008). This document is available for download from the PCI Security Standards web site at:

<https://www.pcisecuritystandards.org/tech/instructions.htm>

Click D in the summary table for SAQ D. Then go to the section "Compensating Controls Worksheet."

Manage 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.

QUALYS GUARD® PCI ON DEMAND SECURITY

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

Home
Network
└ New Scan
└ Scheduled Scans
└ Scan Results
└ Vulnerabilities
└ Compliance Status
└ Submitted Reports
└ False Positive History
Questionnaires
└ Saved Questionnaires
└ New Questionnaire
Account
└ Settings
└ IP Assets
└ Users
Contact Support
Resources

Last Submitted Questionnaire

Status: Not Compliant **Submitted:** Never Compliant **Next Due:** Never Compliant

Saved Questionnaires

Delete [New](#) [Search](#) 1 - 1 of 1

<input type="checkbox"/>	View	Edit	Submit	Title	Status	First Name	Last Name	Updated	Submitted
<input type="checkbox"/>			Submit	Acme Sports Questionnaire		Irina	Rockster	12/04/2007	N/A
<input type="checkbox"/>	View	Edit	Submit	Title	Status	First Name	Last Name	Updated	Submitted

© 2008 Qualys, Inc. [Privacy Policy](#)

Do any of the following from the Saved Questionnaires list:

- Submit a questionnaire to your acquiring banks
- Edit a questionnaire in progress
- View/Download a questionnaire in PDF format
- Start a new questionnaire
- Delete a non-submitted questionnaire
- Search for questionnaires by user name, compliance status, last update date or submission date

Important! Beginning **May 1st, 2008** the PCI compliance service requires merchants to manage questionnaires following the SAQ v1.1 standard. Editing and submitting questionnaires following the SAQ v1.0 standard is not supported. Any questionnaires stored in your account following the SAQ v1.0 standard are available for viewing in PDF format.

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, go to Questionnaires—>Saved Questionnaires on the left menu. Identify the questionnaire you want to submit and click the Submit link in the Submit column. Only a questionnaire following the SAQ v1.1 standard may be submitted. (Note that if N/A appears in the Submit column, then the questionnaire is not complete and cannot be submitted. Edit the questionnaire to finish it.)

The Submit Questionnaire page appears.

Review the questionnaire status and bank information on the screen, provide section comments, and review the list of banks in your account.

Questionnaire Status

Title: Acme Sports Questionnaire
 Last Updated: 03/24/2008 at 15:31:45 (GMT -07)
 Status: ✔
 Yes ✔: 25
 N/A ✔: 0
 No ⊖: 0

Section Comments

Section Number	Description	Status	Remediation date and plan OR comment
3	Protect stored cardholder data	✔	
4	Encrypt transmission of cardholder data and sensitive information across public networks	✔	
7	Restrict access to data by business need-to-know	✔	

© 2008 Qualys, Inc. [Privacy Policy](#)

Questionnaire Status

The overall questionnaire status is shown, including the questionnaire title, the date the questionnaire was last updated, the compliance status, and the number of questions with a Yes, N/A, No, and Compensating Controls response. Keep in mind that to be compliant with the self-assessment portion of the PCI Data Security Standard, you cannot have a “No” response in the questionnaire. Note that a compensating controls response is valid only in questionnaire D. See “Questionnaire D Guidance” for guidance and instructions for completing questionnaire D.

Section Comments

Each section of the questionnaire represents a single requirement from the PCI Data Security Standard. Each section is listed with the requirement number and description, and the compliance status for the requirement. A check mark (✔) indicates that you are compliant with the requirement. A dash (⊖) indicates that you are not compliant with the requirement. You are not compliant with a requirement when at least one question in the section was answered “No”.

Section comments are mandatory if a requirement is not compliant. In this case, it is recommended that you provide a remediation plan and the expected remediation date in the section comments field for the requirement. The section comments will appear in the submitted questionnaire.

Banks in Account

The banks defined for your account are listed. These banks are signed up with the PCI compliance service and can log into the service to view your submitted questionnaire online. If you do not have a bank listed, then no bank will have online access to your submitted questionnaire. You must download the submitted questionnaire in PDF format and manually send it to your acquiring bank using a method outside of the application.

Confirmations and Acknowledgements

Certify that you are eligible to perform and have performed the appropriate questionnaire for your organization. Electronically sign the questionnaire and click Submit to complete the process.

The screenshot shows a web form titled "Eligibility to Complete Questionnaire". It contains three main sections:

- Eligibility to Complete Questionnaire:** A list of three bullet points: "Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data over either a phone line or the Internet", "Merchant retains only paper reports or paper copies of receipts", and "Merchant does not store any cardholder data in electronic format". Below the list is a checked checkbox with the text "I certify eligibility to complete this shortened version of the Questionnaire based on ALL of the above."
- Confirmation of Status:** A list of five bullet points regarding PCI DSS compliance, including completion of the Self-Assessment Questionnaire B, accuracy of information, and adherence to PCI DSS requirements. Below the list is a checked checkbox with the text "I confirm ALL of the above."
- Acknowledge and Sign:** A section with the instruction "Please enter the following information to electronically sign your submission. By entering the following details, you certify that you are authorized to perform this assessment." It contains three input fields: "Executive Officer Name" (filled with "John Smith"), "Executive Officer Title" (filled with "CEO"), and "Executive Officer Company Name" (filled with "Acme Sports").

At the bottom of the form are "Submit" and "Cancel" buttons.

Eligibility to Complete Questionnaire — This section appears for questionnaire versions A-C. Click the check box “I certify eligibility to complete this shortened version of the Questionnaire based on ALL of the above.”

Confirmation of Status — Review your PCI compliance status and then select the check box “I confirm ALL of the above.”

Acknowledge and Sign — Electronically sign your submission by providing this information: Executive Officer Name, Executive Officer Title, and Executive Officer Company Name.

After you click Submit, these updates take place automatically:

- 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.)

- The questionnaire is saved on the Saved Questionnaires list where you can download the questionnaire in PDF format.
- On the Home page, a check mark (✔) appears next to Questionnaire to indicate that you are compliant with the self-assessment portion of the PCI Data Security Standard.