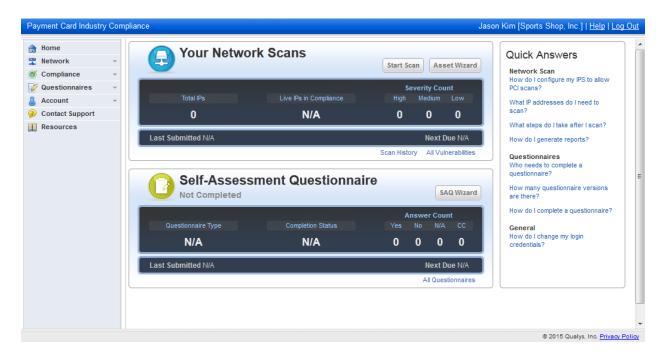


# **PCI Compliance**

### **Getting Started Guide**

Qualys PCI provides businesses, merchants and online service providers with the easiest, most cost effective and highly automated way to achieve compliance with the Payment Card Industry Data Security Standard (PCI DSS). This standard provides organizations with the guidance needed to ensure that credit cardholder information is kept secure from possible security breaches.

Qualys PCI is the most accurate and easiest to use tool for PCI compliance testing and reporting for certification. Qualys is an Approved Scanning Vendor (ASV).



## **Network Scanning**

Per PCI DSS v3.0 requirement 11.2.2, merchants are required to perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV). Every part of cardholder data system components needs to be scanned. Using the PCI module you can meet the external network scans requirement.

You are responsible for adding IP assets to your PCI account for all in-scope infrastructure for the PCI DSS external network scan requirement. To see the IP assets in your account go to Account > IP Assets. You can add IP addresses up to the total IPs purchased.

### **Check Scanner IP Addresses Before Scanning**

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

The scanner IPs are: 64.39.96.0/20 (64.39.96.1-64.39.111.254)

### **Define Your In-Scope Infrastructure**

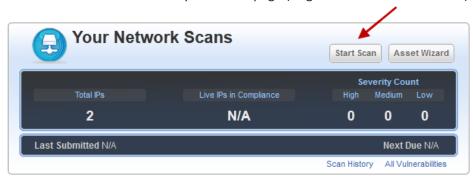
Click the Asset Wizard button on your Home page (or go to Account > IP Assets and select the wizard). The wizard helps you define the in-scope infrastructure for the external network scan. You must add to your account all Internet-facing IP addresses and/or ranges. If you have domains that host in-scope PCI infrastructure you need to add these domains to your account.



Important! The wizard prompts you to confirm scans can be performed without interference. The service provides multiple scanners for external (perimeter) scanning and lists the scanner IP addresses. Depending on your network, it may be necessary to add the scanner IPs to your list of trusted IPs.

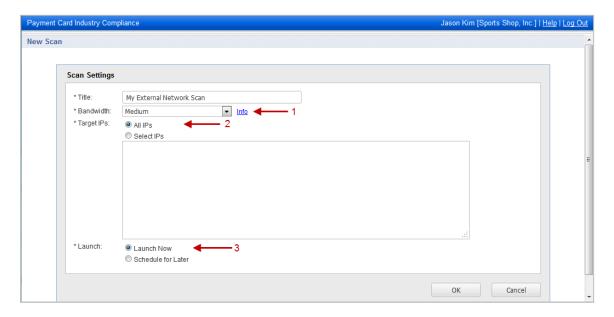
### Start an External Network Scan

Click the Start Scan button on your Home page (or go to Network > New Scan).

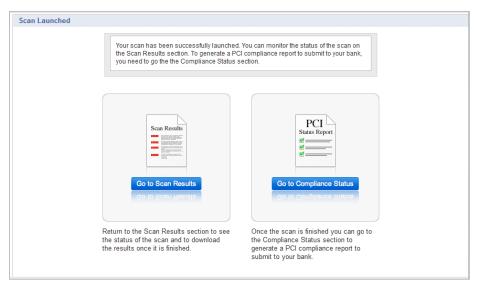


Tip – You may have already run an external PCI network scan using Qualys VM and then shared this scan with the PCI module. In this case you're ready to run reports and complete certification steps. Jump ahead to the section "Create Network Reports for Certification" later in this document.

Next you'll see the New Scan page. Select your scan settings and click OK.

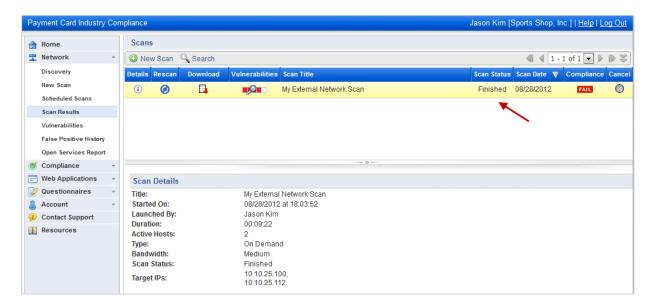


- 1) The bandwidth represents a set of scan performance settings. We recommend Medium to get started. Click the Info link to understand the settings.
- 2) Choose to scan All IPs in your account or just certain IPs. Tip To meet PCI compliance all the IPs in your account must be scanned and there can be no detected PCI vulnerabilities on any IPs. If you have a large number of IPs that must be compliant, you may want to scan a few IPs at a time to help you with the remediation process.
- 3) You can schedule the scan to run later or on a regular basis daily, weekly or monthly. We recommend you set up a schedule so you'll receive vulnerability scan results on an ongoing basis.



Once the scan is launched you can monitor the scan progress by going to Scan Results.

The scan status will be Running while the service is performing vulnerability testing. Once the status is Finished you'll see the overall PCI compliance of the scan as PASS or FAIL, and you can view detected vulnerabilities in your scan results. Just click (Download) to download your results in PDF format.



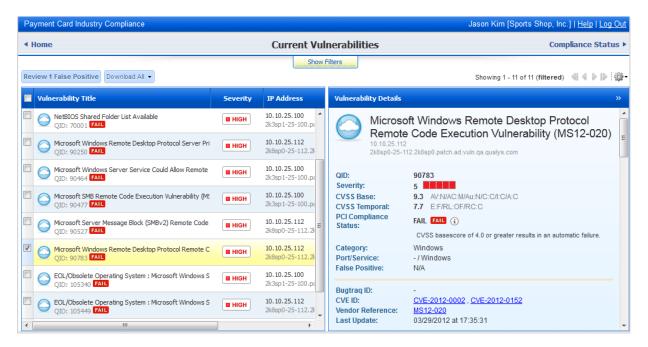
What does the scan status Importing mean? Importing means a user requested to share an external PCI network scan using the VM module and the service is importing this scan. Once complete, the status will change to Finished and any of the scanned IPs not already in your PCI account will be added.

### View Current Vulnerabilities and Fix

Go to your scans list and click to view the current vulnerabilities for your scan. You'll see filters for helping you to find vulnerabilities you're interested in. To find the detected vulnerabilities that are causing you to fail PCI compliance click the check box "Display only PCI Fail Vulnerabilities".

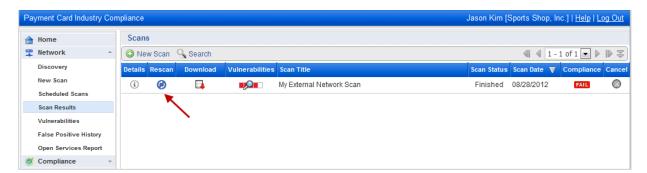


For each vulnerability in your scan results the PCI compliance status is marked as PASS or FAIL, and you'll find a detailed description of the issue along with a verified solution from our security experts. Select a vulnerability from the list and view the detection details on the right. Next to PCI Compliance Status click (1) (Information) to see the reasons for passing or failing PCI compliance.



### Rescan to Verify Vulnerabilities are Fixed

Fix vulnerabilities and then rescan to validate that systems are no longer vulnerable. You can rescan as often as necessary to track your remediation progress. Tip – Click next to your scan to re-run your scan without having to enter your scan settings again.



### **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 case, 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:

- 1) Work with your system administrator to fix all vulnerabilities in your scan results using the recommended solutions. A custom solution is provided for each detected vulnerability.
- 2) Before you submit a false positive, be sure to fix all vulnerabilities except the false positive issues. Your last rescan should show only the false positive issues.

If you believe that the PCI compliance service has identified a false positive in your scan, submit your false positive request by going to Network > Vulnerabilities. Select the check box next to vulnerabilities you want to submit and then click "Review False Positives". A Technical Support representatives will work with you to confirm the issue is indeed a false positive. Once approved, the false positive is approved for 90 days and this will not appear in your vulnerabilities list or your reports.

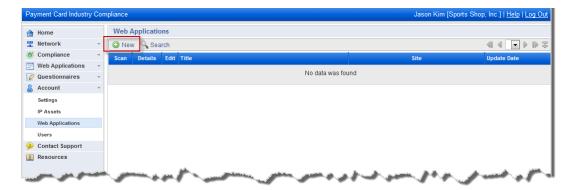
### **Secure Web Applications**

Per PCI DSS v3.0 requirement 6.6, merchants are required to perform scans of public-facing web applications and review detected vulnerabilities. Using the PCI module you can meet the web application scans requirement. Note that web application scanning is available when this option is turned on for your subscription. Please contact your Account Manager or our Support Team if you would like to use this option.

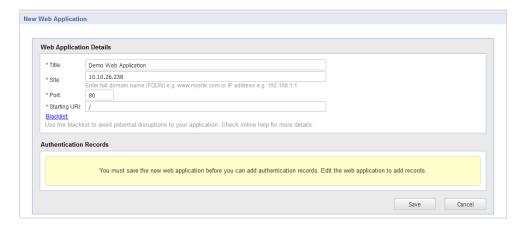
You are responsible for adding web applications to your PCI account for all in-scope applications for the PCI DSS requirement. To see the IP assets in your account go to Account > Web Applications. You can add web applications up to the total applications purchased.

### **Add Your Web Application**

To add a web application to your account, go to Account > Web Applications and click the New link.



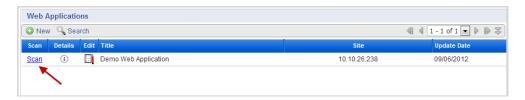
Enter the web application settings and click Save. Tip – Click Help on the top menu bar for guidance.



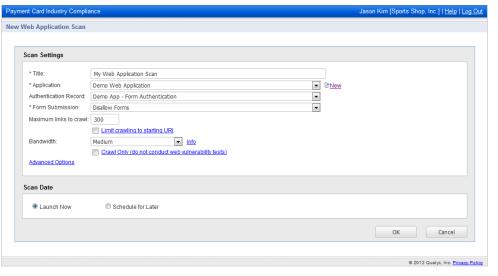
What are authentication records? Authentication to HTML forms is optional but may be required to scan your web application. These authentication techniques are supported: HTTP Basic server-based authentication and simple form authentication. If authentication to the web application is required add one or more authentication records by editing the web application.

### Start a Web Application Scan

On the web applications list, click the Scan link next to your web application. (Or you can go to Web Applications > Scans and click New Scan.)



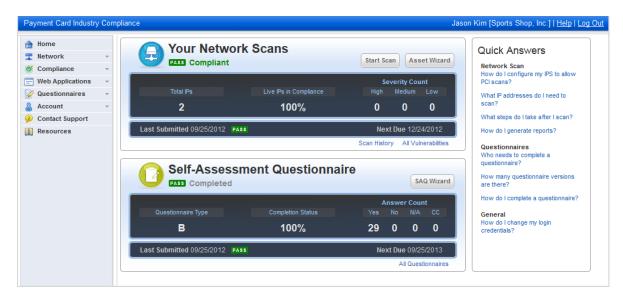
Choose your scan settings. Want to use authentication? Select an authentication record already defined for your web application. Then click OK to start the scan.



Your scan will appear under Web Applications > Scan Results where you can track its progress and download the results.

### **Submit Compliance Status**

Your Home page shows your PCI compliance status. Your Network Scans will be marked as page when you are compliant with the quarterly external network scans requirement. (Self-Assessment Questionnaire shows status of v2 questionnaires, if any.)



### **Create Reports for Certification**

You are ready to create network reports when the Compliance Status shows that the number of hosts in your account matches the number of hosts that are compliant. In the example below there are 2 hosts in the account and 2 hosts that are compliant.



To create your reports, click Generate (under Actions) and simply follow the steps in the report generation wizard. Your reports will appear on the submitted reports list.

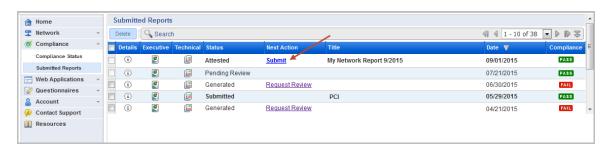
#### Next steps:

- 1) Preview the reports online in PDF format for completeness and accuracy.
- 2) Request a review from your Approved Scanning Vendor (ASV) using the report wizard or from the submitted reports list. You will receive an email with the review status (approved or rejected).
- 3) Once approved by the ASV, the report is considered certified and can be submitted to your acquiring banks for PCI certification.

### **Auto-Submit to Acquiring Banks**

The Qualys PCI auto-submission feature allows you to submit compliance status directly to your acquiring banks. Entering your bank and merchant IDs in your "Account Settings" activates the auto-submission feature. You can also download PCI compliance reports in PDF to submit to your acquiring bank(s) or use to assist in remediation efforts.

Go to Compliance > Submitted Reports and click the Submit link.



#### **PCI Bank Service**

We offer our PCI Bank service to acquiring banks. When your bank has signed up you can submit your compliance status to them directly, without having to send it manually via email or other means. A bank representative gets a PCI Bank account and logs in to our PCI Bank application where they get a view of your compliance status and direct access to your submitted reports.



**View merchant details** like the current compliance status, and the last date when the scan report was submitted for certification. Only the final, submitted scan report is visible to bank users. Scans and remediation efforts that are in progress are not visible.

**Download PCI network reports** in PDF format from the preview pane. Merchants can no longer submit questionnaires online; the latest questionnaires are not visible to bank users.

Can a bank user log in to a merchant account? No, bank users do not have access to merchant accounts.

# **Looking for More Information?**

Check out these references to help you meet PCI Compliance requirements.

Qualys Community: How to Satisfy the New PCI Internal Scanning Requirements https://community.qualys.com/docs/DOC-3923

PCI Security Standard Council

https://www.pcisecuritystandards.org/

PCI Data Security Standards

https://www.pcisecuritystandards.org/security\_standards/index.php

PCI DSS: Self-Assessment Questionnaire

https://www.pcisecuritystandards.org/merchants/self\_assessment\_form.php

**PCI Security Standards Documents** 

https://www.pcisecuritystandards.org/security\_standards/documents.php