Scan Management System Guide

Contents

1. PCI DSS Scan Requirements

If your business has externally facing IP addresses connected to your card data environment, as well as completing an annual Self-Assessment Questionnaire or Report on Compliance, you must also provide a quarterly compliant PCI DSS Vulnerability Scan. This scan must be run using a software solution provided by an Approved Scanning Vendor (ASV) and the scan results must be attested by you the merchant, and an agent of the ASV.

Sysnet Global Solutions is an Approved Scanning Vendor (ASV) and our Scan Management System has been designed to help you to complete this task. Our Scan Management System will guide you through scheduling your scan, interpreting the results, attestation of your scan results and finally reporting those results so that your PCI compliance status is updated in the compliance portal. This document will help you through each step of the process.

2. Getting Started

2.1 What steps do I need to take within the Scan Management System?

Firstly you must set up a scan schedule. Once your scan is complete and returns a passing result, you must attest to the scan result. When you have attested your scan results, Sysnet Global Solutions as the Approved Scanning Vendor must also attest to the results. When this final step is completed your official certified scan reports will be made available and your scan results will automatically update your overall PCI Scan Compliance in the compliance portal.

If you do not receive a passing scan result, the Scan Management System will help you to remediate any failures so that you can complete all necessary resolution steps.

2.2 Navigating Scan Management System

Dashboard

You can navigate to your dashboard at any time to view the current status of your scans and their corresponding results if available. You can also choose to edit or cancel the scan if it has not yet commenced, or action the scan if the result has been received, by clicking the “Review Scan” button beside each scan.

Setup a Scan

This section will allow you to set up and schedule a scan of your PCI DSS in-scope IP addresses or domains.

Manage My Domain/IP List

In this section you can set up a default master list of IP addresses or domains to be included in the next scan. This is useful if you have IP addresses or domains that move in and out of scope for PCI scanning, or if you want to set up a default list for scanning so that you do not need to add the IP addresses/domains each time you schedule a scan.

Contact PCI Helpdesk

If you have a question for the scanning help desk you can submit it in this section and they will respond to you by either phone or email.

2.3 Setup & Schedule Your Scan

Take these steps to set up a scan schedule:

- Click “Setup a scan” from the dashboard menu.
- Enter the domain or IP that you want to scan and Click “Add”. Continue to add in domains/IP addresses until you have entered all details that you wish to scan.(Note: the system will automatically present the default set of IP/Domains maintained in the “Manage My Domain/IP list” page).
- Enter a date and time on which you wish the scan to run.
- Specify if Load Balancers are in scope.
- You will need to verify that your system will allow Sysnet’s IPs access to complete the scan. Please make sure that any active protection (including Intrusion Prevention System) is either disabled, or that Sysnet’s scanners are white-listed throughout duration of the test.
- Read the Website Disclaimer and confirm that you will allow access to Sysnet to scan your system.
- Click “Schedule this scan”.

Congratulations, you have just scheduled your scan!

Note: You can only schedule one scan at a time.

2.4 Retrieving Your Scan Results

You will receive an email to the email address specified on the compliance portal, notifying you of when your scan results are available for review. You can then log in as normal to the compliance portal, navigate to “Scan>Sysnet Scan Management System” on the compliance portal. You will be brought to your Scan Management System dashboard where you can view the results of your scan.

2.5 Interpreting Your Scan Results

Your scan results will be displayed on the dashboard. The details displayed under “Status” and “Results” will allow you to interpret the results of your scan:

Scan Status

My scan’s status	What does it mean?
Scheduled	The scan has been scheduled but has not yet started.
Running	The scan is currently running.
Aborted	The scan process did not complete.
Review	The scan results have been received and require your review before you can attest.
Complete	The scan has completed but is not ready to be attested as it requires your attention. This may be due failing vulnerabilities.

Contest	You have raised one or more False Positive Requests against failing vulnerabilities. These requests are pending review by the Approved Scanning Vendor.
Merchant Attested	You have validated the scan but it is pending validation from the Approved Scanning Vendor.
Attested	The scan result has been attested by both you the scan customer, and the Approved Scanning Vendor. The report is now final and unalterable for the scan period. The results will affect your PCI compliance.

Scan Results

My scan's results	What does it mean?
Pending	The scan has either been scheduled but not yet started, or is currently running and the results have not yet been received.
Pass	The scan has passed. Either no failing vulnerabilities were found, or if this is a re-scan, previous vulnerabilities have been approved by the Approved Scanning Vendor.
Fail	PCI Failing Vulnerabilities have been found in your scan. Alternatively vulnerabilities were found in a previously run scan and were approved by the Approved Scanning Vendor, but the approval period has now expired.
False Positive Approved	Your scan failed due to PCI vulnerabilities which were presented to the Approved Scanning Vendor for review. The Approved Scanning Vendor has approved the vulnerabilities so that the scan can be marked as passed.
False Positive Rejected	Your scan failed due to PCI vulnerabilities which were presented to the Approved Scanning Vendor for review. The Approved Scanning Vendor has rejected the request for approval and the scan remains in a failed status.

Scanning Reports

The Scan Management System will produce three reports:

1. PCI Vulnerability Report
   This draft report or working document outlines the overall initial results of your scan so that you can review and take action if necessary.

   This report will be made available for download under the "Review Scan>Status" page after your scan has completed.

2. PCI DSS Scan Report Executive Summary
   This report is an official document and provides an overall summary of the results of your scan by host and by vulnerability. It is only available when your scan has been attested by both you as the scan customer and Sysnet Global Solutions as the Approved Scanning Vendor.

This report will be made available for download under the “Review Scan>Status” page after your scan has been attested by the ASV.

3. PCI DSS Scan Report Technical Details
   This report is an official document and provides an overall summary of the results of your scan by host and by vulnerability, plus any remediation details that were created during the scan process. It is only available when your scan has been attested by both you as the scan customer and Sysnet Global Solutions as the Approved Scanning Vendor.

   This report will be made available for download under the “Review Scan>Status” page after your scan has been attested by the ASV.

2.6 Managing Passing Scans

Once your scan has passed, your next step is to attest or validate the results. You can do this by clicking the “Review Scan” button on the dashboard next to the scan results.

Your Scan Status will be displayed including tabs relating to Related Hosts, Vulnerabilities and Special Notes that were raised as part of the scan. These will be marked in red when they require your action, amber when they are partially resolved and finally green once completely resolved. You must ensure that if you have any of these three items, you resolve them (they will be marked as green once resolved) before you can proceed to Attest to your scan.

If Related Hosts, Vulnerabilities and Special notes have not been created as part of your scan result, your next step is to Attest to your scan.

2.7 Managing Discovered/Related Hosts

If a discovered/related host is identified during your scan the “Related Hosts” tab will be displayed to you when you click “Review Scan”.

Related Hosts which need your attention will be marked in red. Once you have resolved the outstanding task pertaining to Related Hosts it will turn to green and you can proceed with your next step.

A Related Host is an IP or domain that is discovered during the scanning process to be in the same domain as the original target of the scan. These hosts may or may not be connected to your card data environment and as a result you must confirm if they are in scope for the scan. Examples of related hosts can include the mail exchange for the primary scan target’s domain, or perhaps the host has a DNS address record for the same domain as the primary target.

If you determine that the discovered related hosts are in scope, you must add the details of the related hosts to the original set of IP addresses or domains you scanned and then re-schedule the scan to run again.

If you determine that the discovered related hosts are not in scope, you must confirm this on screen. Details relating to the hosts will be added to your scan report with the statement that the scan customer (you) have confirmed they are out of scope.

2.8 Managing Failing Vulnerabilities

If your scan result is failed, PCI Failing Vulnerabilities have been found. You will be able to view Vulnerabilities by clicking “Review Scan” on the dashboard. Any vulnerability that requires action will be highlighted in red. Full details of these vulnerabilities will be included in the PCI Vulnerability Report that will be made available to you for download. You must fix each of the vulnerabilities listed and re-schedule your scan.

Alternatively if you disagree with the findings of the scan, you can raise a False Positive Request with the Approved Scanning Vendor. You may decide to dispute the results based on a number of factors including for example:

- Vulnerabilities which are incorrectly found
- Vulnerabilities that have a disputed CVSS score
- Vulnerabilities for which a compensating control is in place
- Report exceptions
- Report conclusions
- Some components may be out of scope

You can raise a False Positive request for each individual vulnerability by clicking the “Raise False Positive” link on the “Review Scan>Vulnerabilities” page. A pop up window will appear and you can add in details here about why you want to contest the result and then click “Submit”. The status of the request will be marked as “Submitted”. These details will be then passed to Sysnet Global Solutions for review.

You will receive an email notification once your request has been reviewed. Log into the Scan Management System, click “Review Scan” and choose the “Vulnerabilities” tab. You will see the outcome of your request beside the relevant vulnerability. Sysnet Global Solutions will either Accept or Reject the False Positive requests. You may need to raise multiple false positive requests depending on the number of vulnerabilities found and how many you wish to dispute. From time to time Sysnet may require additional information from you relating to your request. You will receive an email notifying of you of this and prompting you to log into the Scan Management System to view the current status.

You will receive an email notification when False Positive requests are accepted. Where False Positive requests are accepted, Sysnet will approve the scan and the Technical Scan Report will include details of Sysnet's conclusions with references to any supporting evidence under 'Exceptions, False Positives, or Compensating Controls Appendix B of Executive Summary’, or as an appendix to the report.

Where a request is Rejected, you must resolve any failing vulnerabilities and re-run the scan until a passing scan is achieved.

Once all vulnerabilities are resolved the Vulnerability tab will change to green on the Review Scan page.

2.9 Managing Special Notes

Special Notes are created and attached to your scan results if the scan has detected issues which while they are not vulnerabilities, still need review and confirmation.
Special Notes will be visible when you click Review Scan. The Special Notes tab will be marked in red if one or more still need to be resolved. Once all Special Notes are resolved the tab will be marked in green.

2.10 Attesting To Scan Results

Once your scan is ready for attestation a "Confirm and Attest Scan" button will appear on the "Review Scan" page. If Related Hosts, Vulnerabilities or Special Notes were applicable to your scan, each of the relevant tabs will be marked in green if no further action is required from you. Click "Confirm and Attest Scan". A pop up with attestation statements will appear on screen. Once you are happy to confirm the statements that are presented to you, click "OK". The overall status of your scan will update to "Merchant Attested". It will now be passed to Sysnet Global Solutions as the Approved Scanning Vendor for attestation. Once this final step is completed your overall scan status will update to "Attested". The results will be passed into the compliance portal and your PCI scan status on the compliance portal will update to "Compliant".

2.11 Scheduling Quarterly Scans

You are required to supply a quarterly compliant external vulnerability scan. Once you schedule a scan you will receive reminder emails from the Scan Management System to advise you of when your next scan is due (usually 7 days from the date of the email).

3. Frequently Asked Questions

3.1 How do I know I have a scan requirement?

If your business has externally facing IP addresses that connect to your card data environment, you have a scan requirement. Simply put, if your card processing systems have externally facing IP addresses, you have a scan requirement.

3.2 How often do I need to run a scan?

At a minimum you must run a compliant scan and report the results once a quarter. You must also run a scan anytime there is significant change in your card data environment even if this is in between your usual quarterly scans.

3.3 What is an ASV?

An ASV is an Approved Scanning Vendor, an organisation that validates adherence to PCI DSS requirements by performing vulnerability scans of internet facing environments. Sysnet Global Solutions is an ASV. The Scan Management System is the software used by Sysnet to run PCI external vulnerability scans in adherence with the requirements of the PCI Council.

3.4 What is the difference between a Network Vulnerability Scan and a PCI DSS Vulnerability Scan?

Both scans are external vulnerability scans however a PCI DSS scan has additional steps as it is reviewed by and must be approved by an Approved Scanning Vendor, before it is deemed compliant. Only PCI DSS Vulnerability Scans will affect your PCI DSS Compliance.

3.5 What are Load Balancers?

Load balancers are devices in front of your application server that manage requests to your application so that congestion is reduced, throughput is maximised and response times are minimised.

When load balancers are used, the scan may only be able to see part of the configuration. You must confirm that configuration behind the load balancers is synchronised, otherwise a special note will be applied to the executive summary report.

3.6 How long does a scan take to run?

The average length is one hour but it may take less or more time depending on the number of IPs or domains being scanned.

3.7 My scan results say "Pass" but my PCI Scan Compliance Status has not updated. What do I do?

First you must check your scan status on the dashboard. If the scan status equals "Review" you must review the details including any Special Notes or Related Hosts, and then attest. Once you have attested the scan will automatically be passed to Sysnet Global Solutions for attestation.

If the scan status equals "Complete", the scan has finished but there are failing vulnerabilities. Navigate to the dashboard in the Scan Management System and click "Review Scan" beside the scan in question. The Review Scan page will open. The Vulnerabilities tab will be marked in red. Go to the relevant section and follow the instructions outlined.

If the scan status equals "Contest", you had previously raised false positive requests for the scan which are pending review by Sysnet Global Solutions. You cannot proceed until the results of Sysnet's review are received (either approved or rejected). If your request is rejected you must remediate and re-run the scan until it is passing.

If the scan status equals "Merchant Attested", the next step is for Sysnet Global Solutions to attest to your scan. Once this is completed the overall status will change to "Attested" and your scan results will automatically update your PCI Scan Compliance in the compliance portal after 15 minutes.

If your question is not answered by the above, please feel free to contact the PCI Help Desk to request further assistance.