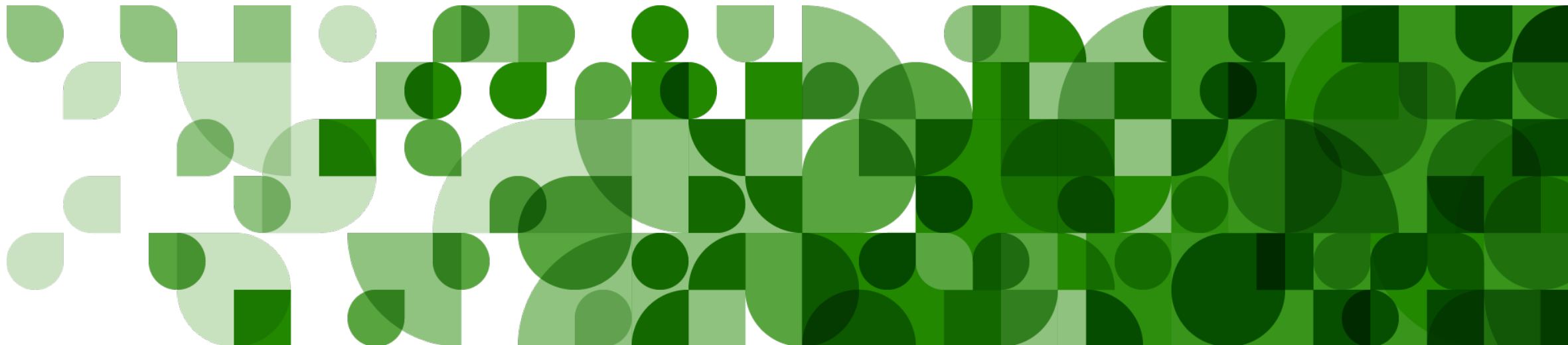


# Getting Started with Cardpointe PCI Compliance



# Registration - Two Steps

- You will receive two separate emails containing your username and a link to set your password respectively.

### Secure your business and your customers' data.

Through your relationship with CardConnect, you have been pre-registered for your customized CardPointe account – the industry's leading data security and compliance certification program.


Your CardPointe account will guide you step-by-step through the [PCI DSS compliance process](#), and provide information and resources so you can protect your customers' data today.


**LOGIN WITH CARDPOINTE**

To register your account, you will need to enter the temporary username provided at the bottom of this email.

A link to select your password will be sent to you in a separate email. Once you have set up your password, you can then log in.

**Need Help?**

 1-877-257-0239

 [ccsupport@securetrust.com](mailto:ccsupport@securetrust.com)

Company Name  
Marketing Test

Merchant ID  
1234marketing

Username  
1234marketing

### Set your password for your CardPointe PCI compliance account


**Dear customer,**


Click the button below to set up your password.

Using your username (issued separately) you can now log in to your PCI DSS reporting portal using the button below.

**SET PASSWORD HERE**

**Need Help?**

 1-877-257-0239

 [ccsupport@securetrust.com](mailto:ccsupport@securetrust.com)

Company Name  
Marketing Test


Merchant ID  
1234marketing

# Registration - Two Steps

- Upon clicking “Set Password” you will be able to create your password for your account

**Update password**

Please create a new password

   
0/200

Your password should meet the following criteria:

- ✗ \* Your password should be a minimum of 8 characters.
- ✗ \* Your password should at least contain 1 upper-case letter.
- ✗ \* Your password should at least contain 1 lower-case letter.
- ✗ \* Your password should at least contain 1 special character (e.g.: #?!@\$%^&\*-)
- ✗ \* Your password should at least contain 1 number.
- ✗ \* Your password shouldn't contain more than 2 repeating characters in the same case.

FOR EXAMPLE:

AAxA = Not Allowed	AAxa = Allowed
aaXa = Not Allowed	AXaa = Allowed

# PCI Assessment Overview

- Guided workflow that provides step by step instructions on screen.

## What's next?


- 1 We will ask you some questions

Mostly around how your business is set up to handle credit and debit card payments. Your answers help us to figure out the level of security risks that your business may have so we only ask you questions relevant to your business.
- 2 We will help you protect your business

To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.
- 3 Confirm your business is secure

You will be asked to confirm and validate your responses and any scanning tasks that you were required to undertake. PCI DSS refer to this as your Attestation of Compliance (AoC).

### Getting Started with PCI Data Security Standard



[START BUSINESS PROFILE](#)

# PCI Assessment Overview

- Select how you would like you assess your PCI Compliance.

### Pick an assessment method

---

Guide Me - Choose this option to receive step-by-step guidance throughout the compliance validation process. Next series of questions will help determine your PCI scope. Your PCI scope is used to ensure the right PCI requirements for your business type are covered.

Expert - Choose this option to be able to select from a list of available PCI SAQ forms to complete without step-by-step guidance. Next series of questions will help recommend a SAQ form.

Upload - Choose this option if you are already certified with another provider and need to upload your compliance documents to this account.

[PREVIOUS](#) [NEXT](#)






This [helpful video](#) walks you through the “Guide Me” assessment method.

# Guided PCI Questionnaire

- Describe how you accept and process card payments.

## What Are The Ways You Accept Credit Card Payments

How do you accept credit cards? Select all that apply.

My business has a physical location where payments with a credit card are made in-person.

My business allows payments with a credit card by mail or over the phone (MO/TO).

My business has a website where payments with a credit card are made online.


[PREVIOUS](#) [NEXT](#)


# Guided PCI Questionnaire

- Get Help along the way! Throughout the guide you will see clickable “?” symbols with assistance and definitions to guide you through the process.

that

*E-Commerce is a form of retailing over the Internet, where products are ordered online from a website without the card being physically presented for the transaction. Please select this option if you are an e-Commerce merchant.*





My business has a website where payments with a credit card are made online.


[NEXT](#)

# Guided PCI Questionnaire


- Scoping questions that help determine the right questionnaire.


## Credit Card Data Storage

---

**Does your business store any sensitive credit card data electronically? **

Yes, I have a payment application or device that stores credit card data.

Yes, I store credit card data in a computer. 

Yes, I receive credit card data from a third-party in electronic format. 

Yes, I store credit card data in some other way.

None of the above - I never store credit card data.

[PREVIOUS](#) [NEXT](#)




# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Web Site Control

---

Does your business have administrative control over any part of your web site? 

Yes

No - a third-party service provider handles ALL administration.

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Payment Handling

---

When customers make purchases on your website, where is the credit card data submitted?

- Directly to a third-party; my web site NEVER receives the credit card data. ?
- My web site receives the credit card data first then sends it on for processing.

PREVIOUS

NEXT

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Checkout Page

---

Do the web servers you administer have control over the payment page that is presented to your customers? ?

No - the payment page comes ENTIRELY from the third-party. ?

Yes - some or all of the payment page is generated from my web site


[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Website Isolation

---

Is your e-commerce website isolated from all other systems within your environment? 

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Service Providers

---

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

Yes  No

## Multiple Acquirer

---

Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## E-Commerce Websites

---

Identify all websites where your customers can make online purchases.

You agree you have full authority to allow Sysnet Global Solutions to monitor the above website(s).

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Service Providers

Identify any service providers you use either to host your website or to handle the credit card processing from website or mail/telephone orders, and specify the type of services provided.

Filter

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

### Wireless Network for POS Devices

---

Do any of your POS devices connect to your network wirelessly (using Wi-Fi)? 

Yes  No



# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Other Wireless Networks

---

Do you use wireless networks or devices anywhere else in your business (office computers or laptops, free Wi-Fi for customers, etc.)?

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Unauthorized Wireless Access Points

---

Do you check your store or office for unauthorized wireless access points on at least a quarterly basis? ?

Yes, I physically inspect my store's network for unauthorized wireless devices.

Yes, I use the Network Discovery Scan service to monitor my network.

Yes, I use a different automated method such as a wireless analyzer, NAC or Wireless IDS/IPS.

No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Recognize POS Device Tampering

---

Does your business develop (build or customize) its own applications that store, process, or transmit credit card data? (This is not common for small businesses.) ?

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Public-Facing Websites

---

Do you have any public-facing websites? 

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Websites and Payments

---

Do these websites collect payments? Or are they connected to any computers that are part of your credit card payment environment?

Yes  No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Defend Your Websites

---

For your public-facing web sites, are new threats and vulnerabilities addressed on an ongoing basis? ?

I rely on my service providers to perform this function.

Yes, I regularly use manual or automated application vulnerability security assessment tools or methods.

Yes, I use a web-application layer firewall in front of my Web site.

No

[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Control Physical Access

---

(check all that apply) Do you control physical access to areas where credit card data is present: ?

- Restrict access to publicly accessible network jacks.
- Restrict access to critical equipment: wireless access points, firewalls, cable/dsl modems, etc.
- Provide an easy way to distinguish between employees and visitors.
- None of the above


[PREVIOUS](#) [NEXT](#)

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.

## Secure Data Area

---

Do you have a data center, server room, or other area that houses systems that store, process, or transmit credit card data? 

Yes  No

[PREVIOUS](#) [NEXT](#)



# Guided PCI Questionnaire

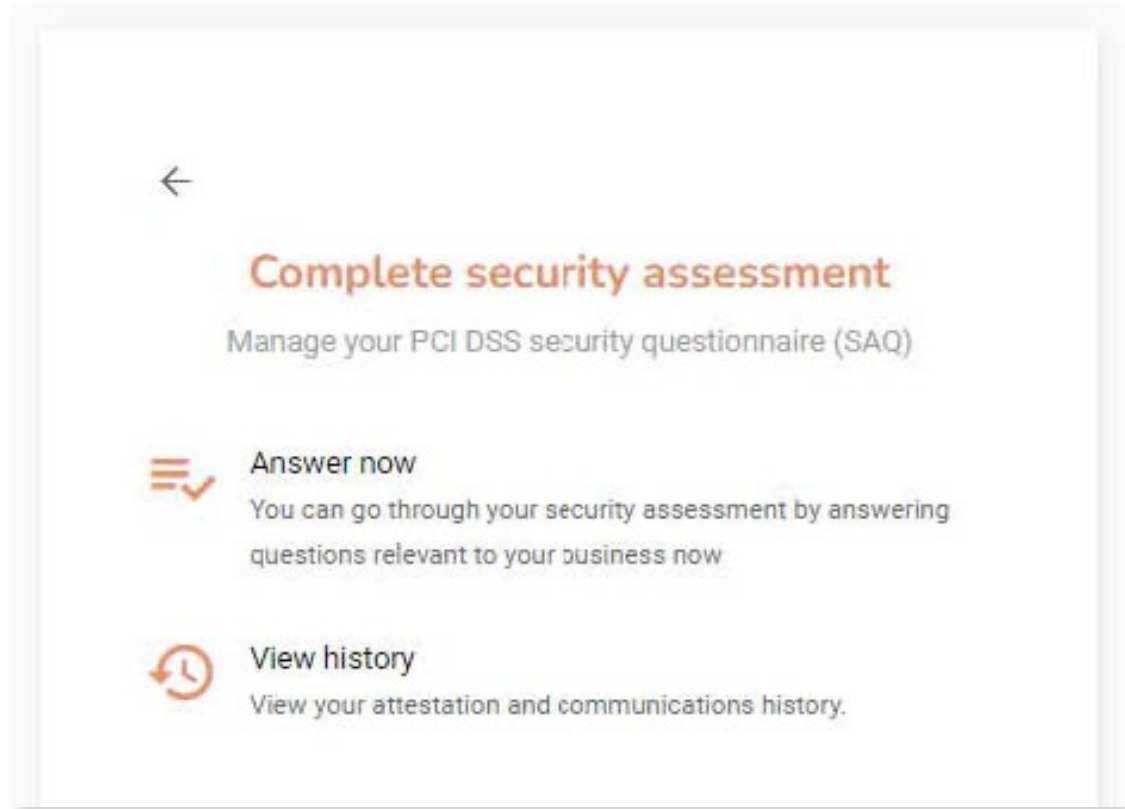
- Scoping questions that help determine the right questionnaire.

The dashboard displays the following information:

- Compliance Status:** A shield icon with a red 'X' indicates that the user is not compliant. The text reads: "You're not compliant. Please complete your remaining compliance tasks." A "VIEW SUMMARY" button is located below.
- YOUR NEXT STEP:** A section with the heading "YOUR NEXT STEP" and the instruction "Schedule your scan and be scan compliant". It explains: "As you have one or more devices connected via the internet you have scanning tasks to do. To maintain your compliance you will need to run an external vulnerability scan every three months." A "BEGIN STEP" button is provided.
- Available Compliance Tools:** A section titled "Here are your available compliance tools" contains three cards:
  - Your business profile:** Includes a calendar icon with a green checkmark. Text: "Your business profile. Complete SAQ type A-EP." Buttons: "MORE INFO", "MANAGE".
  - Be scan compliant:** Includes a globe icon with a red 'X'. Text: "Be scan compliant. Run PCI DSS External Vulnerability Scan." Buttons: "MORE INFO", "MANAGE".
  - Complete security assessment:** Includes a document icon with a red 'X'. Text: "Complete security assessment. 171 Unanswered questions. 0 Remediation tasks." Buttons: "MORE INFO", "MANAGE".

# Guided PCI Questionnaire

- Scoping questions that help determine the right questionnaire.



# Guided PCI Questionnaire

Show me:  Show Help Text:

## Build and Maintain a Secure Network and Systems

Install and maintain a firewall configuration to protect cardholder data

---

Are firewall and router configuration standards established and implemented to include the following:

1.1.2(b)  
Is there a process to ensure the diagram is kept current?

### Sections

- 44 Build and Maintain a Secure Network and Systems
- 10 Protect Cardholder Data
- 13 Maintain a Vulnerability Management Program
- 36 Implement Strong Access Control Measures
- 48 Regularly Monitor and Test Networks
- 18 Maintain an Information Security Policy
- X Confirm your compliance

# Guided PCI Questionnaire

- Help Text provides further information on each question.

Show me:  Show Help Text:

---

### Build and Maintain a Secure Network and Systems

Install and maintain a firewall configuration to protect cardholder data

---

Are firewall and router configuration standards established and implemented to include the following:

1.1.2(b)  
Is there a process to ensure the diagram is kept current?

I have implemented a compensating control

**i Information**

#### PCI Council Guidelines

Network diagrams describe how networks are configured, and identify the location of all network devices.

Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.


#### PCI Audit Procedures

Interview responsible personnel to verify that the diagram is kept current.

# Guided PCI Questionnaire

- SAQ answers resulting in a failing status will be flagged for remediation.
- The sidebar will keep track of your remaining questions.
- Remediate all issues prior to confirming your compliance.


Are all anti-virus mechanisms maintained as follows:

5.2(b) 

Are automatic updates and periodic scans enabled and being performed?

I have implemented a compensating control

N/A  NO  YES


 Remediation task

Reason for non-compliance

0 / 1500

Complete documentation

0 / 1500

Target date:   You will receive a reminder email

## Sections

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- 1** Maintain a Vulnerability Management Program
- 36 Implement Strong Access Control Measures
- 48 Regularly Monitor and Test Networks
- 18 Maintain an Information Security Policy
- Confirm your compliance

# Guided PCI Questionnaire

- Upon completion of your SAQ, you will be prompted to confirm your account information.
- If ASV scan is required for your account, you must complete and pass your scan prior to submission.

**Confirm your compliance**  
Please review the form below and ensure all sections are correct and complete

✓ Your organization information details

Company name: Marketing Test  
Contact name: Mike Smith  
Title: President  
Telephone numbers:  
Email address: ryanmcgriff@vikingcloud.com  
Business address:  
Country: USA

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ A, EP

✓ Acknowledgement of status and attestation

✗ Merchant Executive Officer

✗ Attestation

⚠ Attention! You cannot attest. No compliant ASV scan result available.  
You will not be able to attest until you have a compliant PCI DSS external vulnerability scan result available. Please use our scanning solution to schedule a scan or upload a third party result now.

[GO TO SCAN MANAGEMENT](#)

[PREVIOUS](#)

**Sections**

- ✓ Build and Maintain a Secure Network and Systems
- ✓ Protect Cardholder Data
- ✓ Maintain a Vulnerability Management Program
- ✓ Implement Strong Access Control Measures
- ✓ Regularly Monitor and Test Networks
- ✓ Maintain an Information Security Policy
- ✗ Confirm your compliance

# Integrated PCI Scanning

- You can set up and run your scans by clicking “Manage” from your Portal Home Page.

The screenshot displays a user interface for a compliance portal. At the top, a blue header reads "Here are your available compliance tools". Below this, there are three main tool cards. The first card, "Your business profile", shows a status of "Complete SAQ type B-IP" and has "MORE INFO" and "MANAGE" buttons. The second card, "Be scan compliant", is highlighted with a green border and shows a status of "Run PCI DSS External Vulnerability Scan" with "MORE INFO" and "MANAGE" buttons. The third card, "Complete security assessment", shows "17 Unanswered questions" and "0 Remediation tasks" with "MORE INFO" and "MANAGE" buttons. Below these is a "Document Repository" card showing "Contains 0 documents" with "UPLOAD" and "VIEW DOCUMENTS" buttons. At the bottom, a blue header reads "Here are the additional security products", followed by a card for "PROTECT YOUR DEVICE(S)" with a status of "Compliance and security manager application" and "MORE INFO" and "INSTALL" buttons.

Here are your available compliance tools

- Your business profile  
Complete  
SAQ type B-IP  
[MORE INFO](#) [MANAGE](#)
- Be scan compliant  
Run PCI DSS External Vulnerability Scan  
[MORE INFO](#) [MANAGE](#)
- Complete security assessment  
17 Unanswered questions  
0 Remediation tasks  
[MORE INFO](#) [MANAGE](#)

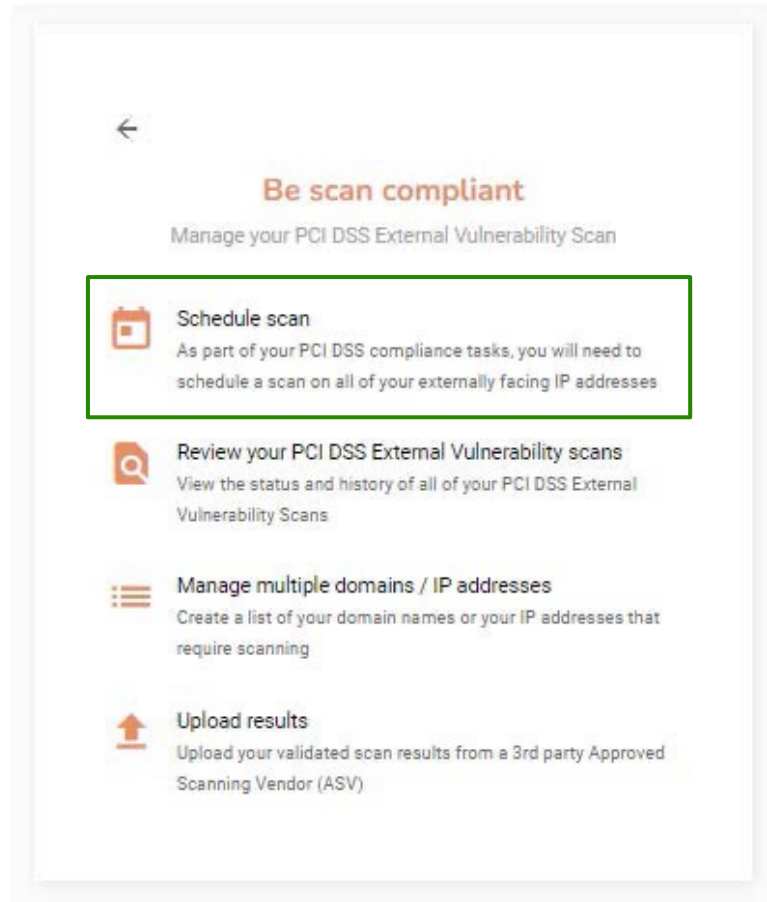
Document Repository  
Contains 0 documents  
[UPLOAD](#) [VIEW DOCUMENTS](#)

Here are the additional security products

- PROTECT YOUR DEVICE(S)  
Compliance and security manager application  
[MORE INFO](#) [INSTALL](#)

# Integrated PCI Scanning

- Click Schedule scan to setup your scan(s) for the first time.





# Integrated PCI Scanning

- Enter your web address and initiate scan.

Review your scans   Schedule Single Scan   Manage Group Scanning

### What would you like to scan?

Domain   Schedule group scan

Please enter domain address(es) or IP address(es) that you require to be scanned.

38.69.40.150

Domain / IP address   ADD

### Scan date

Please enter a preferred time and date for the scan to occur.

Scan date   08:31 AM

### Load Balancer?

Do you use Load Balancers as a part of your in-scope PCI Infrastructure?

Yes    No

#### Sysnet access

In order to run the scan, we need you to grant access to the IP addresses listed below:

If you use security software such as a firewall in your organisation, you may need to white-list the below addresses in order for the scan to run successfully. Otherwise, you may block access to the scan, meaning it will fail. This will result in you being unable to successfully report your compliance.

If you are unsure how to do this, consult the help section of your firewall or contact your internet service provider for assistance.

#### What is an IP address?

An IP address is a series of numbers and dots that is your address on the internet. We need the correct address for your internet connection, to allow us to scan the correct connection – otherwise, we may scan someone else's network.

#### Dynamic IP addresses

Some internet service providers will assign you a "Dynamic IP Address." This is an IP address that changes every time you connect and disconnect your internet router.

If you have a dynamic IP address, you need to update us with this new number every time you run your scan. This allows us to scan the correct connection.

If you are unsure as to whether you have a dynamic IP address, please contact your internet service provider who will be able to advise you. If you do have a dynamic IP it's advisable to refrain from scheduling scans in advance, as your IP address may have changed by the time the scheduled scan runs.

- 64.39.96.0/20
- 139.87.112.0/23

#### Website disclaimer notice

##### Granting Sysnet access

By using this Website you are accepting all the terms of this disclaimer notice. If you do not agree with anything in this notice you should not use this Website.

##### Warranties and Liability

I understand that Sysnet requires access be granted to the above IP addresses in order to complete a scan.

I will ensure that any active protection (including Intrusion Prevention System) is disabled or that I will white-listed Sysnet's above IP's for the duration of the test.

I confirm that our domain and IP addresses will grant access to the IP address(es) stated above.

In no event will Sysnet be liable for any incidental, indirect, consequential or special damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of profit, loss of contracts, goodwill, data, information, income, anticipated savings or business relationships, whether or not advised of the possibility of such damage, arising out of or in connection with the use of this website or any linked websites. In addition, Sysnet shall not be liable for any fees, charges, costs or penalties imposed by any third party vendors used by you or any other person on your behalf (including but not limited to any internet or other service provider or other third party) in connection with, on foot of, or a result of your use of this website or the services contained therein.

##### Exceptions

Nothing in this disclaimer notice excludes or limits any warranty implied by law for death, fraud, personal injury through negligence, or anything else which it would not be lawful for Sysnet to exclude.

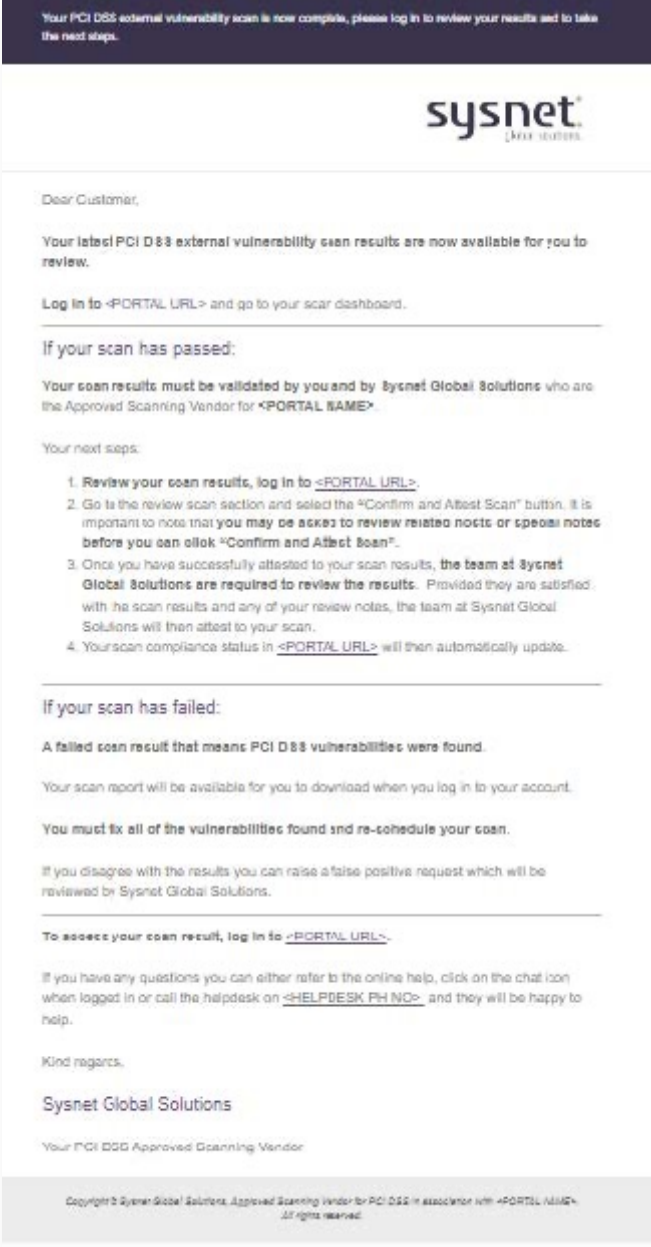
##### License to use this Website

By using this website you agree to the exclusions and limitations of liability stated above and accept them as reasonable. Do not use this website if you do not agree that they are reasonable. If any of the points in this disclaimer notice are found to be unenforceable under applicable law that will have no bearing on the enforceability of the rest of the disclaimer notice. Material on this website, including text and images, is protected by copyright law and is copyright to Sysnet unless credited otherwise. It may not be copied, reproduced, republished, downloaded, posted, broadcast or transmitted in any way except for your own personal, non-commercial use. Prior written consent of the copyright holder must be obtained for any other use of material. Copyright of the images on this site shall remain with the copyright owner at all times. No part of this site may be distributed or copied for any commercial purpose or financial gain. All intellectual property rights in relation to this website are reserved and owned by Sysnet.

I confirm that our domain and IP addresses will grant access to the IP address(es) stated above

# Integrated PCI Scanning

- You will receive an email when your scan has finished running.
- Login to your account from here to attest to your scan results.



Your PCI DSS external vulnerability scan is now complete, please log in to review your results and to take the next steps.

**sysnet**  
Global Solutions

Dear Customer,

Your latest PCI DSS external vulnerability scan results are now available for you to review.

Log in to <PORTAL URL> and go to your scan dashboard.

---

**If your scan has passed:**

Your scan results must be validated by you and by Sysnet Global Solutions who are the Approved Scanning Vendor for <PORTAL NAME>.

Your next steps:

1. Review your scan results, log in to <PORTAL URL>.
2. Go to the review scan section and select the "Confirm and Attest Scan" button. It is important to note that you may be asked to review related notes or special notes before you can click "Confirm and Attest Scan".
3. Once you have successfully attested to your scan results, the team at Sysnet Global Solutions are required to review the results. Provided they are satisfied with the scan results and any of your review notes, the team at Sysnet Global Solutions will then attest to your scan.
4. Your scan compliance status in <PORTAL URL> will then automatically update.

---

**If your scan has failed:**

A failed scan result that means PCI DSS vulnerabilities were found.

Your scan report will be available for you to download when you log in to your account.

You must fix all of the vulnerabilities found and re-schedule your scan.

If you disagree with the results you can raise a false positive request which will be reviewed by Sysnet Global Solutions.

---

To assess your scan result, log in to <PORTAL URL>.

If you have any questions you can either refer to the online help, click on the chat icon when logged in or call the helpdesk on <HELPLESK PH NO> and they will be happy to help.

Kind regards,


Sysnet Global Solutions

Your PCI DSS Approved Scanning Vendor

Copyright © Sysnet Global Solutions. Approved Scanning Vendor for PCI DSS in association with <PORTAL NAME>. All rights reserved.

# Integrated PCI Scanning

- Review your Scan Results.



You're not compliant  
Please complete your remaining compliance tasks

[VIEW SUMMARY](#)


**YOUR NEXT STEP**

Schedule your scan and be scan compliant


As you have one or more devices connected via the internet you have scanning tasks to do.

To maintain your compliance you will need to run an external vulnerability scan every three months.

[BEGIN STEP](#)




**Here are your available compliance tools**




Your business profile  
Complete SAQ type A-EP

[MORE INFO](#) [MANAGE](#)



Be scan compliant  
Run PCI DSS External Vulnerability Scan

[MORE INFO](#) [MANAGE](#)







Complete security assessment  
171 Unanswered questions  
0 Remediation tasks

[MORE INFO](#) [MANAGE](#)

←

**Be scan compliant**

Manage your PCI DSS External Vulnerability Scan

-  **Schedule scan**  
As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses
-  **Review your PCI DSS External Vulnerability scans**  
View the status and history of all of your PCI DSS External Vulnerability Scans
-  **Manage multiple domains / IP addresses**  
Create a list of your domain names or your IP addresses that require scanning
-  **Upload results**  
Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

# Integrated PCI Scanning

- Review and attest to your Scan Results.

### Scan Dashboard

You can view & edit your current scan status and scan history

SCAN STATUS:	SCAN RESULT:	SCAN DATE:	SCAN ATTESTED DATE:	ASV:	ACTIONS:
Ready to attest	✓ Pass	Jun 10, 2022 17:21	Jun 10, 2022 17:22	Sysnet Global Solutions	<a href="#">OPTIONS</a>

### Scan Status

Status	Ready to attest
Result	✓ Pass
Scan date	Jun 10, 2022 5:21:36 PM
Date updated	Jun 14, 2022 7:25:52 AM
Do you use load balancers as part of your in-scope PCI infrastructure?	No
PCI Vulnerability Report	<a href="#">Download</a>
ASV False Positive Approved	-
Merchant attested	No
ASV Attested	No

[Confirm and attest scan](#)

# Integrated PCI Scanning

- Shortly after you attest, your dashboard will prompt you complete your compliance assessment.

**You're not compliant**  
Please complete your remaining compliance tasks  
[VIEW SUMMARY](#)

**YOUR NEXT STEP**  
Your compliant scan results will be here shortly  
Please check back later.

**Here are your available compliance tools**

- Your business profile**  
Complete SAQ type B-IP  
[MORE INFO](#) [MANAGE](#)
- Be scan compliant**  
Scan is fully compliant  
Valid until Sep 8, 2022, 5:21:36 PM  
[MORE INFO](#) [MANAGE](#)
- Complete security assessment**  
Awaiting compliant scan results  
[MORE INFO](#) [MANAGE](#)

**Attestation**

**Information for Submission.**  
Based on the results noted in the SAQ B-IP dated Jun 14, 2022, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Jun 14, 2022:  
  
Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby TEST-MERCHANT VIEW has demonstrated full compliance with the PCI DSS.

[CONFIRM YOUR ATTESTATION](#)

[PREVIOUS](#)

# You are now PCI Compliant!

- You may download your Attestation of Compliance for your records from your dashboard.

The screenshot displays a user interface for PCI compliance. At the top, a large green checkmark icon is centered within a shield, with the text 'You're compliant' below it. Underneath, it states 'Valid until 14 June 2023' and provides two buttons: 'VIEW SUMMARY' and 'DOWNLOAD AOC'. To the right, a light blue panel features a coffee cup icon and the text 'YOU ARE NOW COMPLIANT' and 'Congratulations, you're all done.' Below this, a section titled 'Here are your available compliance tools' contains three cards. Each card has an icon, a title, a status, a date, and two buttons: 'MORE INFO' and 'MANAGE'.

Tool Name	Status	Last Attested / Valid Until
Your business profile	Complete	SAQ type B-IP
Be scan compliant	Scan is fully compliant	Valid until Sep 12, 2022, 5:33:13 AM
Complete security assessment	Last attested	Jun 14, 2022, 4:52:10 PM

# Resources

- **PCI Security Standards Council:**

→ [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

List of validated payment applications, services providers, and more

- **VISA CISP:**

→ <http://www.visa.com/cisp>

- **MasterCard SDP:**

→ <http://www.mastercard.com/sdp>

# Questions?

**We are here to help.**

Please have your Merchant ID handy.

---

## Customer Support Number

- 1-877-257-0239
- [ccsupport@securetrust.com](mailto:ccsupport@securetrust.com)

