SecureTrust™
a Sysnet company

PCI Portal

User Guide for Merchants

Table of Contents

What's Included?

- **Report your PCI DSS compliance**
  - Streamlined and simplified journey
  - Download your information security policy template
- **Maintain your compliance throughout the year**
  - Login to complete regular scanning and maintenance tasks
- **Receive email alerts and reminders so you always stay up to date**
- **Rich online, chat and phone support available if you get stuck**

The Process

1

Login

Login to the portal and change your password

2

Profile

Complete your business profile by answering questions on how you accept payments

3

Scanning

Complete scanning on your network if applicable to your business profile type

4

Security Assessment

Complete your Security Assessment Questionnaire (SAQ) – an online assessment of your security practices

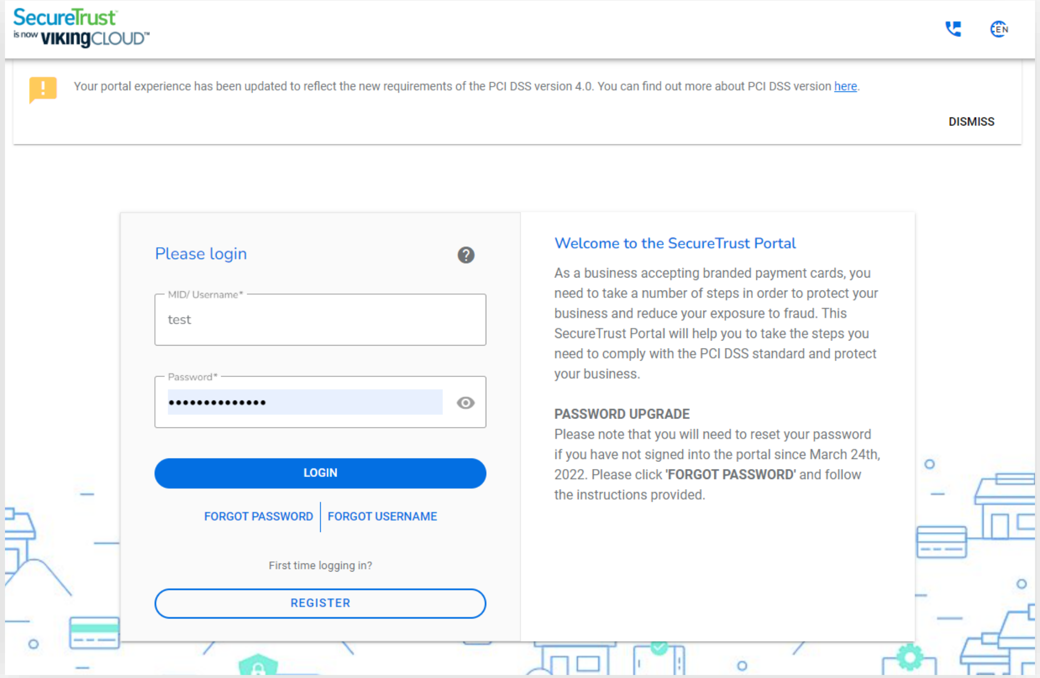
5

Maintenance

You may need to maintain your compliance. We'll remind you by email if this is the case.

Login

- Upon first logging in to the portal, use the username and password provided in your emails and click ‘Login’.
- You will then be prompted to update your password. Your password will need to meet the minimum-security criteria outlined on the screen.
- Once you have completed this, you will be brought to an information page that gives you an overview of what you need to do and an information video.
- **Note: If you did not receive a welcome email, you can select the register button once you have confirmed your MID is already enrolled into the PCI program**



Your portal experience has been updated to reflect the new requirements of the PCI DSS version 4.0. You can find out more about PCI DSS version here.

Please login

MID/ Username* test

Password* ••••••••••••••

First time logging in?

Welcome to the SecureTrust Portal

As a business accepting branded payment cards, you need to take a number of steps in order to protect your business and reduce your exposure to fraud. This SecureTrust Portal will help you to take the steps you need to comply with the PCI DSS standard and protect your business.

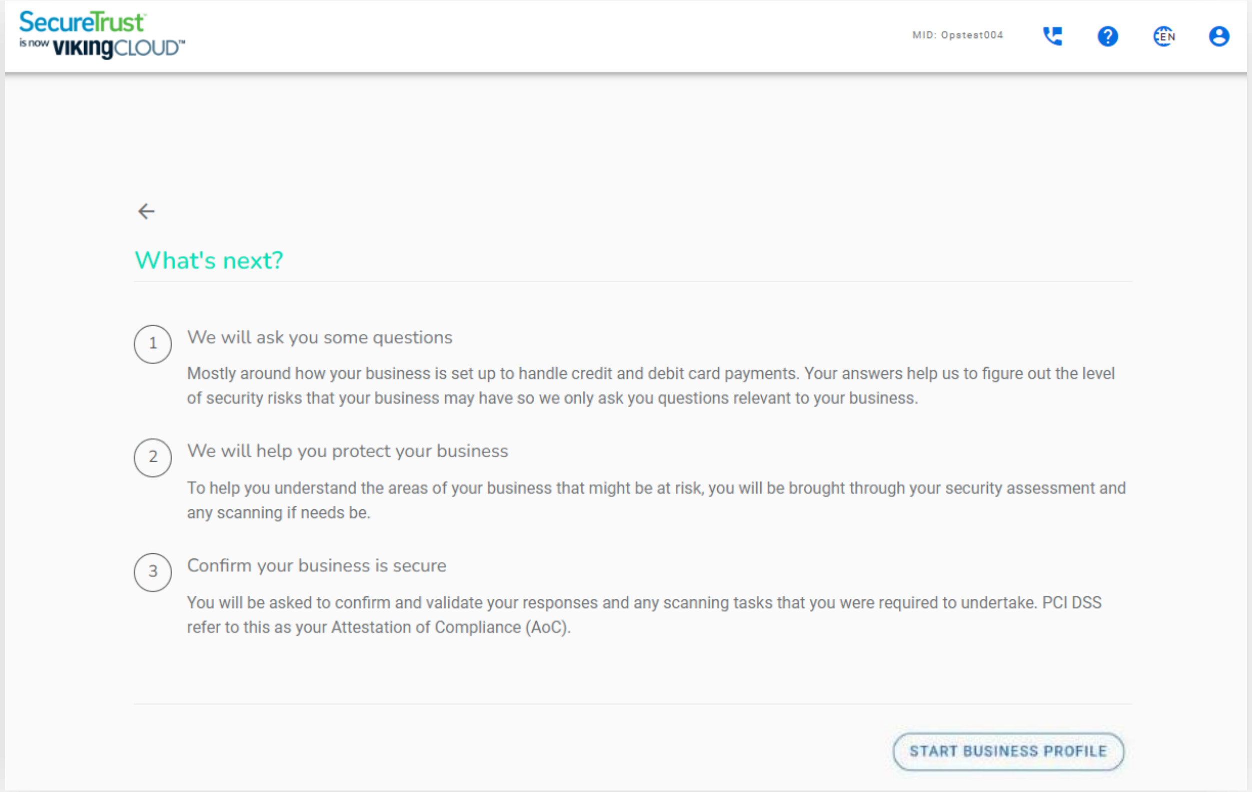
PASSWORD UPGRADE
Please note that you will need to reset your password if you have not signed into the portal since March 24th, 2022. Please click '**FORGOT PASSWORD**' and follow the instructions provided.

Your Profile

How you accept payments

Start Business Profile

- Once logged in, you will be brought to an information page that gives you an overview of what you need to do and a short information video.
- Click ‘Start Business Profile’ to begin.



MID: Opstest004

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

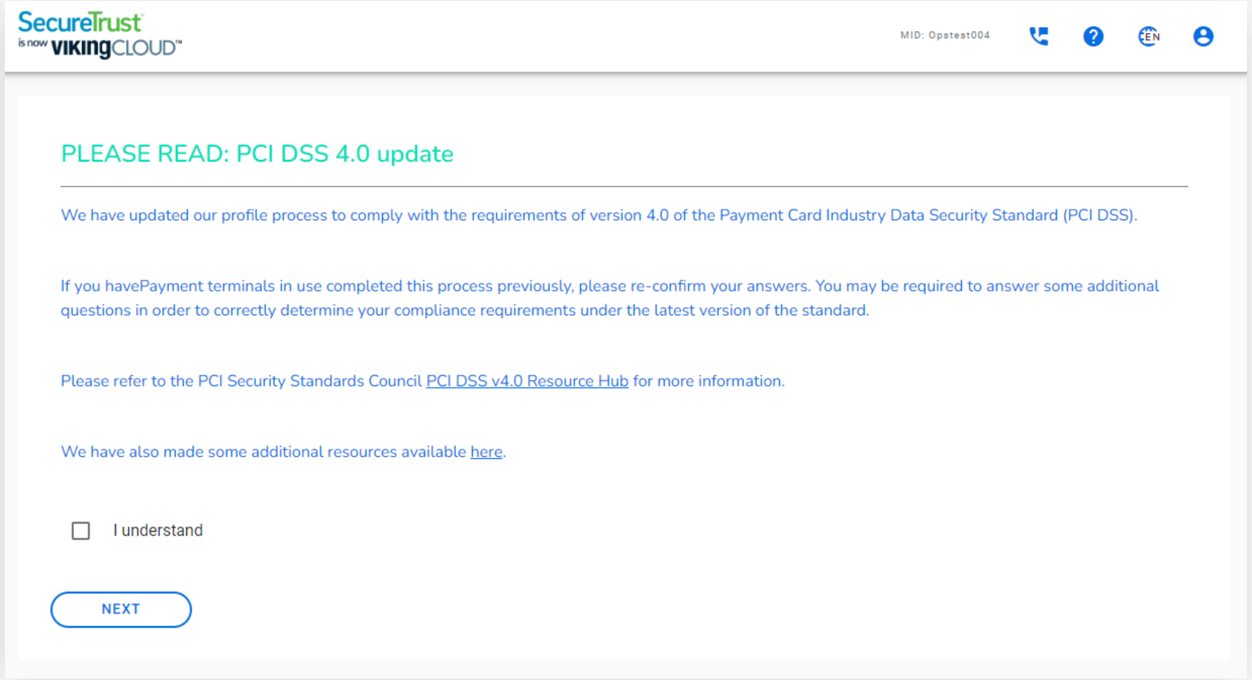
To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.

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).

PCI DSS v4.0

- You will be presented with a notification regarding PCI DSS v4.0. Here you will need to select the box to confirm you understand what the introduction of this new standard means for your compliance.



PLEASE READ: PCI DSS 4.0 update

We have updated our profile process to comply with the requirements of version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS).

If you havePayment terminals in use completed this process previously, please re-confirm your answers. You may be required to answer some additional questions in order to correctly determine your compliance requirements under the latest version of the standard.

Please refer to the PCI Security Standards Council PCI DSS v4.0 Resource Hub for more information.

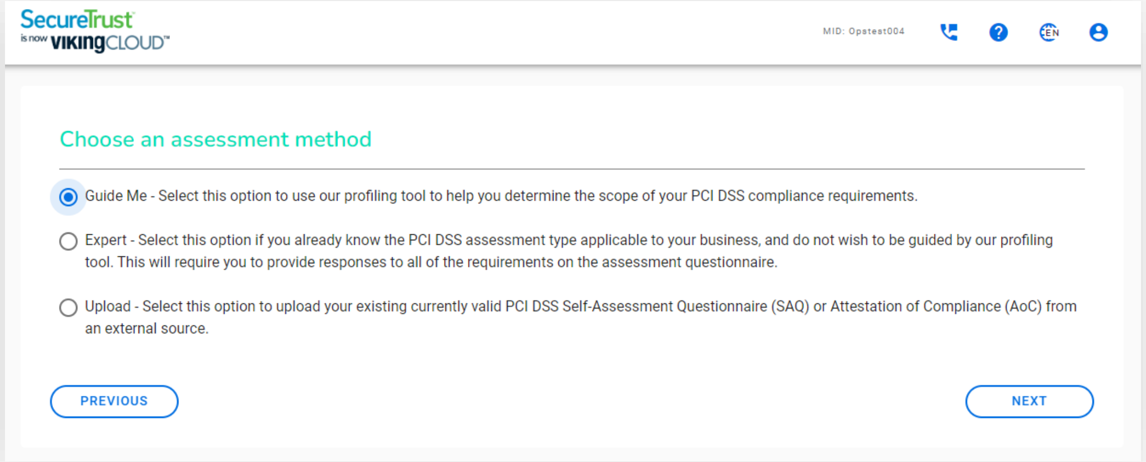
We have also made some additional resources available here.

□ I understand

NEXT

First time using the portal?

- The first screen you will encounter is a question as to whether you have completed this process before.
- In some cases, you may have already completed your PCI compliance with an assessment company. If this is the case, select "Upload" and proceed to page 28 of this guide for instructions on uploading your existing documentation.
- You also have the option to select ‘Expert’ allowing you to choose from a selection of PCI SAQ forms.
- **If you do not already have a valid certificate and need to complete your compliance online, select the first option on this screen and continue to page 9 of this guide.**



Choose an assessment method

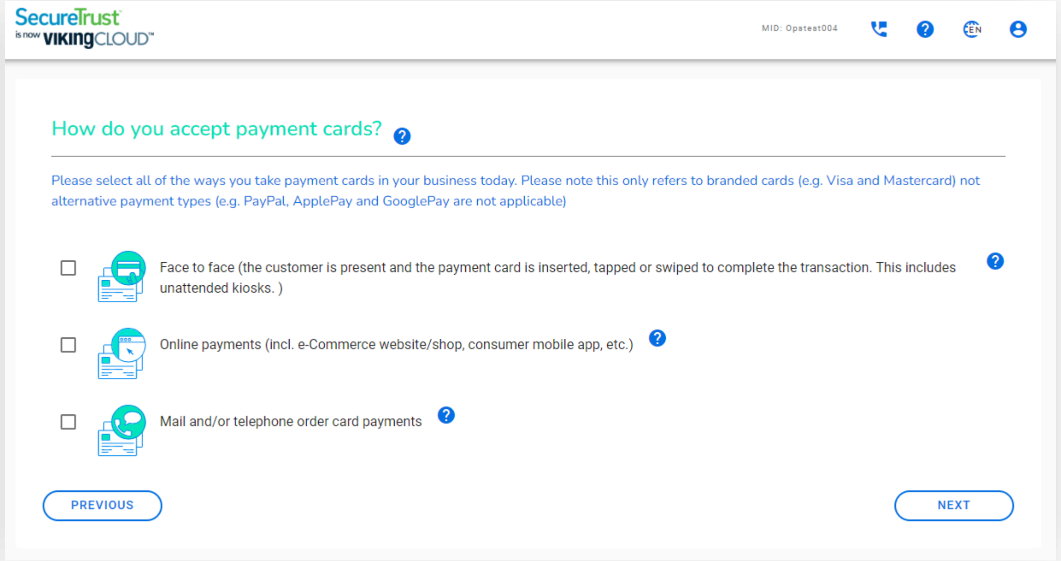
● Guide Me - Select this option to use our profiling tool to help you determine the scope of your PCI DSS compliance requirements.

○ Expert - Select this option if you already know the PCI DSS assessment type applicable to your business, and do not wish to be guided by our profiling tool. This will require you to provide responses to all of the requirements on the assessment questionnaire.

○ Upload - Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external source.

Your Profile – How do you accept payments?

- You will be guided through some questions asking how you accept payments in your business.
- You will be asked questions about the technology you use as well as methods by which you may transfer or store data.
- Select the options that apply to your company and click through via the ‘Next’ buttons. You can select more than one option in many cases.
- If you are unsure about any of the options or need further clarification, more information is available by clicking the help icon found in the top right of the screen.



How do you accept payment cards?

Please select all of the ways you take payment cards in your business today. Please note this only refers to branded cards (e.g. Visa and Mastercard) not alternative payment types (e.g. PayPal, ApplePay and GooglePay are not applicable)

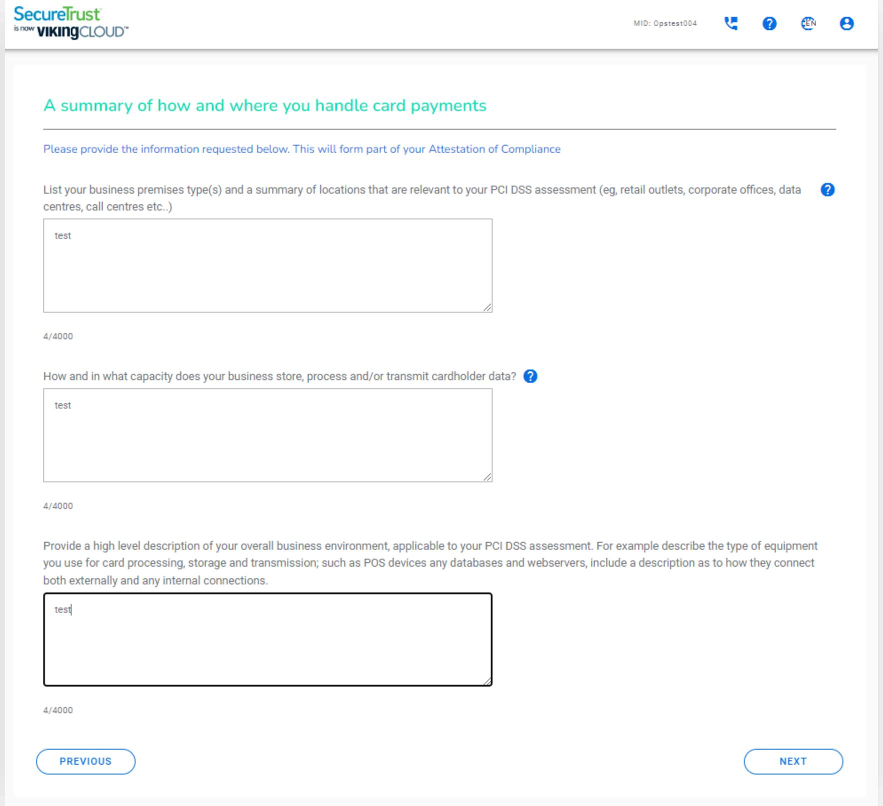
☐ Face to face (the customer is present and the payment card is inserted, tapped or swiped to complete the transaction. This includes unattended kiosks.)

☐ Online payments (incl. e-Commerce website/shop, consumer mobile app, etc.)

☐ Mail and/or telephone order card payments

Your Profile – Payment Summary

- You will be asked to provide a summary of your payment acceptance processes.
- **You will be asked to:**
  - List your business premises and provide a summary of the locations where you accept payments
  - Explain how your business handles cardholder data
  - Provide a high-level description of how you accept payments
- Please provide as much information as possible. If you are stuck, help is available by clicking the help icons.



A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc..) ?

test

4/4000

How and in what capacity does your business store, process and/or transmit cardholder data? ?

test

4/4000

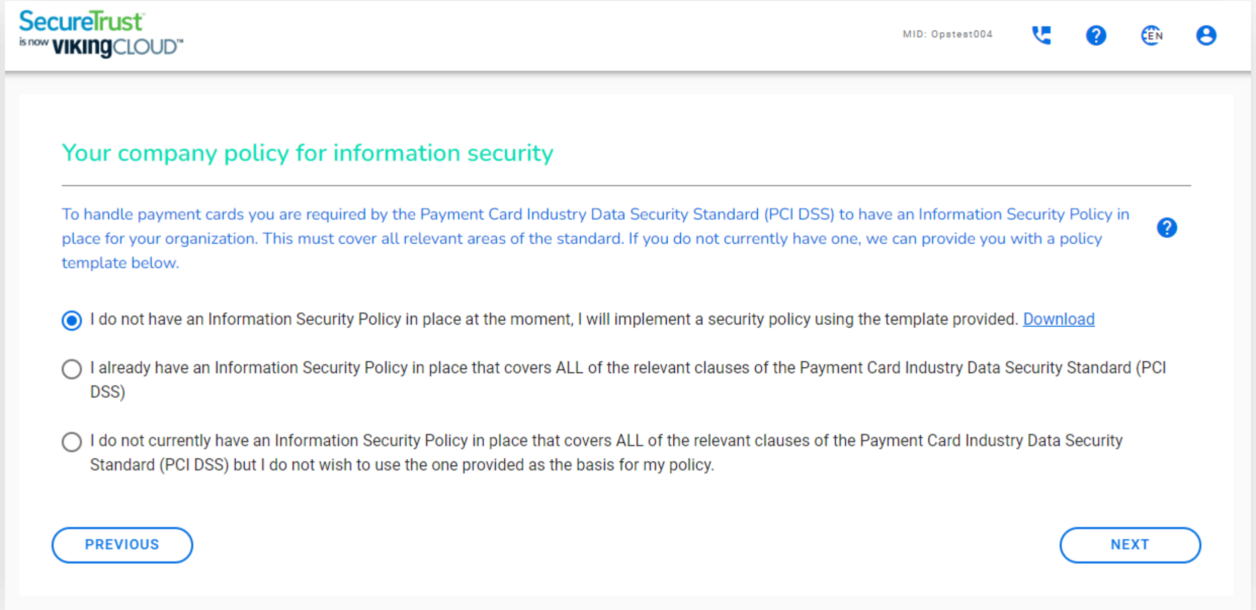
Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and webservers, include a description as to how they connect both externally and any internal connections.

test

4/4000

Your Profile – Information Security Policy

- It’s mandatory to apply an Information Security Policy
  - This is a document that sets out the procedures you need to follow to handle information securely
- You will be asked if you have a policy in your business. If you don’t, you can download a sample template by clicking ‘I use the security policies included in my subscription’. Afterward you will answer additional questions on your information security policy.



Your company policy for information security

To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template below.

● I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided. Download

○ I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

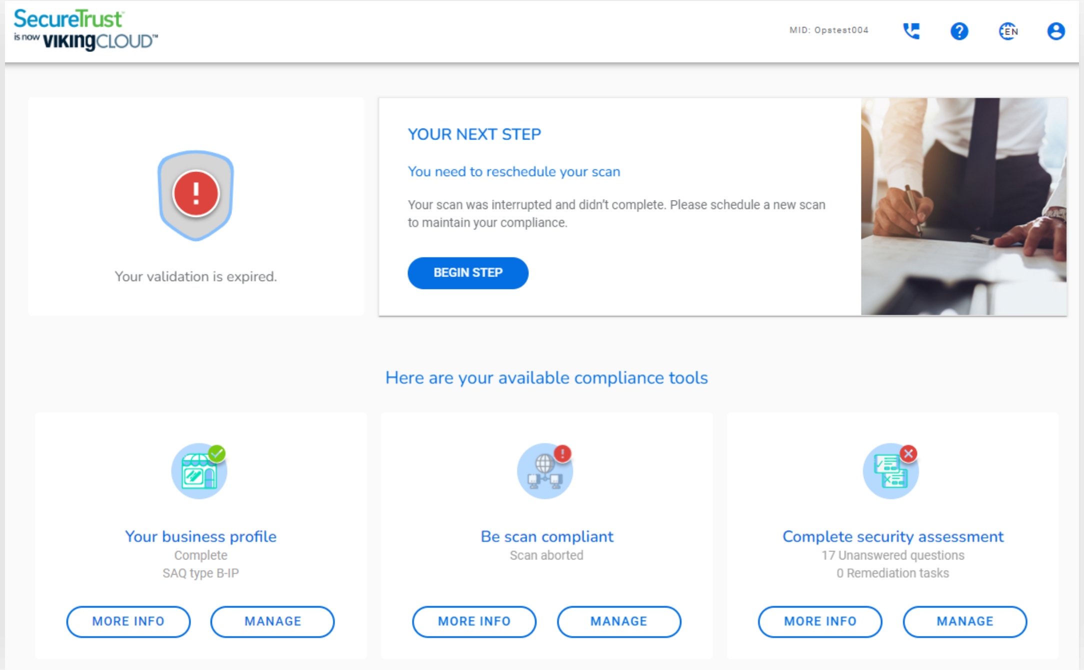
○ I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy.

Your Dashboard

You have completed your profile journey

Your Dashboard

- Now that you have answered your profile questions, you will be presented with your dashboard.
  - From here you can complete your security assessment as well as any other tasks that are assigned to you following your questions (e.g., scanning).
  - Your security assessment will be based on the profile type assigned to you.
- You can read more information on how this works via the ‘More Info’ button on the ‘Your business profile’ widget.
- If the scanning widget appears, you must complete a scan by selecting ‘Manage’ from this widget.
- If you do not require a scan, or have completed one, you can begin your security assessment by clicking ‘Manage’ on the relevant widget.



Your validation is expired.

YOUR NEXT STEP

You need to reschedule your scan

Your scan was interrupted and didn't complete. Please schedule a new scan to maintain your compliance.

Here are your available compliance tools

Your business profile
Complete
SAQ type B-IP

Be scan compliant
Scan aborted

Complete security assessment
17 Unanswered questions
0 Remediation tasks

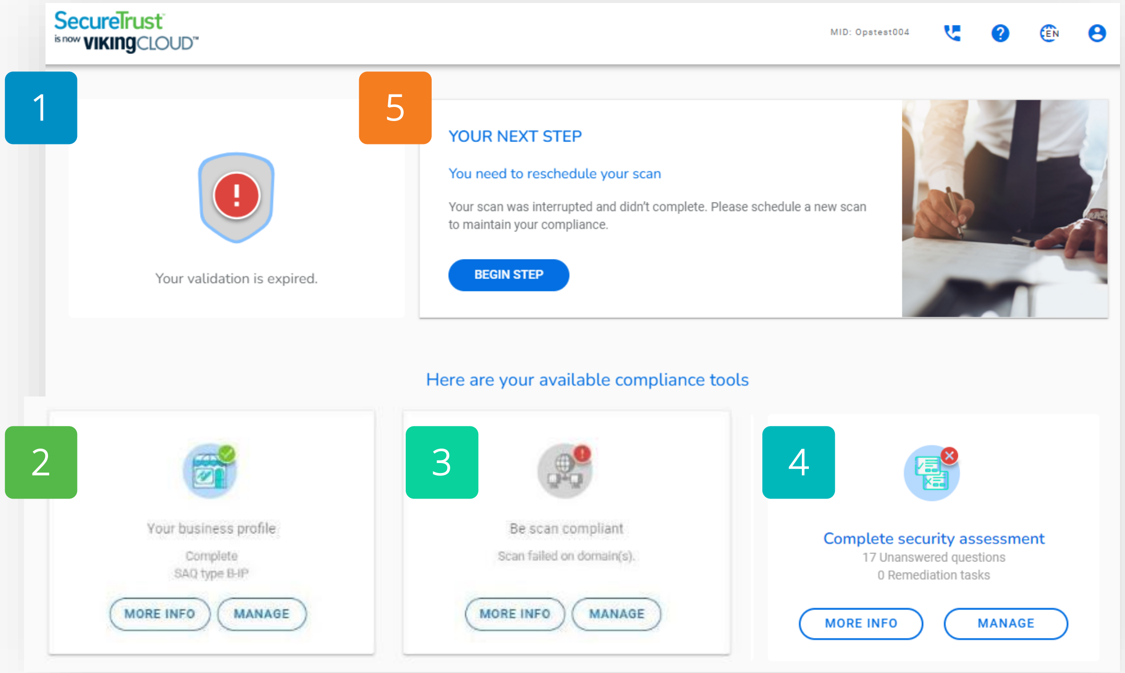
Your Dashboard

1

Your compliance status is listed at the top. You will not yet be compliant as you won’t have completed your scanning (if applicable) or Security Assessment yet.

2

You will have been assigned a business profile type, based on the answers you provided in your questions. You can read more on what this means by clicking ‘More Info’.



MID: Opstest004

Your validation is expired.

YOUR NEXT STEP

You need to reschedule your scan

Your scan was interrupted and didn't complete. Please schedule a new scan to maintain your compliance.

Here are your available compliance tools

Your business profile
Complete
SAQ type B-IP

Be scan compliant
Scan failed on domain(s).

Complete security assessment
17 Unanswered questions
0 Remediation tasks

3

If applicable, you can conduct your scanning from here. Click ‘Manage’ on the scan widget to begin.

5

By clicking ‘Your Next Step’ you will be brought to your current stage of your compliance journey.

4

When you have completed your scanning (if applicable) you can proceed to your security assessment by clicking ‘Manage’.

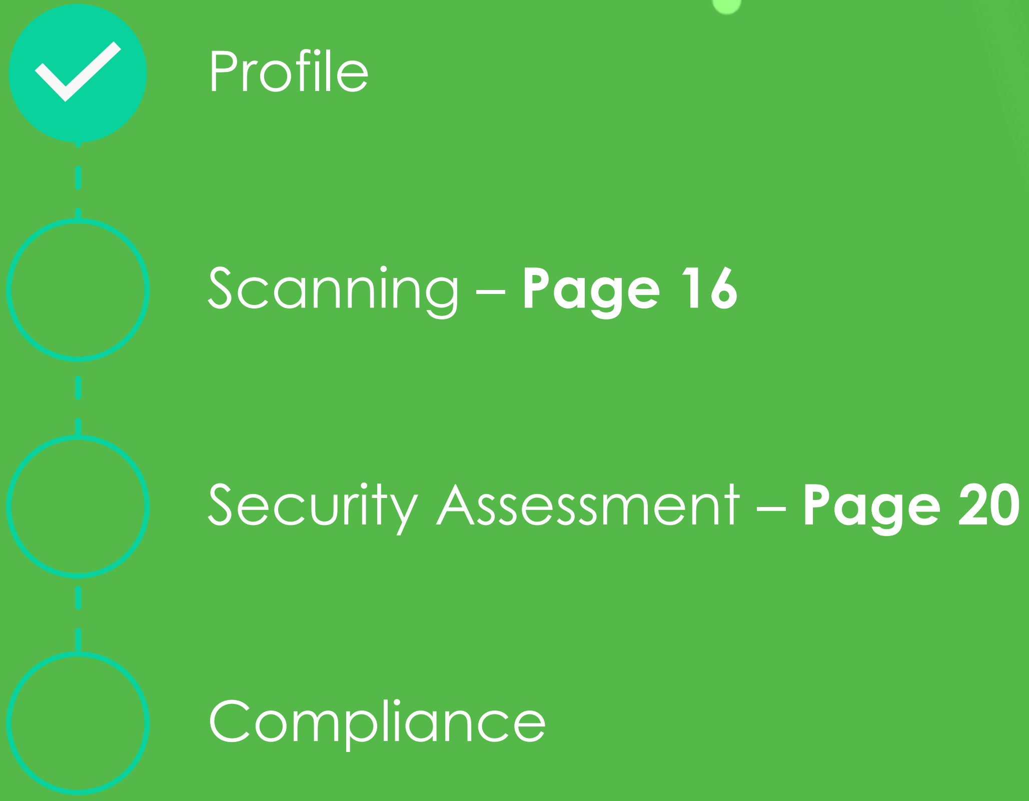
Next Steps

Scanning

If applicable to you, you will need to run a scan on your network. Proceed to page 16 for instructions.

Security Assessment

If don’t have to do a scan, you can proceed to your security assessment on page 20.



✓ Profile

○ Scanning – **Page 16**

○ Security Assessment – **Page 20**

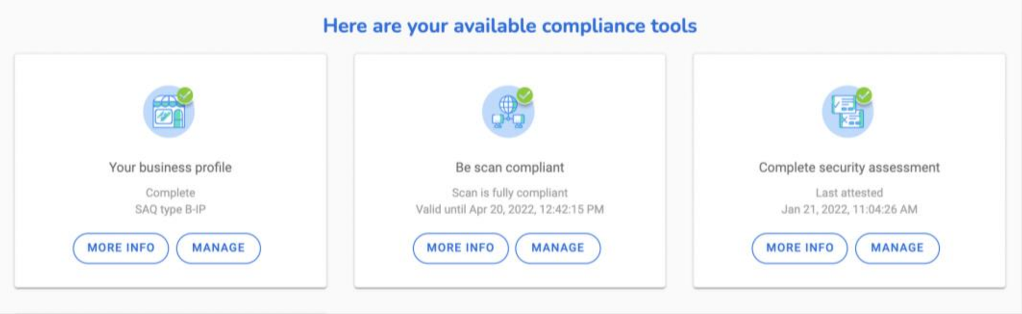
○ Compliance

Scanning and SAQ

Carrying over your scanning and SAQ completion

Scanning and SAQ

- As part of the upgrade, your scan status, scanning targets, historical completed scans and SAQs have been transferred to the upgraded portal automatically.
- If you successfully completed your scan and/or SAQ prior to upgrade, you will see green checkmarks across your dashboard.
- When your scan is due you will be sent a scan notification email. Once received, you can quickly log in and run your scans.
- **Note:** Due to the upgrade, your scans will run on a quarterly basis as opposed to monthly.

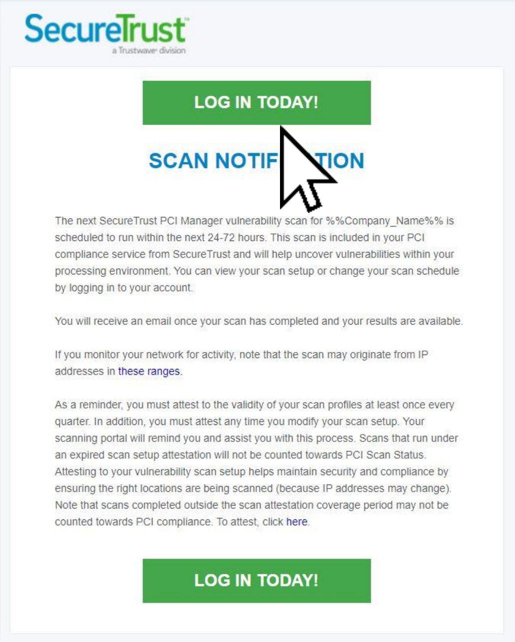


Here are your available compliance tools

Your business profile
Complete
SAQ type B-IP

Be scan compliant
Scan is fully compliant
Valid until Apr 20, 2022, 12:42:15 PM

Complete security assessment
Last attested
Jan 21, 2022, 11:04:26 AM



SecureTrust
a Trustwave division

LOG IN TODAY!

SCAN NOTIF TION

The next SecureTrust PCI Manager vulnerability scan for %%Company_Name%% is scheduled to run within the next 24-72 hours. This scan is included in your PCI compliance service from SecureTrust and will help uncover vulnerabilities within your processing environment. You can view your scan setup or change your scan schedule by logging in to your account.

You will receive an email once your scan has completed and your results are available.

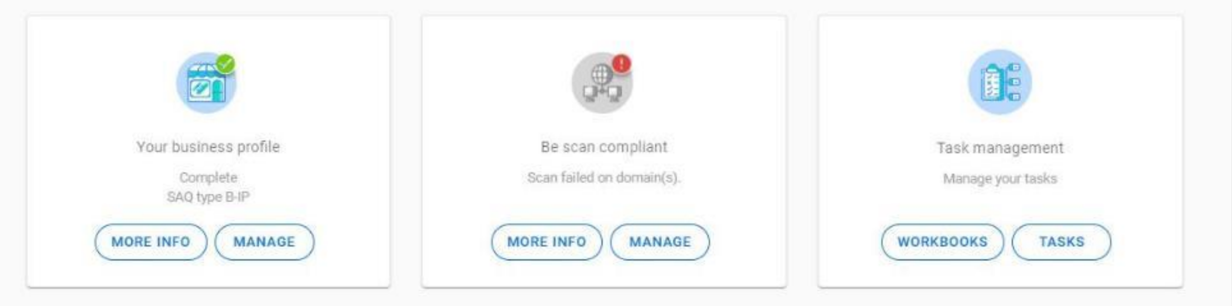
If you monitor your network for activity, note that the scan may originate from IP addresses in these ranges.

As a reminder, you must attest to the validity of your scan profiles at least once every quarter. In addition, you must attest any time you modify your scan setup. Your scanning portal will remind you and assist you with this process. Scans that run under an expired scan setup attestation will not be counted towards PCI Scan Status. Attesting to your vulnerability scan setup helps maintain security and compliance by ensuring the right locations are being scanned (because IP addresses may change). Note that scans completed outside the scan attestation coverage period may not be counted towards PCI compliance. To attest, click here.

LOG IN TODAY!

External Vulnerability Scanning

Scanning



Your business profile

Complete
SAQ type B-IP

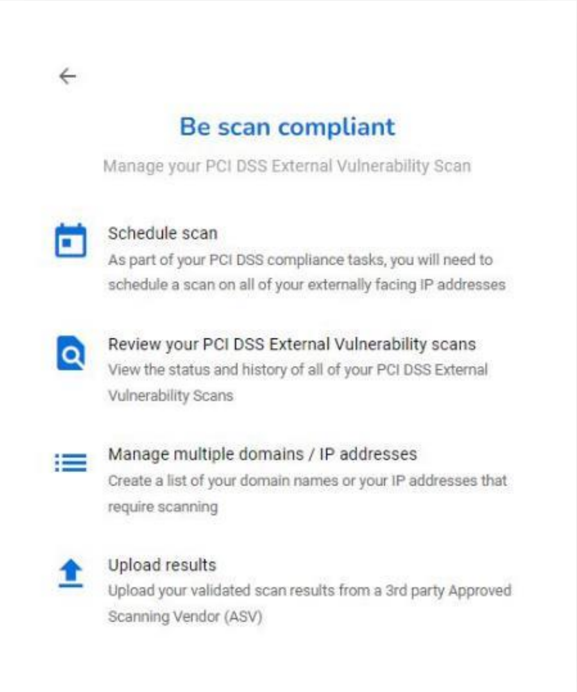
Be scan compliant

Scan failed on domain(s).

Task management

Manage your tasks

- From your dashboard, select ‘Manage’ on the ‘Be scan compliant’ widget.
- On the next page, select ‘Schedule scan’.



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

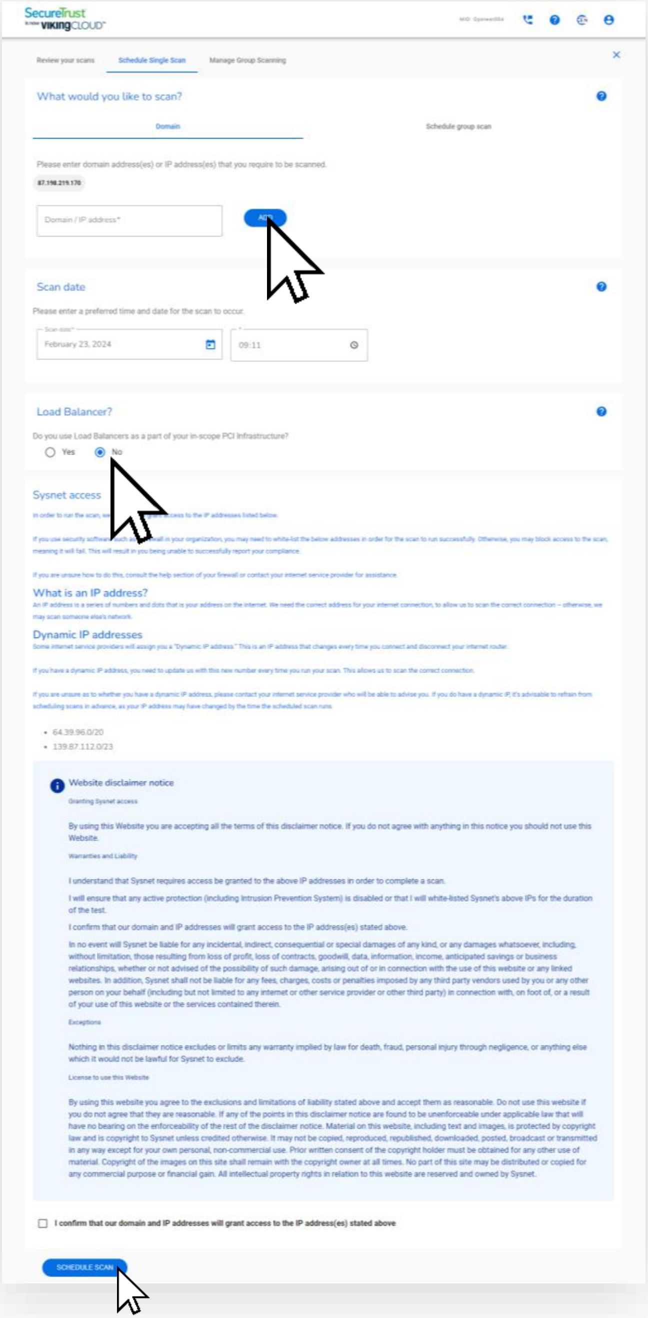
Review your PCI DSS External Vulnerability scans
View the status and history of all of your PCI DSS External Vulnerability Scans

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)

Scanning

- On the next screen you will need to input some details as follows:
  - **The IP address**. This must be the same IP address as used by your card payment machine. Instructions on how to find this is available on the next page.
  - **Scan date**. It will default to the current date and time. You can change this if necessary
  - Confirmation of whether you use a **load balancer**
- Once complete, select 'Schedule Scan'
  - The scan will then run and can take up to 48 hours. You will receive an email when the scan is complete.
  - You will be notified if remediation action is needed via your dashboard.
  - If your scan fails, you will need to complete the recommended remediation and then rerun the scan until a passing grade is achieved.



What would you like to scan?

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

87.198.219.170

Domain / IP address*

Scan date

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

Scan date*: February 23, 2024

09:11

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 [illegible] grant access to the IP addresses listed below.

If you use security software such a[illegible]wall in your organization, 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 IPs 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.

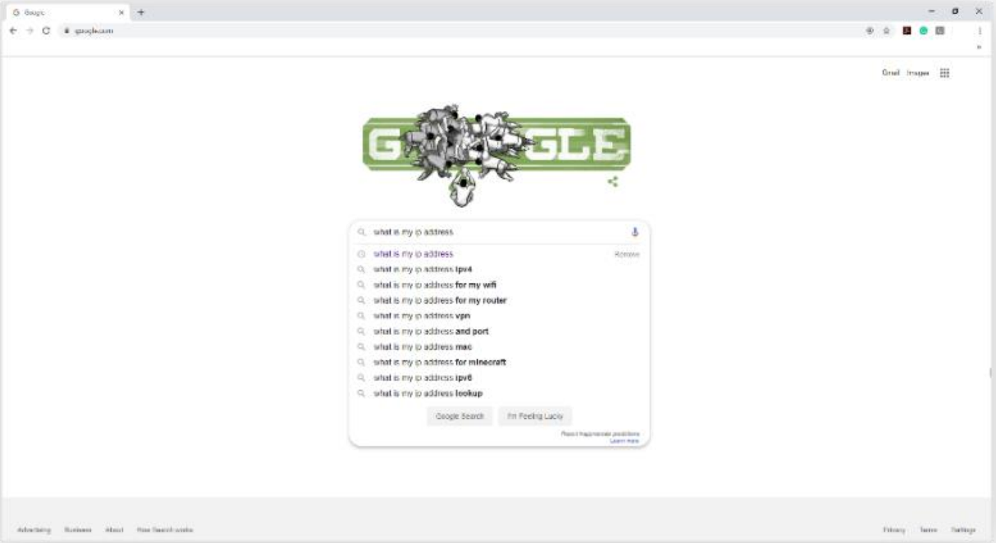
License to use this Website

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.

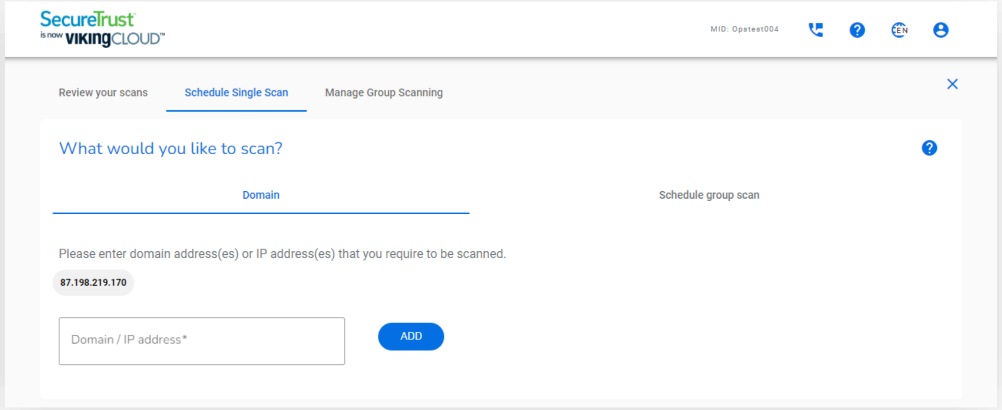
□ I confirm that our domain and IP addresses will grant access to the IP address(es) stated above

Finding your IP address

- To conduct a scan, you will need to provide us with your IP address. This is a series of numbers and dots that is your address on the internet. This helps to ensure the scan runs on the correct network.
- **To find your IP address:**
  - Connect a laptop, desktop or mobile device to the same Wi-Fi network that your card payment machine is connected to
  - Open your preferred search engine or browser and search "What is my IP address"
  - You can find your address from the search results
  - Please note, it is the IPV4 address that is required, not the IPV6


what is my ip address

what is my ip address
what is my ip address **ipv4**
what is my ip address **for my wifi**
what is my ip address **for my router**
what is my ip address **vpn**
what is my ip address **and port**
what is my ip address **mac**
what is my ip address **for minecraft**
what is my ip address **ipv6**
what is my ip address **lookup**



What would you like to scan?

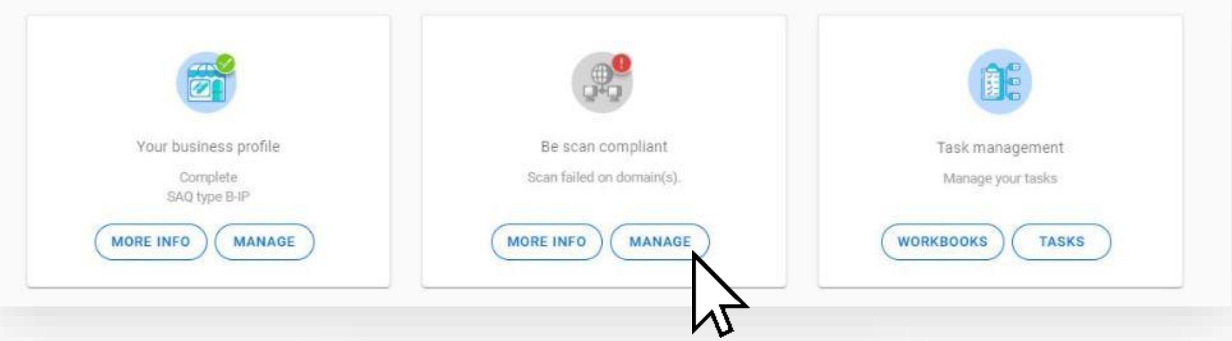
Please enter domain address(es) or IP address(es) that you require to be scanned.

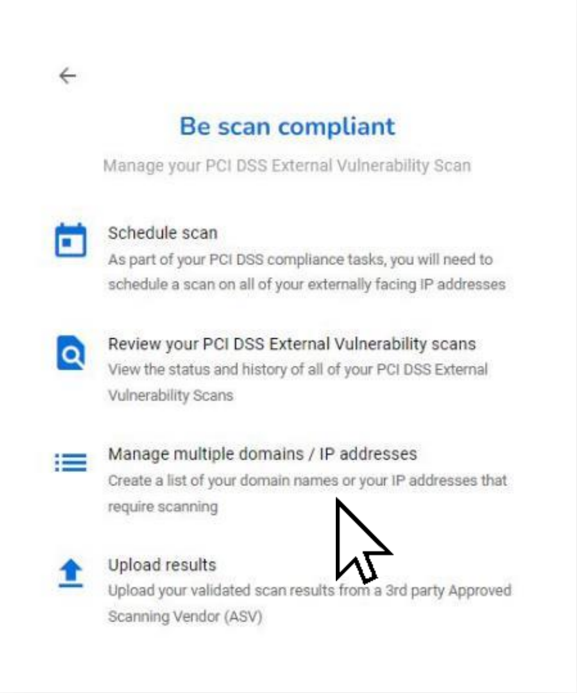
87.198.219.170

Domain / IP address*

Scheduling recurring scans

- To schedule recurring scans (monthly or quarterly) you will need to create a group to manage.
- Select manage and then manage multiple domains / IP addresses.





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

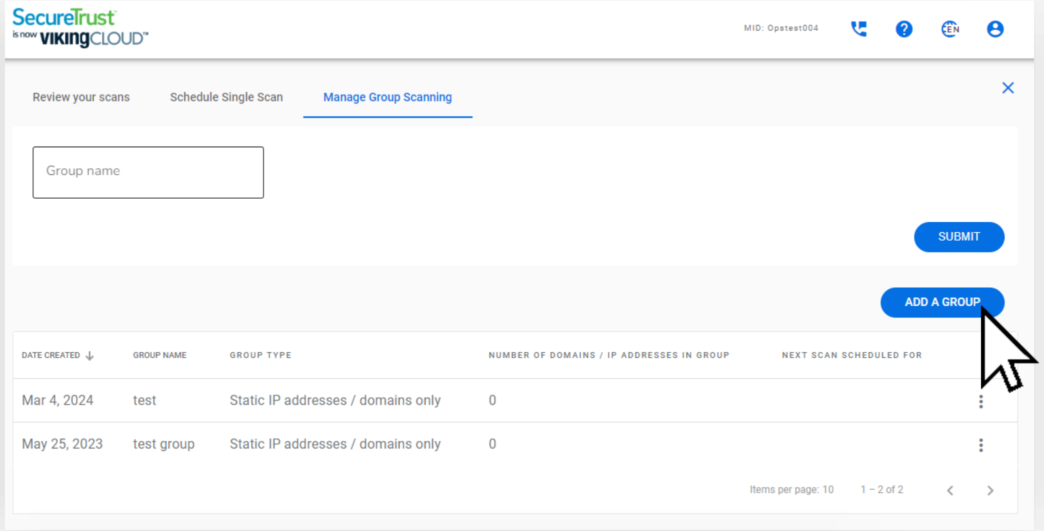
Review your PCI DSS External Vulnerability scans
View the status and history of all of your PCI DSS External Vulnerability Scans

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)

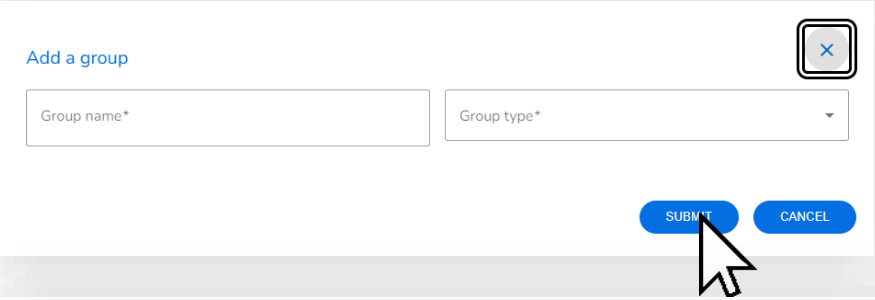
Scheduling recurring scans continued

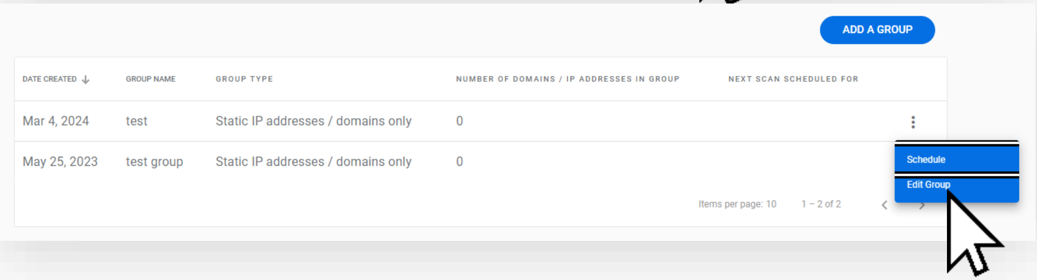
- If you already have a group created you will see it listed here, if not, select **'Add a group'**.
- Select a group name and group type (Static IP addresses or dynamic) and click **'Submit'**.
- Once the group is added select your newly added group and chose **'Edit Group'**.



DATE CREATED ↓	GROUP NAME	GROUP TYPE	NUMBER OF DOMAINS / IP ADDRESSES IN GROUP	NEXT SCAN SCHEDULED FOR
Mar 4, 2024	test	Static IP addresses / domains only	0	
May 25, 2023	test group	Static IP addresses / domains only	0	

Items per page: 10 1 – 2 of 2



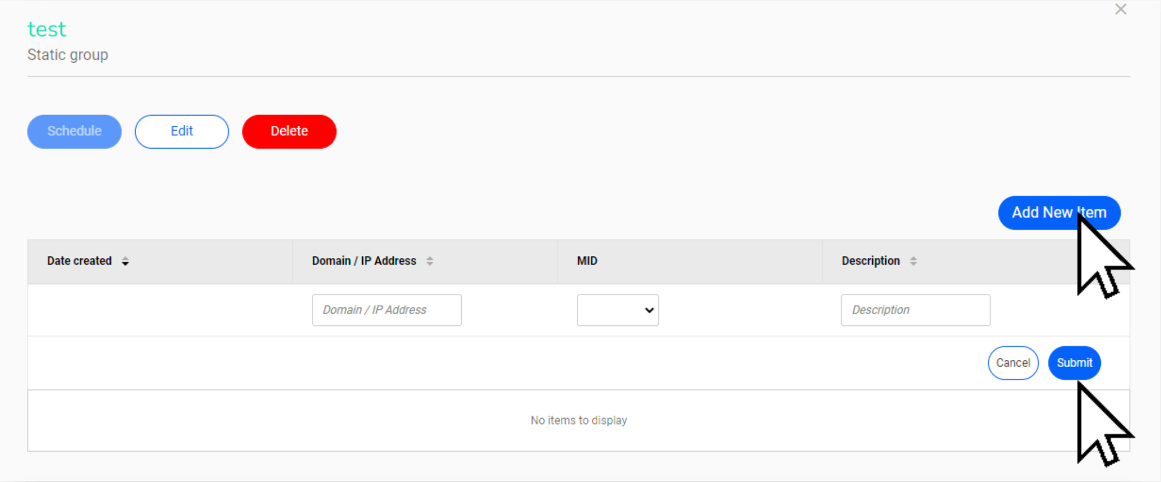


DATE CREATED ↓	GROUP NAME	GROUP TYPE	NUMBER OF DOMAINS / IP ADDRESSES IN GROUP	NEXT SCAN SCHEDULED FOR
Mar 4, 2024	test	Static IP addresses / domains only	0	
May 25, 2023	test group	Static IP addresses / domains only	0	

Items per page: 10 1 – 2 of 2

Scheduling recurring scans continued

- Select **‘Add New Item’** and input the fields requested.
- Click ‘Submit’ when you’re happy with the information provided.
- You will now need to click **‘Schedule’** on the dropdown menu.

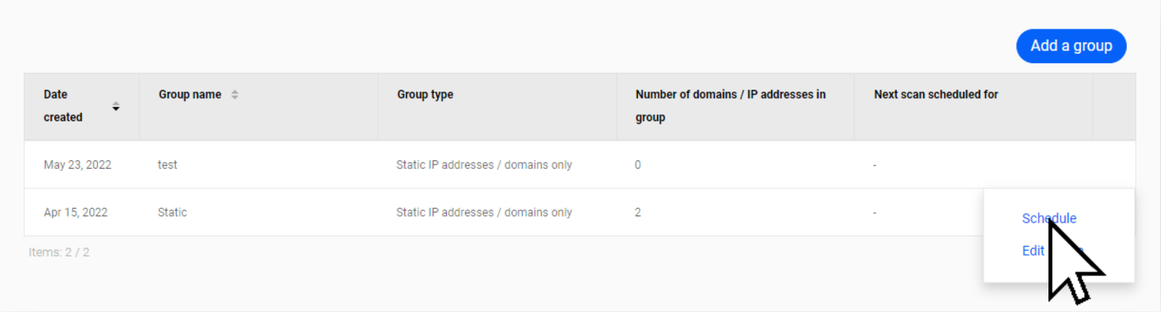


test

Static group

Date created	Domain / IP Address	MID	Description
	Domain / IP Address		Description

No items to display

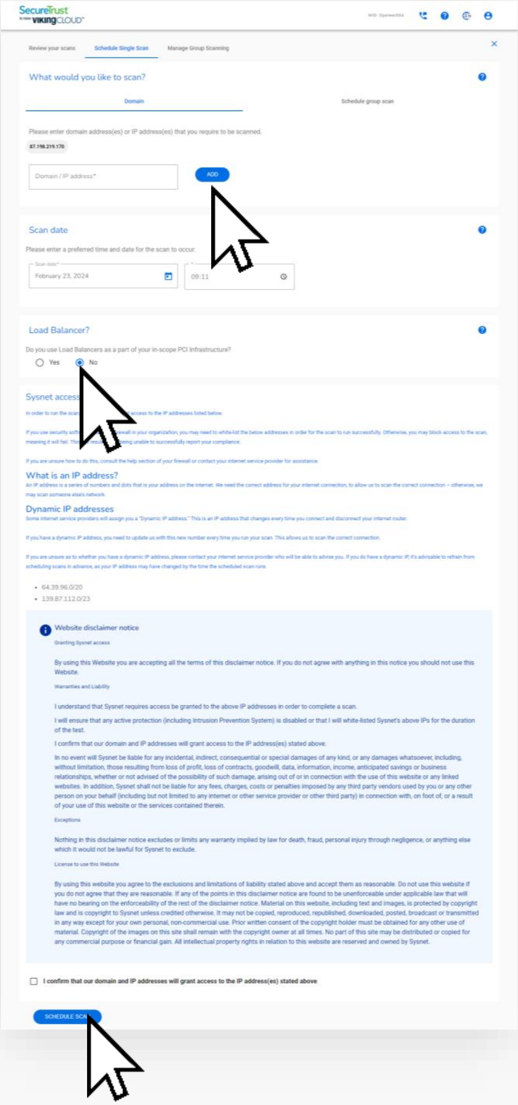


Date created	Group name	Group type	Number of domains / IP addresses in group	Next scan scheduled for
May 23, 2022	test	Static IP addresses / domains only	0	-
Apr 15, 2022	Static	Static IP addresses / domains only	2	-

Items: 2 / 2

Scheduling recurring scans continued

- Much like scheduling a once off scan you will need to select the scan date (your recurring scans will run from this date from your desired occurrence), whether or not a load balancer is present and finally give permission for the scan to run.
- You have the option to run a single, monthly or quarterly scan.



What would you like to scan?

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

87.198.219.170

Domain / IP address*

Scan date

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

Scan date*: February 23, 2024

09:11

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 … access to the IP addresses listed below.

If you use security soft… firewall in your organization, 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 … resul… 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 IPs 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

Security Assessment Questionnaire

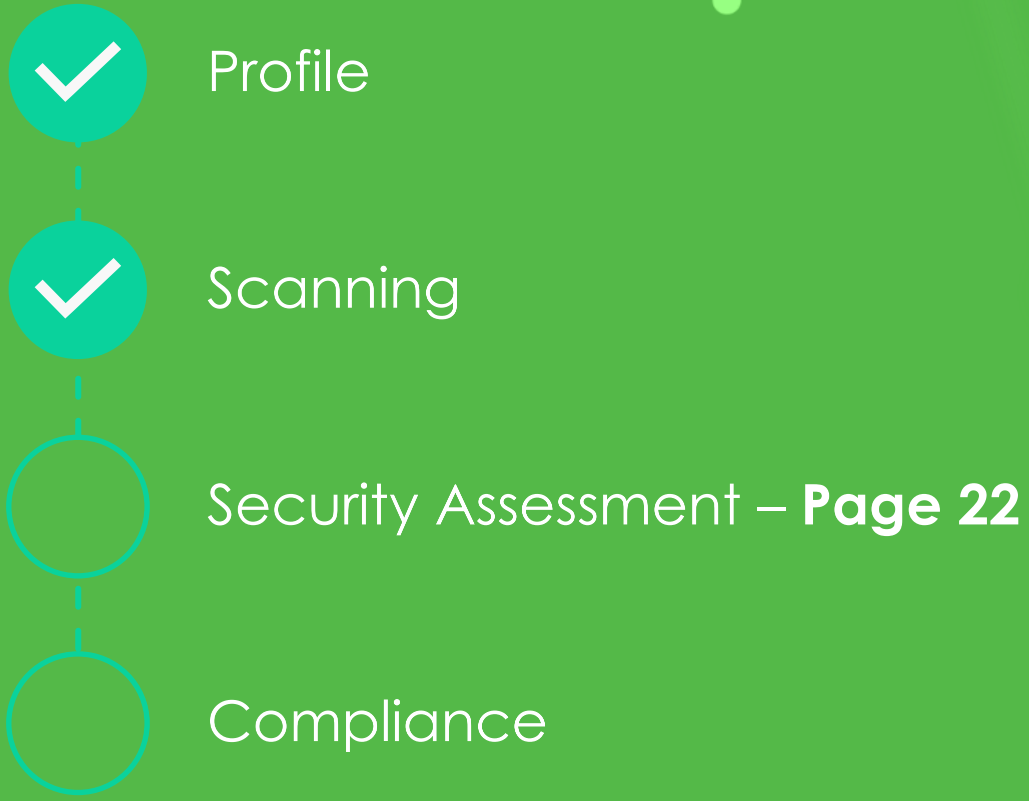
Your SAQ

Next Steps

Security Assessment Questionnaire (SAQ)

Your security assessment is an assessment of how you deal with information in your business. Its length and complexity depends on the results of your business profile.

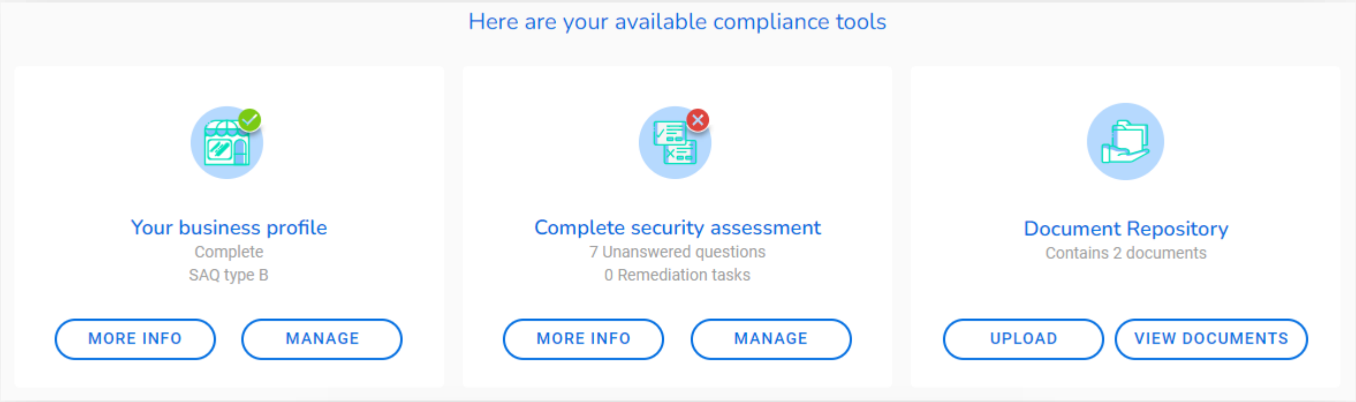
Depending on your choice (guided or expert, explained on page 8) you will be provided with an SAQ that has prepopulated any questions that do not apply to you (guided), or a full SAQ containing all possible questions (expert).



- ✓ Profile
- ✓ Scanning
- ○ Security Assessment – **Page 22**
- ○ Compliance

Security Assessment Questionnaire (SAQ)

- From your dashboard, select ‘Manage’ on the ‘Complete security assessment’ widget.
- You will see on your dashboard how many questions you must answer.
  - The number of questions you must answer depends on the business profile assigned to you and is based on your level of risk.

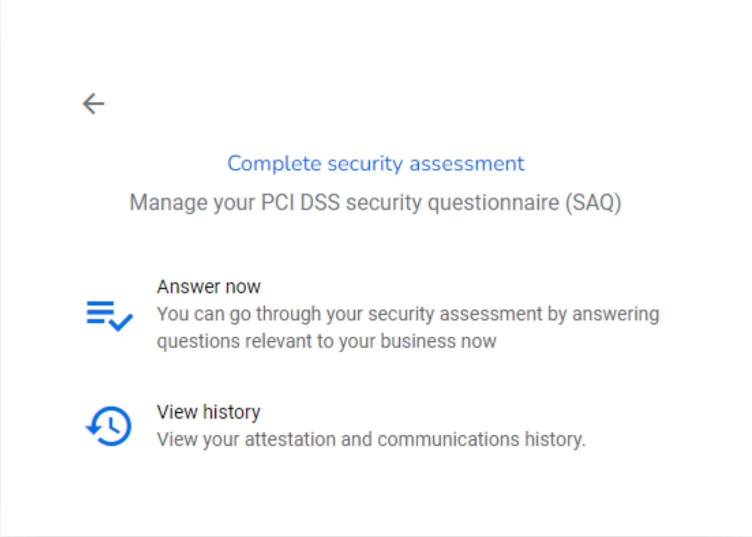


Here are your available compliance tools

Your business profile
Complete
SAQ type B

Complete security assessment
7 Unanswered questions
0 Remediation tasks

Document Repository
Contains 2 documents



Complete security assessment

Manage your PCI DSS security questionnaire (SAQ)

Answer now
You can go through your security assessment by answering questions relevant to your business now

View history
View your attestation and communications history.

SecureTrust

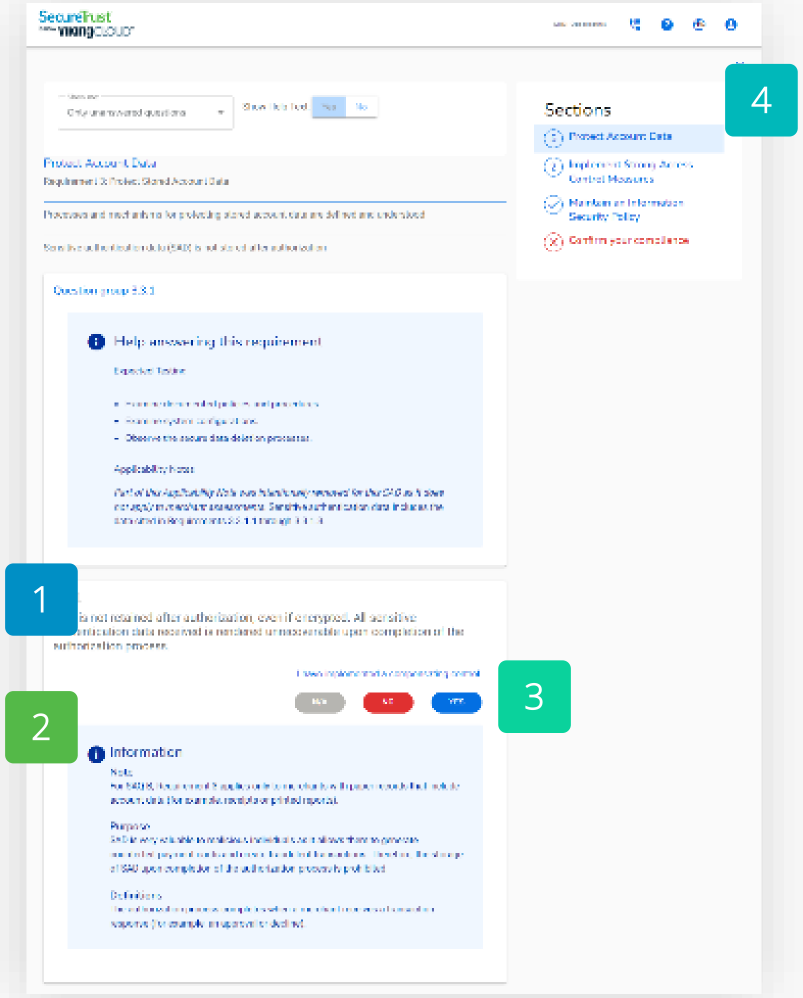
Security Assessment Questionnaire (SAQ)

1

You will be guided through the questions you need to answer to complete your Security Assessment.

2

More information is available via the box underneath to help you understand the question.



Only unanswered questions

Protect Account Data

Requirement 3: Protect Stored Account Data

[illegible]

Sensitive authentication data (SAD) is not stored after authorization

Question group 3.3.1

Help answering this requirement

Expected Testing

- [illegible]
- [illegible]
- Observe the secure data deletion processes.

Applicability Notes

[illegible]

[illegible] is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

I have implemented a compensating control

Information

Note

[illegible]

Purpose

[illegible]

Definitions

[illegible]

4

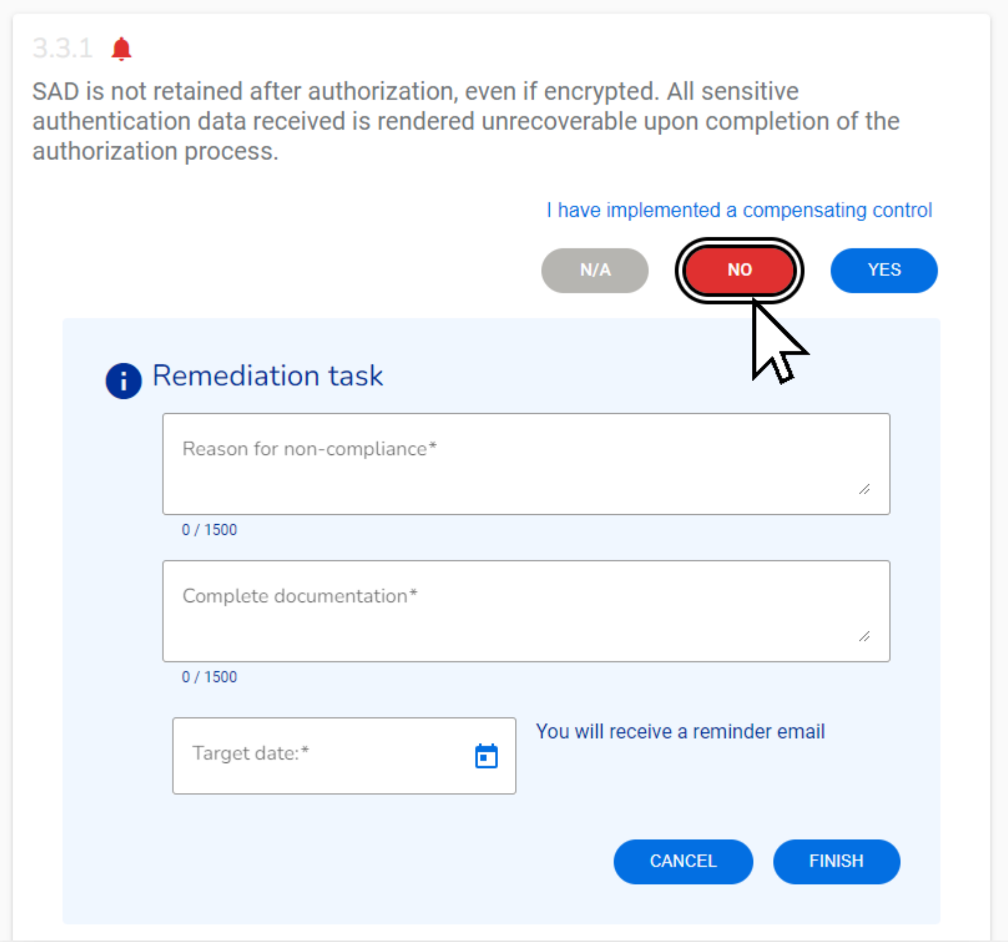
The box on the top right shows your progress through the questionnaire. Many of the questions will have been prepopulated for you based on your answers in the profile section. This greatly streamlines the process.

3

Work your way through the questionnaire by answering “Yes”, “No” or “N/A” to the questions.

Security Assessment Questionnaire (SAQ)

- If an answer you provide is against best practice, you may need to further explain your answer or assign yourself a remediation task.
  - You must then fill out your reasons for non-compliance, the remediation action you intend to take and can then set a reminder to yourself to follow up.
- You can continue with your assessment questions. However, until these tasks are completed correctly you may not be able to complete your assessment.



3.3.1

SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

I have implemented a compensating control

Remediation task

Reason for non-compliance*

0 / 1500

Complete documentation*

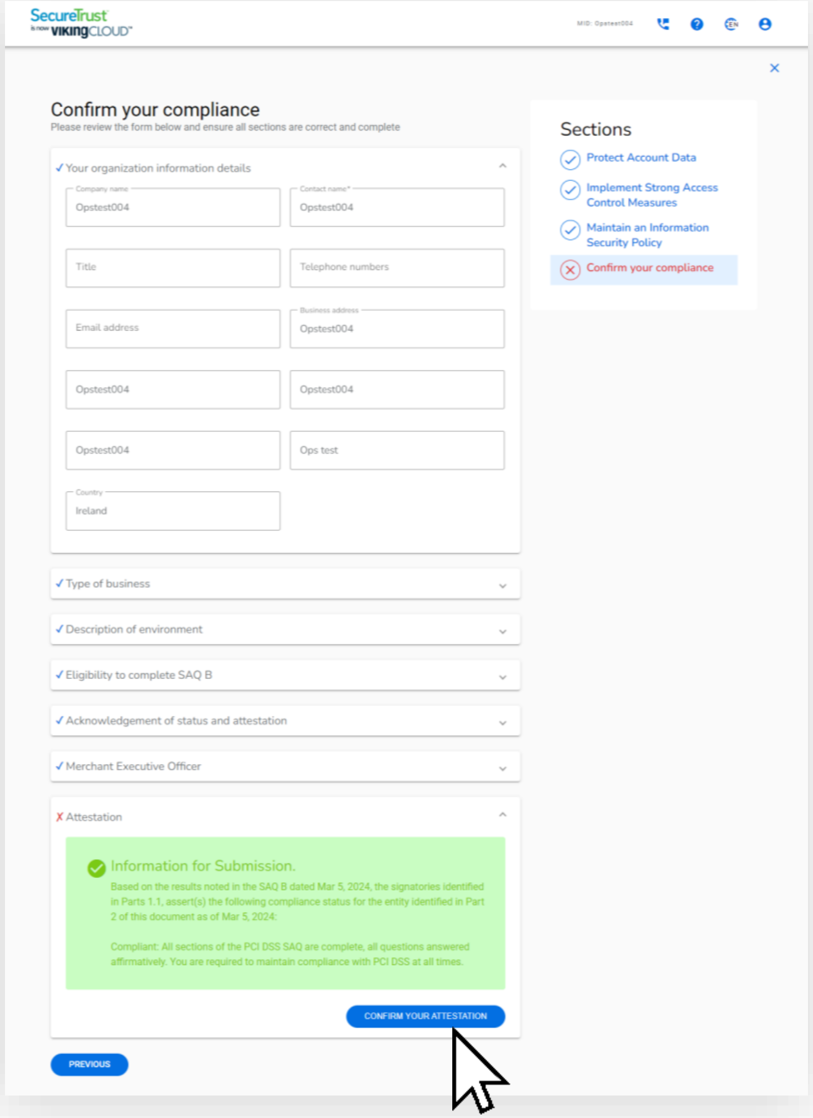
0 / 1500

Target date:*

You will receive a reminder email

Security Assessment Questionnaire (SAQ)

- Once you have answered all your questions correctly, you will need to attest to your compliance. This simply means to confirm the information you have provided is correct.
- You can review all the answers you provided to the questions on this page.
- Once happy, select ‘Confirm your Attestation’ at the bottom of the screen.



Confirm your compliance

Please review the form below and ensure all sections are correct and complete

✓ Your organization information details

Company name: Opstest004

Contact name*: Opstest004

Title

Telephone numbers

Email address

Business address: Opstest004

Opstest004

Opstest004

Opstest004

Ops test

Country: Ireland

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ B

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✗ Attestation

Information for Submission.

Based on the results noted in the SAQ B dated Mar 5, 2024, 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 Mar 5, 2024:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively. You are required to maintain compliance with PCI DSS at all times.

Next Steps

You’ve validated your compliance

Your SAQ is valid for one-year.

If scanning is required for your business, a passing scan is required every 90-days.

Your renewal date will be shown on your dashboard.

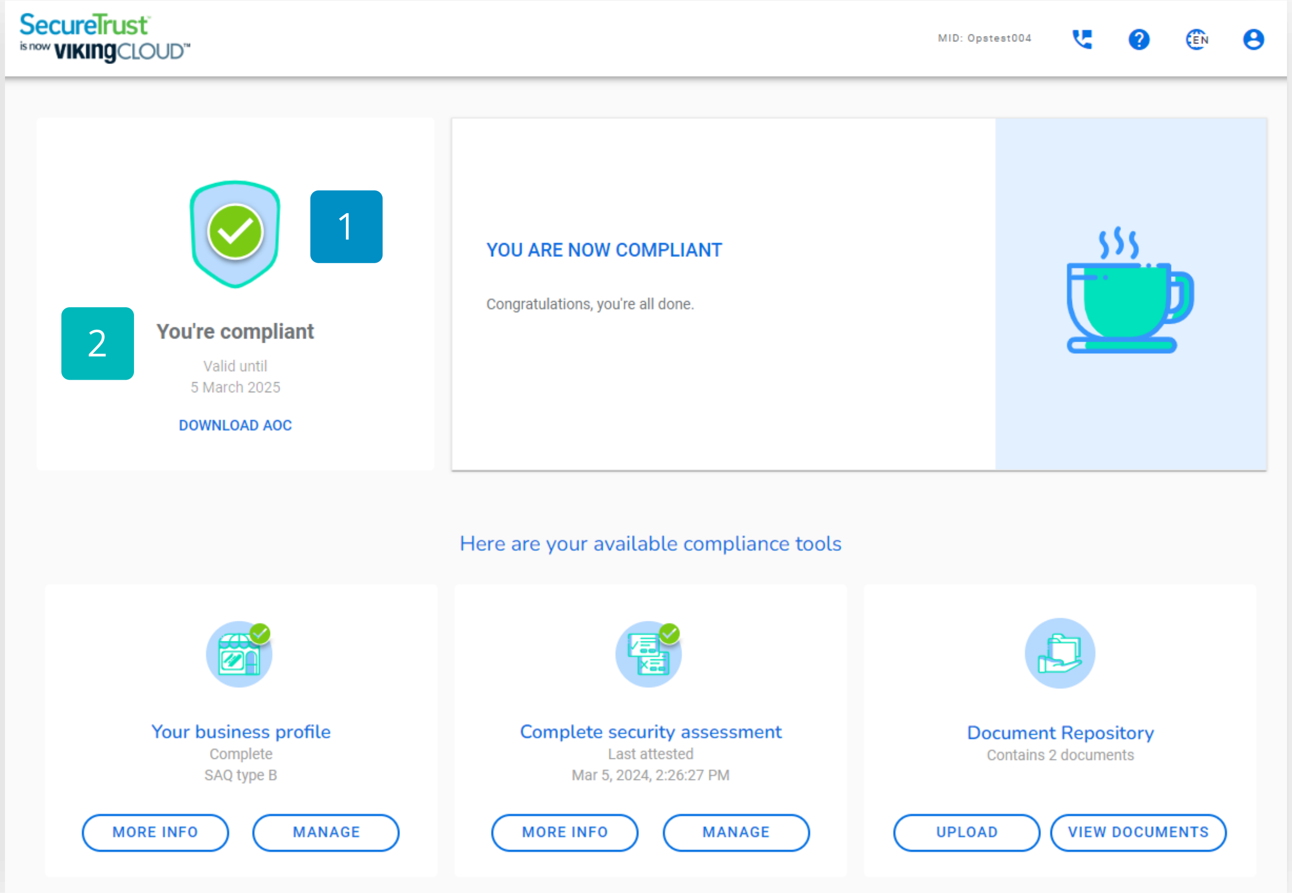
We will email you to remind you when it’s time to revalidate.

- ✓ Profile
- ✓ Scanning
- ✓ Security Assessment
- ✓ Compliance

You’re done for now

1

Your dashboard should have green ticks across the board.



You're compliant

Valid until
5 March 2025

YOU ARE NOW COMPLIANT

Congratulations, you're all done.

Here are your available compliance tools

Your business profile
Complete
SAQ type B

Complete security assessment
Last attested
Mar 5, 2024, 2:26:27 PM

Document Repository
Contains 2 documents

2

Your revalidation date is displayed in the top left corner widget.

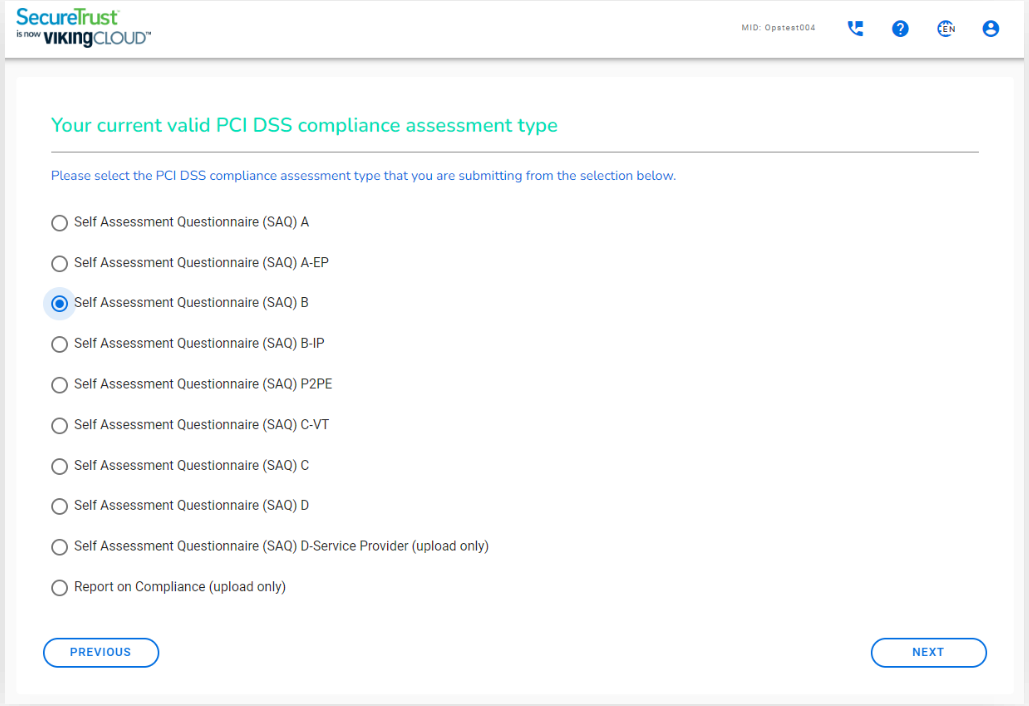
Uploading an Existing Attestation

Already have a valid Attestation of Compliance?

**If applicable under your Acquirer Program.*

Uploading existing Attestation of Compliance

- If you select that you have an existing attestation of compliance, you will then be asked some questions:
  - The PCI Compliance assessment type of your business. You can find this on your existing certificate.
  - You'll also need to confirm if you use a third party to store or process card payments.
  - You may also have to answer additional questions depending on your previous answers.
- You'll then arrive at your dashboard. The main widget will instruct you to confirm your compliance.
  - Select 'Begin Step' to start.



Your current valid PCI DSS compliance assessment type

Please select the PCI DSS compliance assessment type that you are submitting from the selection below.

○ Self Assessment Questionnaire (SAQ) A

○ Self Assessment Questionnaire (SAQ) A-EP

● Self Assessment Questionnaire (SAQ) B

○ Self Assessment Questionnaire (SAQ) B-IP

○ Self Assessment Questionnaire (SAQ) P2PE

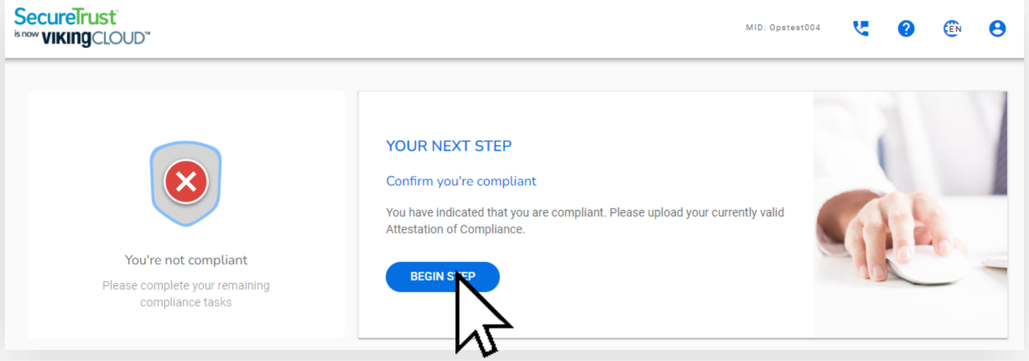
○ Self Assessment Questionnaire (SAQ) C-VT

○ Self Assessment Questionnaire (SAQ) C

○ Self Assessment Questionnaire (SAQ) D

○ Self Assessment Questionnaire (SAQ) D-Service Provider (upload only)

○ Report on Compliance (upload only)



You're not compliant

Please complete your remaining compliance tasks

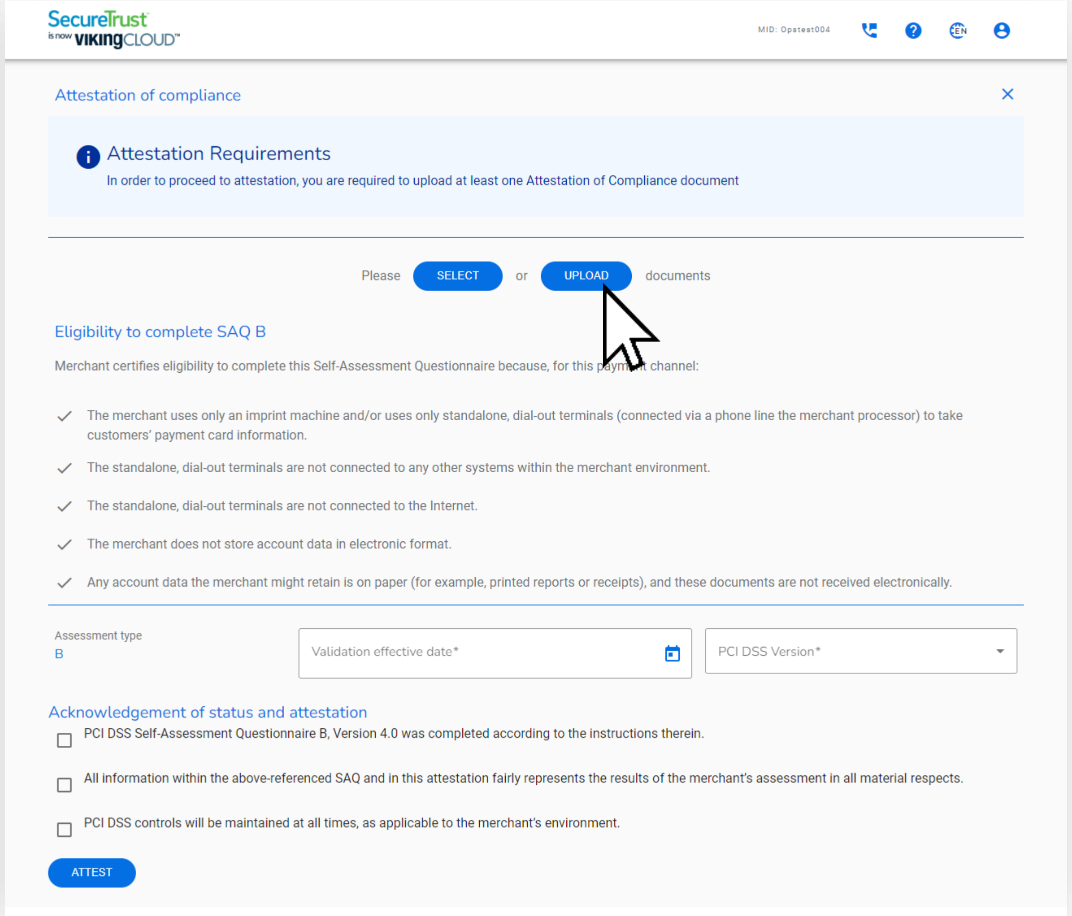
YOUR NEXT STEP

Confirm you're compliant

You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance.

Uploading existing Attestation of Compliance

- On the following page you will need to complete some steps:
  - Upload your existing documents.
  - You will need to upload your Attestation of Compliance (AoC) that proves you are currently compliant.
  - Confirm the details, acknowledge your status and attest to your compliance.
- **Instructions on the following pages.**



Attestation of compliance ✕

Attestation Requirements

In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please SELECT or UPLOAD documents

Eligibility to complete SAQ B

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

- ✓ The merchant uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line the merchant processor) to take customers' payment card information.
- ✓ The standalone, dial-out terminals are not connected to any other systems within the merchant environment.
- ✓ The standalone, dial-out terminals are not connected to the Internet.
- ✓ The merchant does not store account data in electronic format.
- ✓ Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Assessment type
B

Validation effective date*

PCI DSS Version*

Acknowledgement of status and attestation

□ PCI DSS Self-Assessment Questionnaire B, Version 4.0 was completed according to the instructions therein.

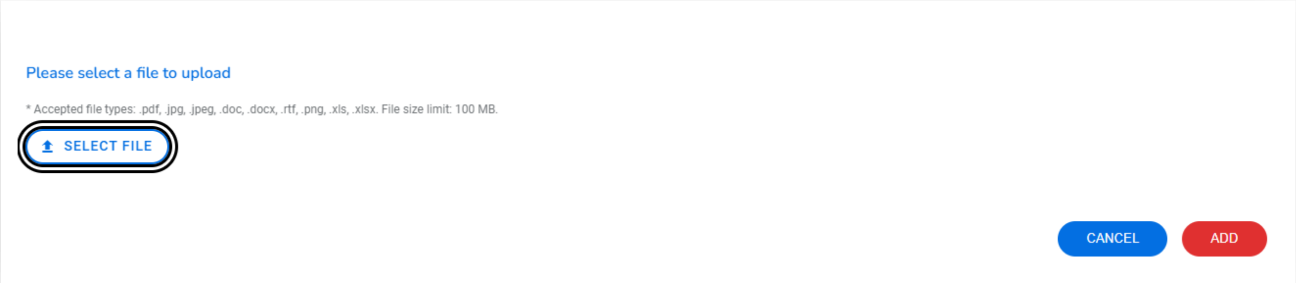
□ All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.

□ PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

ATTEST

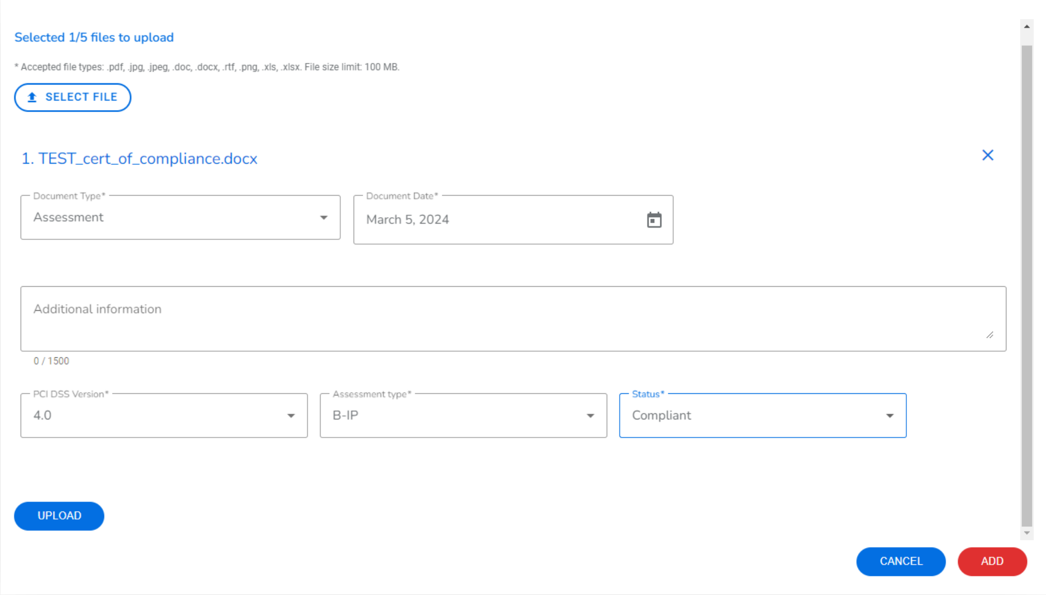
Uploading existing Attestation of Compliance

- Upload your documents
  - Select ‘Upload’ highlighted on the previous page
  - Select the necessary document(s) from your files
  - Provide details of the document you are uploading and select ‘Upload’
  - The document is now attached to your attestation



Please select a file to upload

* Accepted file types: .pdf, .jpg, .jpeg, .doc, .docx, .rtf, .png, .xls, .xlsx. File size limit: 100 MB.



Selected 1/5 files to upload

* Accepted file types: .pdf, .jpg, .jpeg, .doc, .docx, .rtf, .png, .xls, .xlsx. File size limit: 100 MB.

1. TEST_cert_of_compliance.docx

Document Type*: Assessment

Document Date*: March 5, 2024

Additional information

0 / 1500

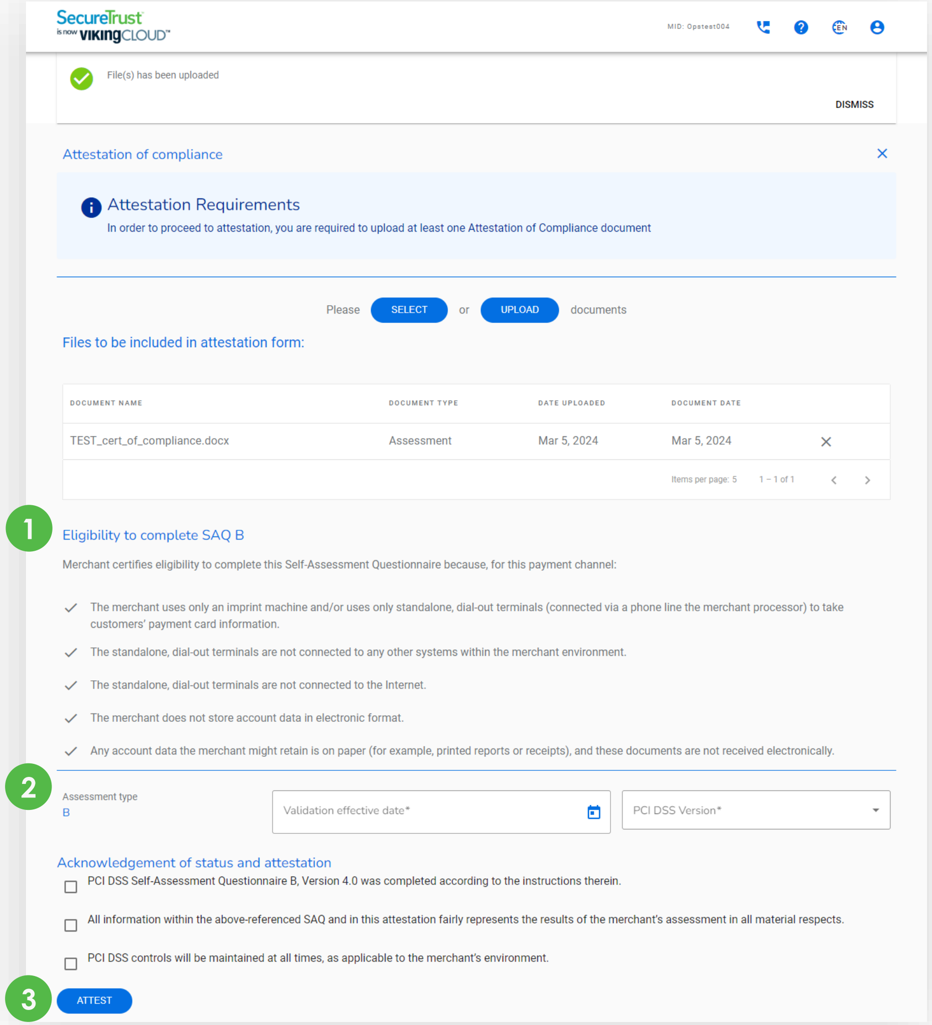
PCI DSS Version*: 4.0

Assessment type*: B-IP

Status*: Compliant

Uploading existing Attestation of Compliance

- Confirm details of your attestation, including:
  - Assessment type.
  - Validation effective date.
  - The version of the PCI DSS to which you are compliant with.
- Confirm by checking the boxes, that you acknowledge a number of conditions in relation to your status and attestation.
- Click 'Attest' to finish. Your validation is now complete.



File(s) has been uploaded

Attestation of compliance

Attestation Requirements

In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please SELECT or UPLOAD documents

Files to be included in attestation form:

DOCUMENT NAME	DOCUMENT TYPE	DATE UPLOADED	DOCUMENT DATE	
TEST_cert_of_compliance.docx	Assessment	Mar 5, 2024	Mar 5, 2024	×

Items per page: 5 1 – 1 of 1

1 Eligibility to complete SAQ B

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

- ✓ The merchant uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line the merchant processor) to take customers' payment card information.
- ✓ The standalone, dial-out terminals are not connected to any other systems within the merchant environment.
- ✓ The standalone, dial-out terminals are not connected to the Internet.
- ✓ The merchant does not store account data in electronic format.
- ✓ Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

2 Assessment type: B | Validation effective date* | PCI DSS Version*

Acknowledgement of status and attestation

- □ PCI DSS Self-Assessment Questionnaire B, Version 4.0 was completed according to the instructions therein.
- □ All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
- □ PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

3 ATTEST

Thank you!