

# PCI Portal

User Guide for Merchants

# Table of Contents

- 3 What's included?
- 4 The process
- 5 Login
- 6 Your profile
- 12 Your dashboard
- 16 Scanning
- 20 Security Assessment Questionnaire (SAQ)
- 27 You're done for now
- 28 Upload an existing certificate



# 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

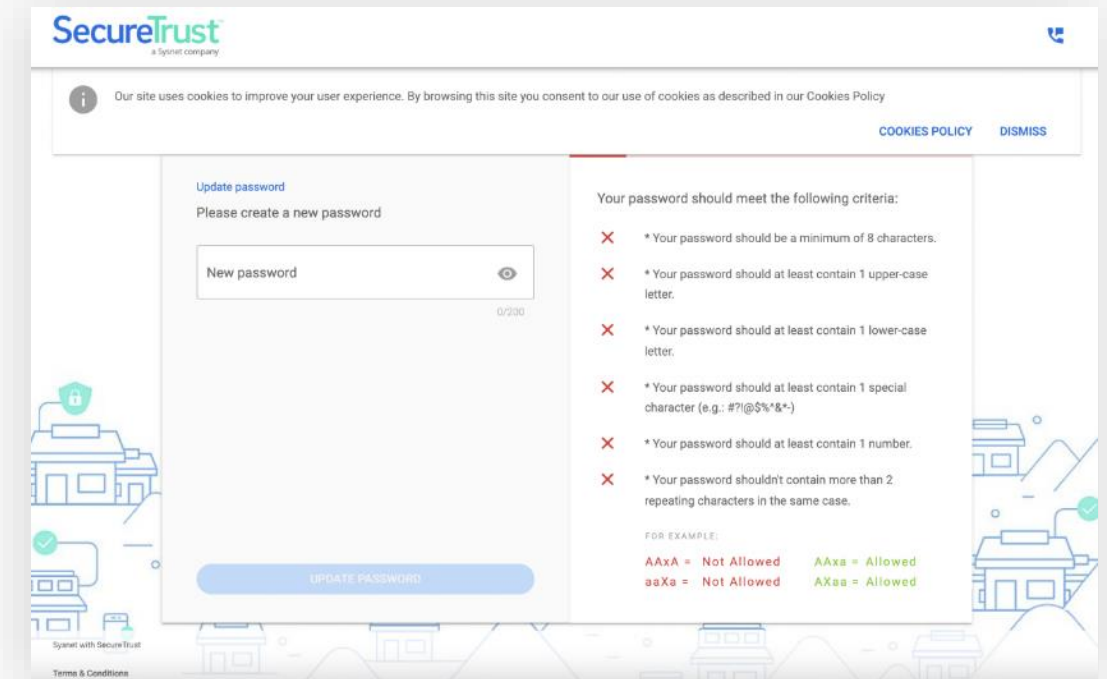
5

**Maintenance**

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

# Login

- You will receive an email prompting you to login to the upgraded portal. To login, please use your existing username and create a new password.
- Once you have selected your password you can then login to the portal.
- Once logged in, you will be brought to an information page that gives you an overview of what you need to do and an information video.
- Click 'Start Business Profile' to begin.



The screenshot shows the SecureTrust password update page. At the top, there is a cookie consent banner. Below it, the 'Update password' section prompts the user to create a new password. A text input field labeled 'New password' is shown with a character count of 0/200. To the right, a list of password criteria is displayed, each with a red 'X' indicating it is not met. The criteria include: minimum 8 characters, at least 1 upper-case letter, at least 1 lower-case letter, at least 1 special character, at least 1 number, and no more than 2 repeating characters in the same case. Examples show 'AAxA' and 'aaXa' as not allowed, while 'AAXa' and 'AXaa' are allowed. The page also features a 'UPDATE PASSWORD' button and a 'Terms & Conditions' link at the bottom.

SecureTrust  
a Syneret company

Our site uses cookies to improve your user experience. By browsing this site you consent to our use of cookies as described in our Cookies Policy [COOKIES POLICY](#) [DISMISS](#)

[Update password](#)

Please create a new password

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

[UPDATE PASSWORD](#)

[Terms & Conditions](#)



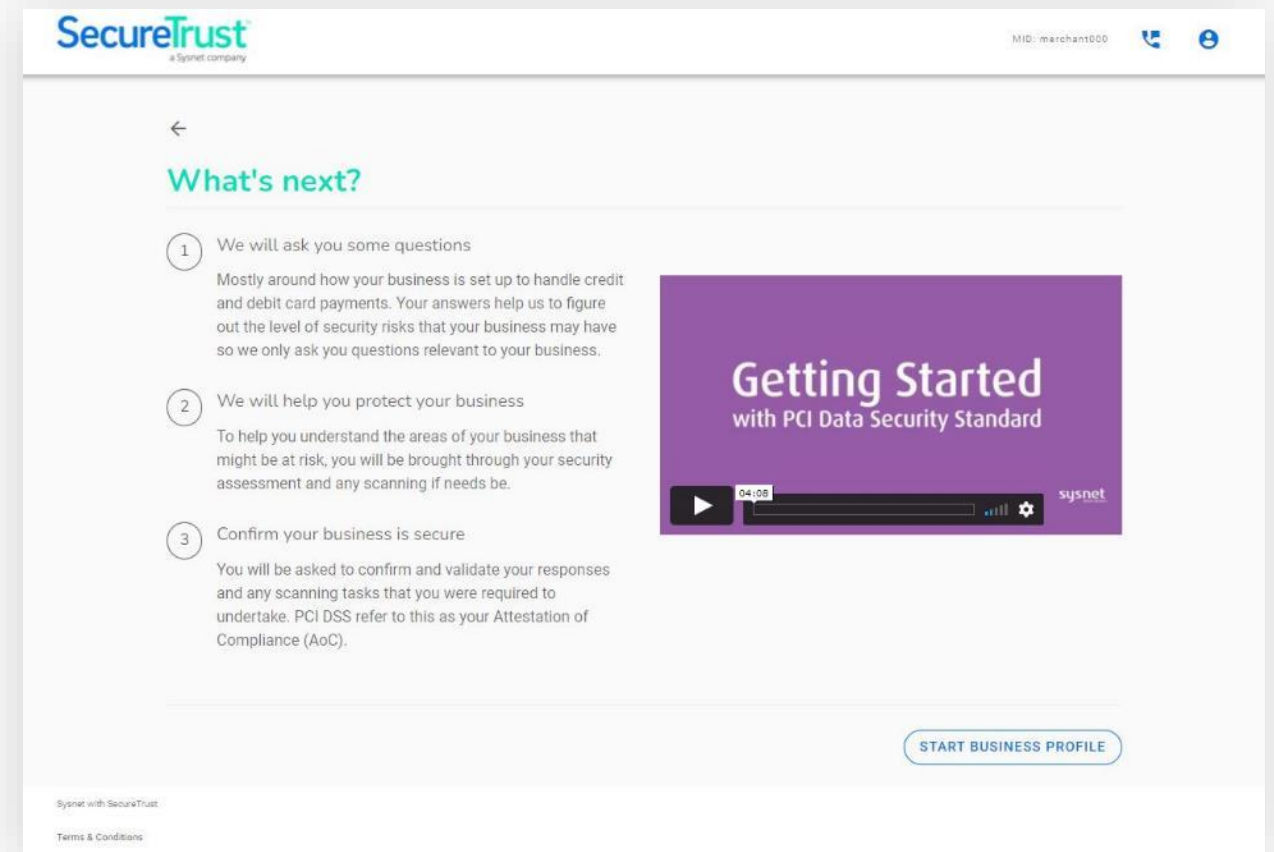
# Your Profile

How you accept payments



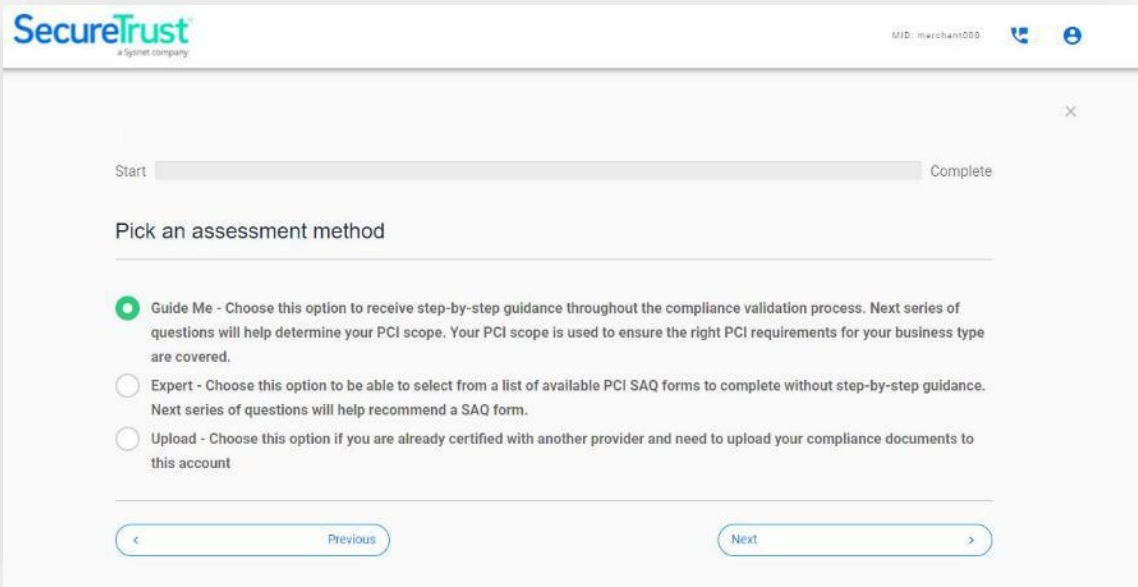
# Start Business Profile

- 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.



# 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 the option and click 'Next'.
- 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.**
- **If you already have a valid certificate, select the third option and proceed to page 28 of this guide for instructions on uploading your existing Attestation of Compliance (AoC).**



The screenshot shows the 'Pick an assessment method' screen in the SecureTrust portal. At the top, the SecureTrust logo is on the left, and 'MID: merchant000' with social media icons is on the right. Below the header is a progress bar with 'Start' and 'Complete' markers. The main heading is 'Pick an assessment method'. There are three radio button options: 'Guide Me' (selected), 'Expert', and 'Upload'. Each option has a descriptive text block. At the bottom, there are 'Previous' and 'Next' navigation buttons.

SecureTrust  
a Symantec company

MID: merchant000

Start Complete

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



# 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.

The screenshot shows a web form titled "What Are The Ways You Accept Credit Card Payments" from SecureTrust. At the top, there is a progress bar from "Start" to "Complete" and a user ID "MID: merchant000". The question is "How do you accept credit cards? Select all that apply." Below this, there are three options, each with a blue circular icon containing a question mark and a computer monitor icon:

- ☒ 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.

At the bottom, there are "Previous" and "Next" buttons.

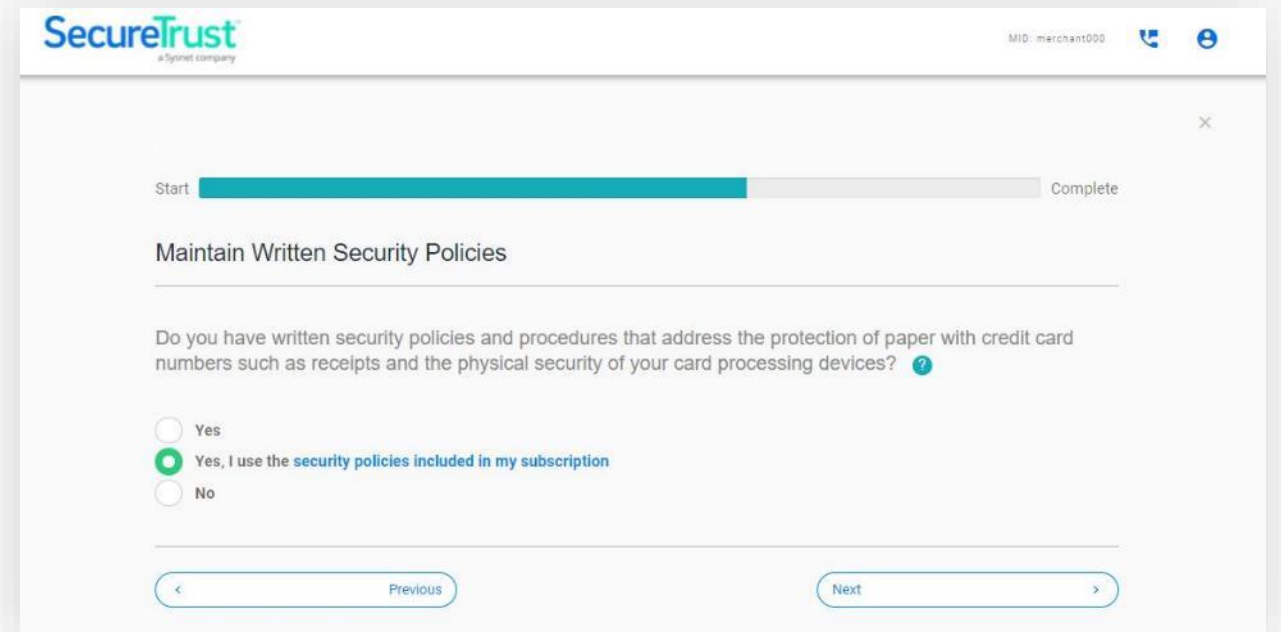
# Your Profile – Payment Summary

- 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.

The screenshot shows a web form titled "SecureTrust" with a progress bar at the top. The progress bar is partially filled with a blue bar, indicating the current step. Below the progress bar, the text "A summary of how and where you handle card payments" is displayed. The form contains three text input fields, each with a "1 / 4000" character count and a help icon. The first field is labeled "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...)" and contains the text "x". The second field is labeled "Generally, how does your business store, process and/or transmit cardholder data?" and contains the text "x". The third field is labeled "Briefly describe the environment and/or systems covered by this assessment" and contains the text "x". At the bottom of the form, there are "Previous" and "Next" buttons.

# 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.



The screenshot shows a web interface for SecureTrust, a Synnet company. The top right corner displays 'MID: merchant000' and a user icon. A progress bar at the top indicates the setup is approximately 75% complete, with 'Start' and 'Complete' labels. The main heading is 'Maintain Written Security Policies'. The question asks: 'Do you have written security policies and procedures that address the protection of paper with credit card numbers such as receipts and the physical security of your card processing devices?'. There are three radio button options: 'Yes', 'Yes, I use the security policies included in my subscription' (which is selected), and 'No'. At the bottom, there are 'Previous' and 'Next' navigation buttons.



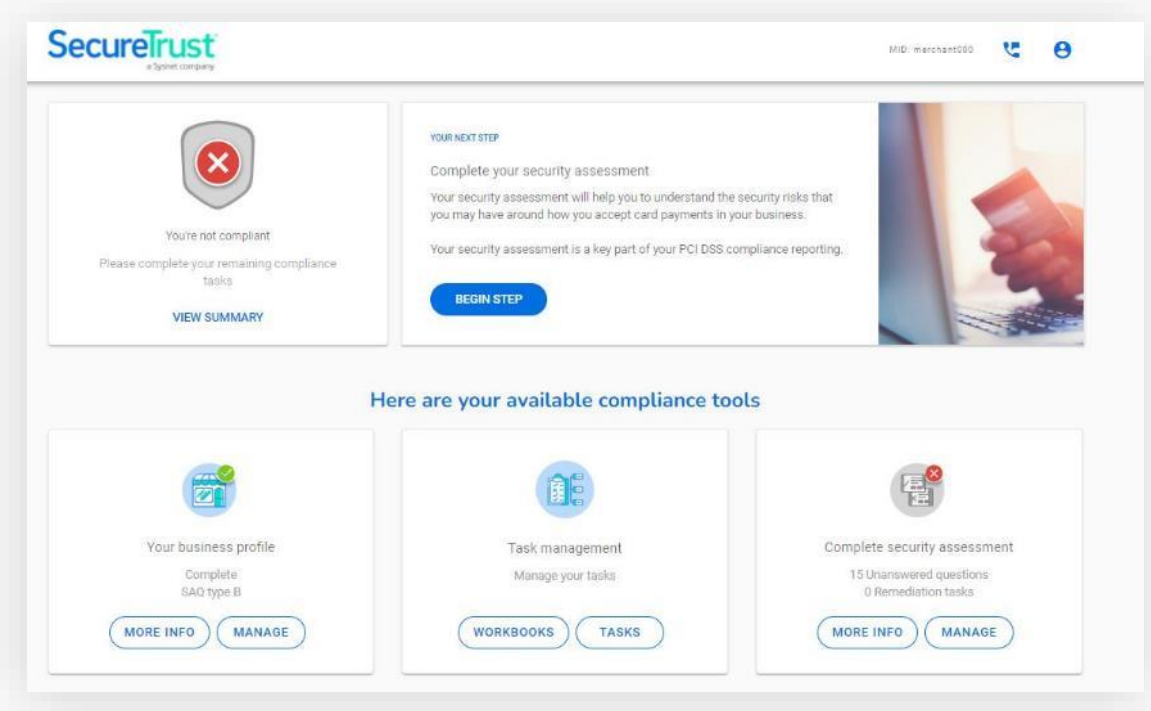
# Your Dashboard

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.



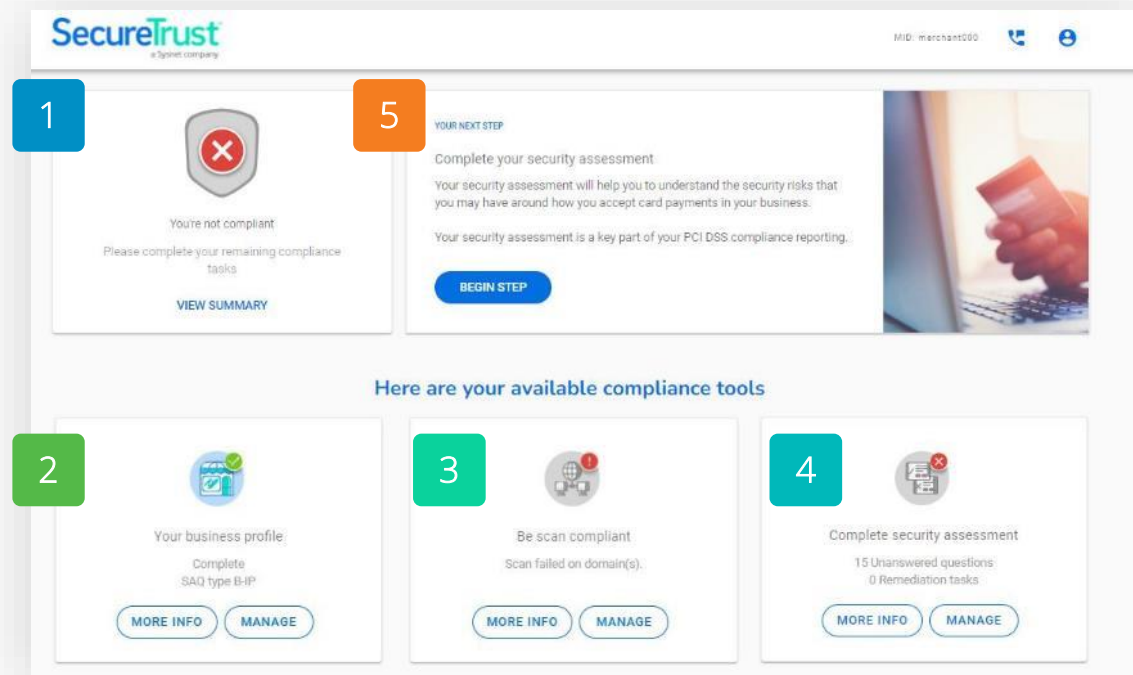
# Your Dashboard

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'.



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

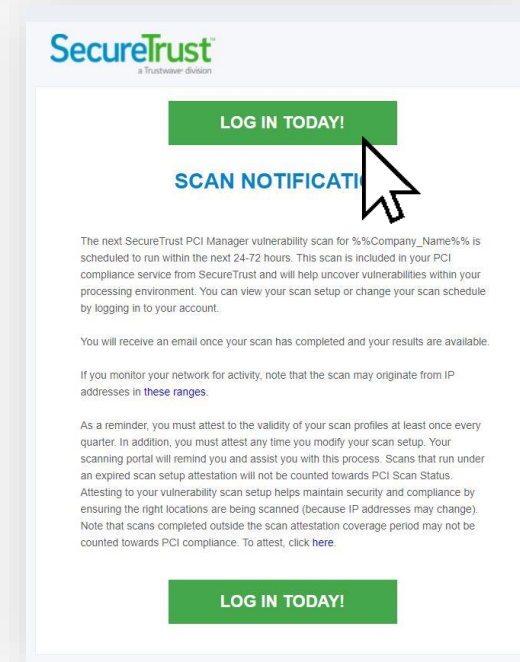
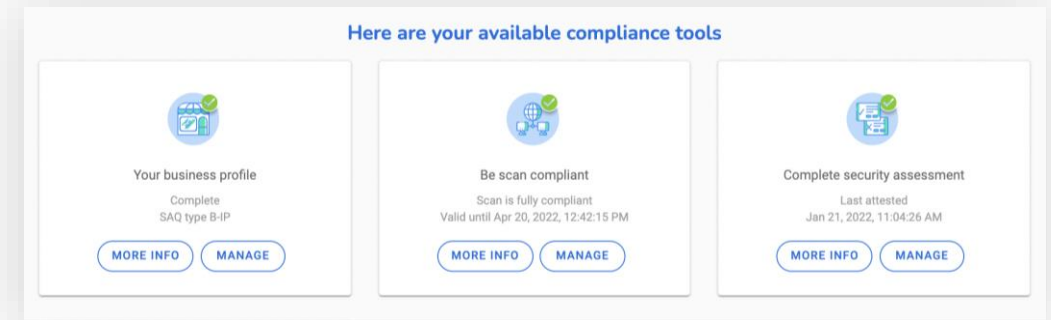
Carrying over your scanning and SAQ completion





# Scanning and SAQ

- As part of your upgrade, your current PCI Scan Status, scanning targets, historical completed scans and SAQs have been transferred 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.



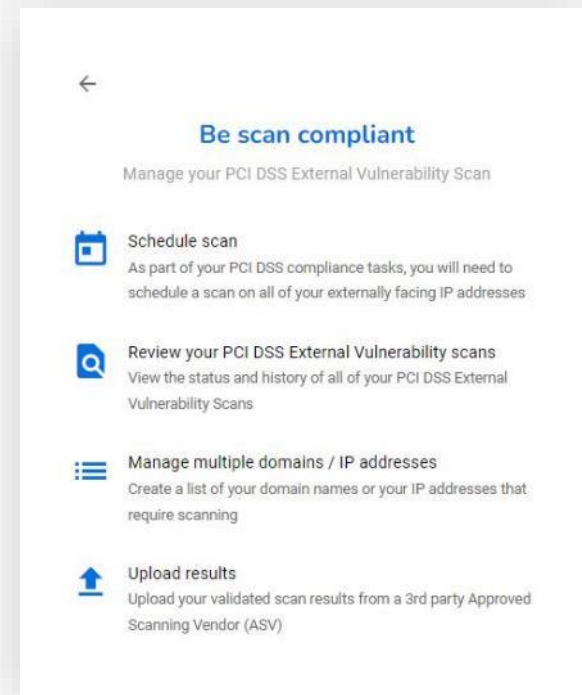
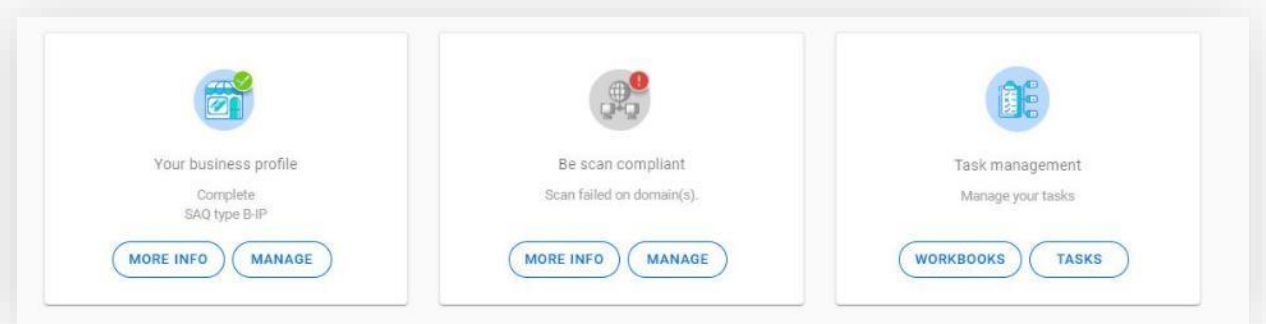


# External Vulnerability Scanning



# Scanning

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



# 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.

SecureTrust  
A Sprint Company

102: merchant100

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.

87.106.218.170

Domain / IP address **Add**

Scan date

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

Jan 14, 2022 15 : 53

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, you need to grant access to the IP addresses listed below.

If you use security software such as a 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 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  
64.39.106.0/24  
154.59.121.0/24

**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.

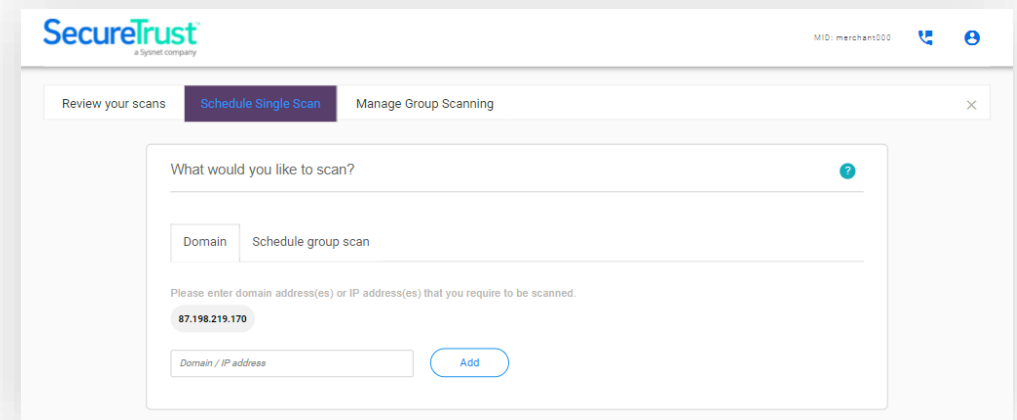
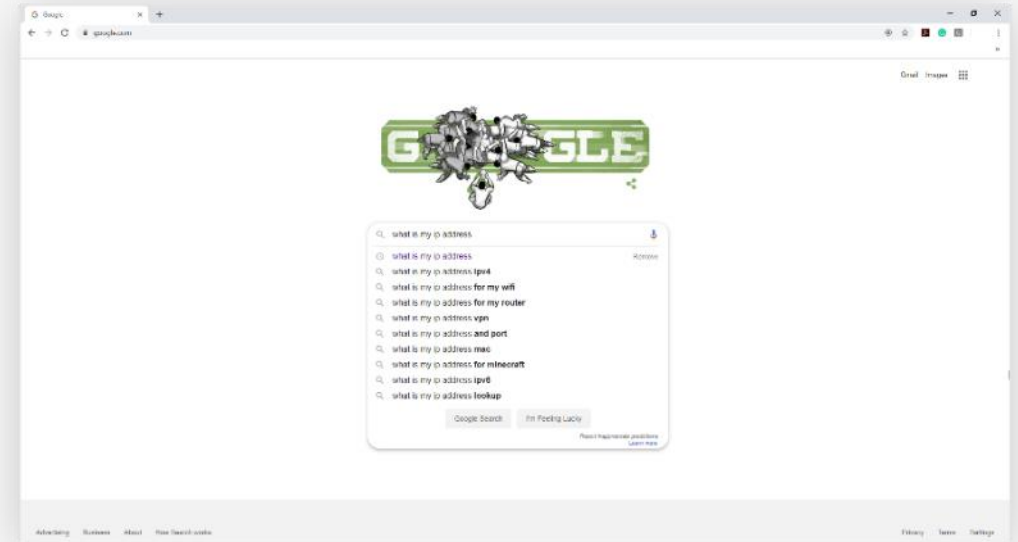
Warranties and Liability

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

**Schedule Scan**

# 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





# 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



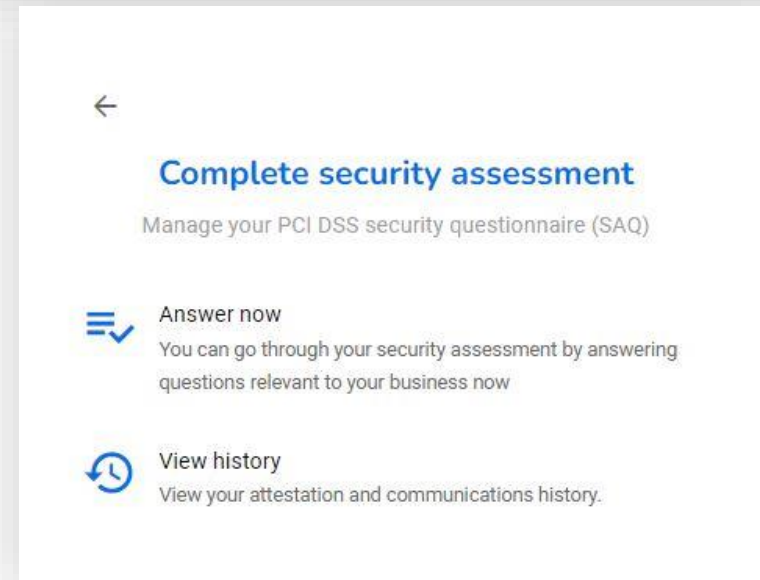
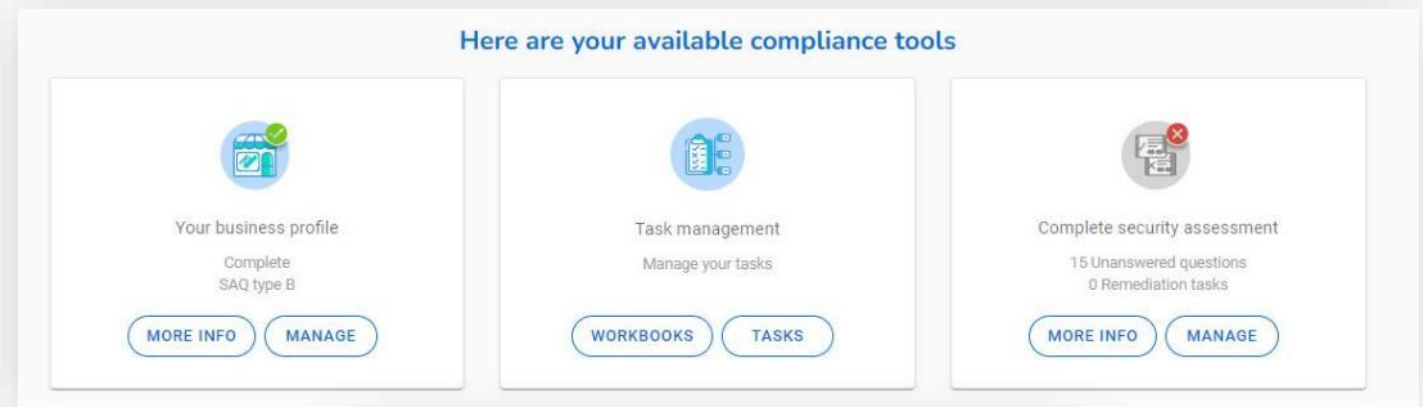
Security Assessment – **Page 22**



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.





# 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.

The screenshot shows the SecureTrust SAQ interface. At the top, the SecureTrust logo is on the left, and the user ID 'MID: merchant003' is on the right. Below the logo, there's a 'Show me:' dropdown set to 'Only unanswered questions' and a 'Show Help Text:' toggle switch that is turned on. A note below says 'Please note, some answered questions may remain shown in order to provide appropriate context status'. The main content area is titled 'Protect Cardholder Data' with the subtitle 'Protect stored cardholder data'. Below this is the question '3.2(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?'. At the bottom of the question are three buttons: 'N/A', 'No', and 'Yes'. To the right of the question is a 'Milestones' sidebar showing a progress list: 'Protect Cardholder Data' (5), 'Implement Strong Access Control Measures' (9), 'Maintain an Information Security Policy' (1), and 'Confirm your compliance' (marked with a red X). Below the question is an 'Information' box with the title 'PCI Council Guidelines' and text explaining that entities that issue payment cards or support issuing services will often create and control sensitive authentication data as part of the issuing function. It also notes that it is allowable for companies to store sensitive authentication data ONLY if they have a legitimate business need to store such data. At the bottom of the information box is the text 'PCI Audit Procedures'.

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.

3.2(c) 🔔

Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?

**Remediation task**

**Reason for non-compliance**

Unable to complete documentation on time

0 / 1500

**Remediation Action**

Complete documentation

0 / 1500

**Target date:**

Jan 14, 2022 📅 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.

SecureTrust  
1400 merchant000

### Confirm your compliance

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

✓ Your organization information details

Company name: merchant000 | Contact name: contactmerchant000

Title: | Telephone numbers: |

Email address: test@sysnet.ie | Business address: 0 Main Street

0 Main Street 2 | 0 Main Street 3

0 Main Street 4 | 0 Main Street 5

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 Jan 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 Jan 14, 2022:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating. thereby merchant000 has demonstrated full compliance with the PCI DSS.

**CONFIRM YOUR ATTESTATION**

PREVIOUS

#### Sections

- ✓ Protect Cardholder Data
- ✓ Implement Strong Access Control Measures
- ✓ Maintain an Information Security Policy
- ✓ Confirm your compliance

Copyright © 2022 - All Rights Reserved - Strictly Confidential - Do Not Distribute

# 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

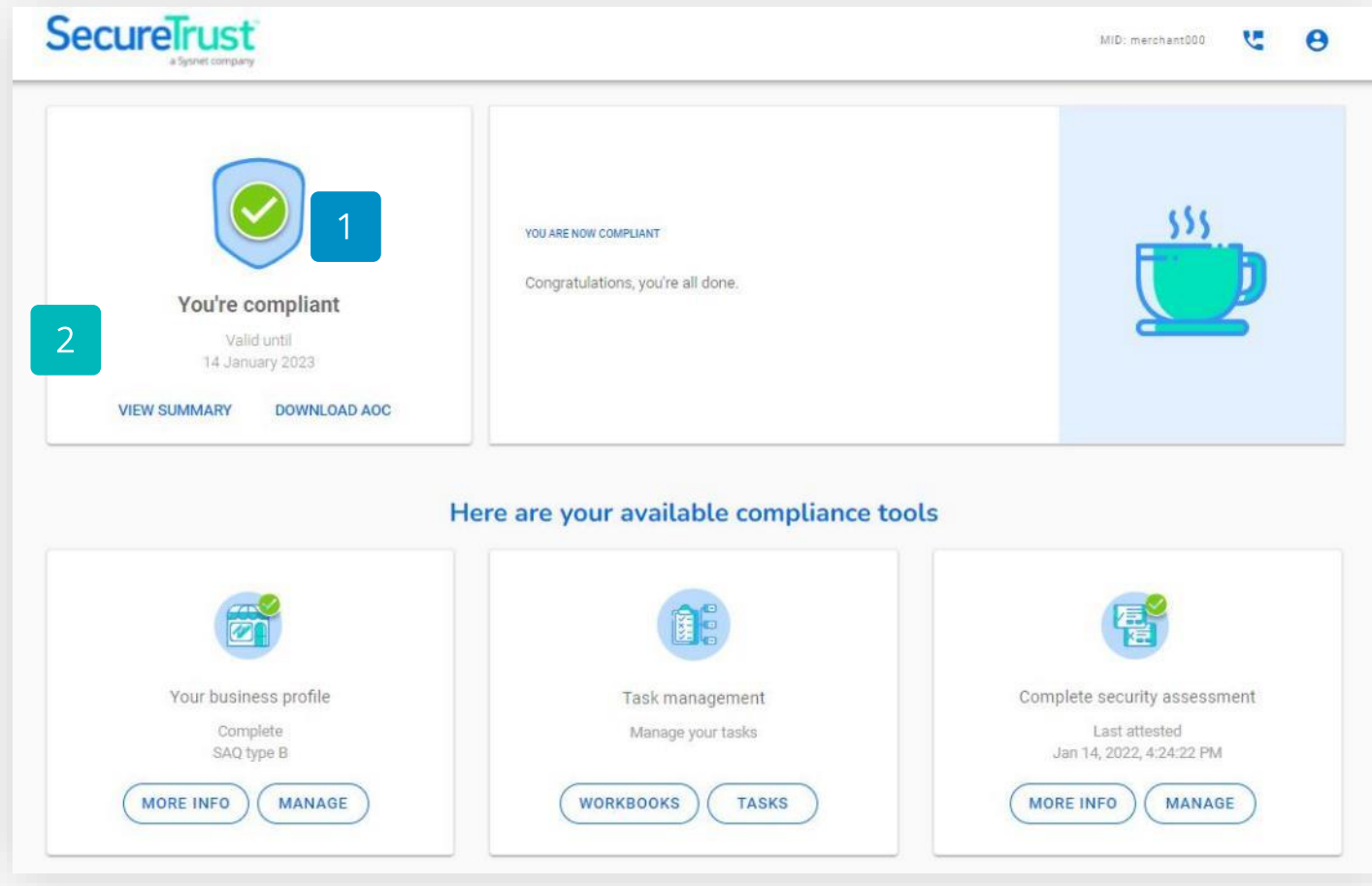


Compliance

# You're done for now

1

Your dashboard should have green ticks across the board.



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.

The image shows two screenshots of the SecureTrust interface. The top screenshot is a form titled 'Your current valid PCI compliance type'. It features a progress bar at the top, a list of radio button options for different PCI assessment types, and 'Previous' and 'Next' navigation buttons at the bottom. The bottom screenshot shows the main dashboard with a 'You're not compliant' warning, a 'VIEW SUMMARY' link, and a 'BEGIN STEP' button highlighted by a mouse cursor.

**SecureTrust**  
a Symantec company

MID: merchant000

Start Complete

Your current valid PCI compliance type

Please select the PCI Compliance assessment type that you are currently valid for from the selection below.

- ☐ Self Assessment Questionnaire (SAQ) A
- ☐ Self Assessment Questionnaire (SAQ) P2PE
- ☒ Self Assessment Questionnaire (SAQ) B
- ☐ Self Assessment Questionnaire (SAQ) C-VT
- ☐ Self Assessment Questionnaire (SAQ) B-IP
- ☐ Self Assessment Questionnaire (SAQ) A-EP
- ☐ Self Assessment Questionnaire (SAQ) C
- ☐ Self Assessment Questionnaire (SAQ) D
- ☐ Self Assessment Questionnaire (SAQ) D-Service Provider
- ☐ Report on Compliance (RoC)

[< Previous](#) [Next >](#)

**SecureTrust**  
a Symantec company

MID: merchant000

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

**YOUR NEXT STEP**  
Confirm you're compliant  
You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance.  
[BEGIN STEP](#)

# 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.**

SecureTrust  
a Symantec company

MID: merchant060

## 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 shortened version of the Self-Assessment Questionnaire because:

- ✓ Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data either over a phone; and/or
- ✓ Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
- ✓ Merchant does not transmit cardholder data over a network (either an internal network or the Internet);
- ✓ Merchant does not store cardholder data in electronic format; and
- ✓ If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically

**Attestation details:**

Assessment type: B  
Validation effective date:   
PCI DSS Version:

**Acknowledgement of status and attestation**

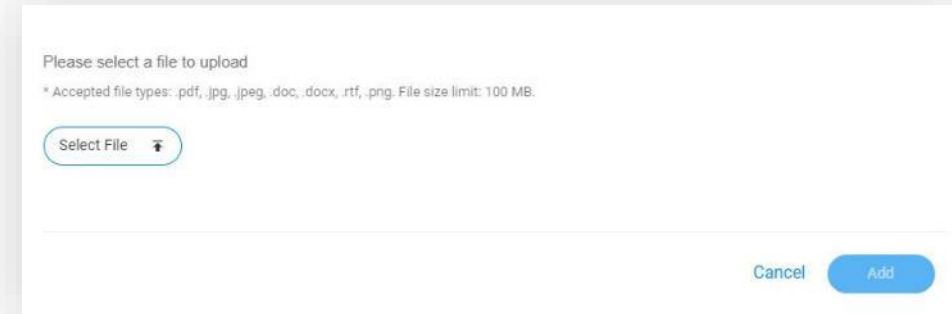
- ☐ PCI DSS Self-Assessment Questionnaire SAQ B, Version 3.2.1 has been completed according to the instructions therein.
- ☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- ☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorisation.
- ☐ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- ☐ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- ☐ No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

[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

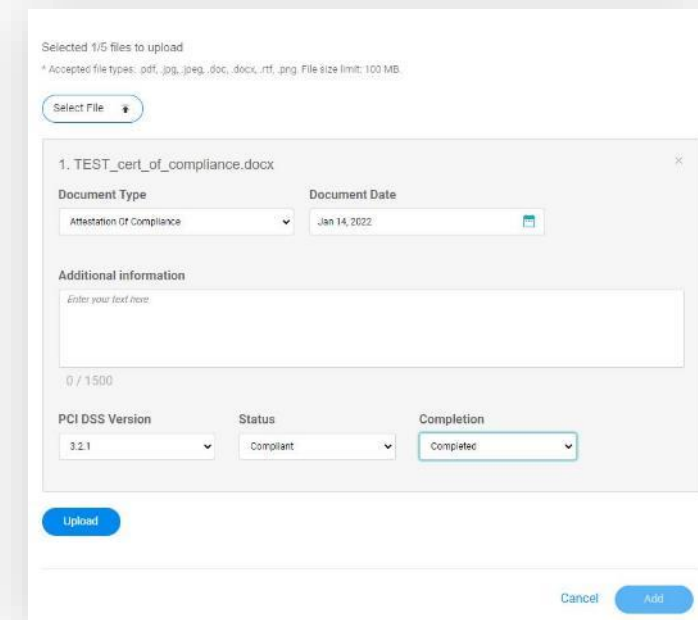


Please select a file to upload

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

Select File

Cancel Add



Selected 1/5 files to upload

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

Select File

1. TEST\_cert\_of\_compliance.docx

Document Type: Attestation Of Compliance

Document Date: Jan 14, 2022

Additional information

Enter your text here:

0 / 1500

PCI DSS Version: 3.2.1

Status: Compliant

Completion: Completed

Upload

Cancel Add

# 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.

SecureTrust  
a tycoor company

WID: merchant000

## Attestation of compliance

**1 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_001_of_compliance.docx	Attestation Of Compliance	Jan 14, 2022	Jan 14, 2022

(Items: 1 / 1)

**Eligibility to complete SAQ B**

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- ✓ Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data either over a phone, and/or
- ✓ Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
- ✓ Merchant does not transmit cardholder data over a network (either an internal network or the Internet);
- ✓ Merchant does not store cardholder data in electronic format; and
- ✓ If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically

**1 Attestation details:**

Assessment type: **B**

Validation effective date:

PCI DSS Version:

**2 Acknowledgement of status and attestation**

☐ PCI DSS Self-Assessment Questionnaire SAQ B, Version 3.2.1 has been completed according to the instructions therein.

☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☐ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☐ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

☐ No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

**3 Attest**



**Thank you!**