



SecureTrust SAQ A Instruction Guide

Purpose: These instructions will assist in registering your account for PCI compliance, validating PCI Compliance readiness, and completing the annual PCI questionnaire for merchants that utilize a software integration with the NMI payment gateway.

SAQ A Instructions


1. Click **Begin Step**.

YOUR NEXT STEP

[Check your business profile](#)

Answer a few simple questions about your business to help us determine the type of security assessment you need to complete.

BEGIN STEP



2. Click **Start Business Profile**.

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).

START BUSINESS PROFILE

3. Click the circle next to “Expert” and then click Next.

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

NEXT

4. Click the circle next to “Self Assessment Questionnaire (SAQ) A” and click Next.

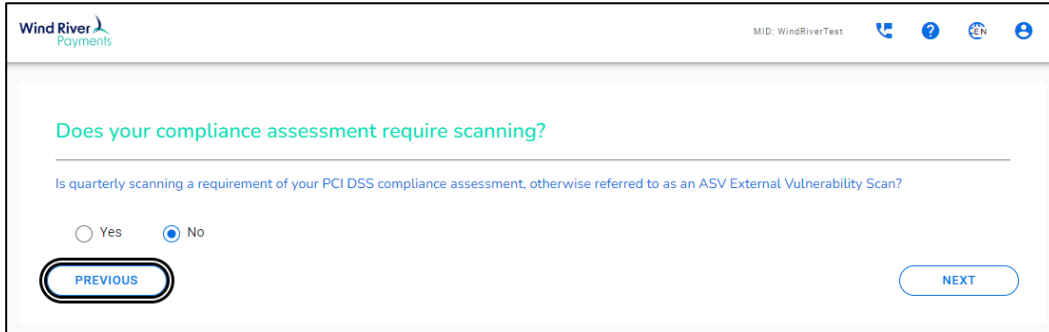
Your current valid PCI DSS compliance assessment type

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)

PREVIOUS NEXT

5. Scanning is not required. Select No.



Wind River Payments MID: WindRiverTest

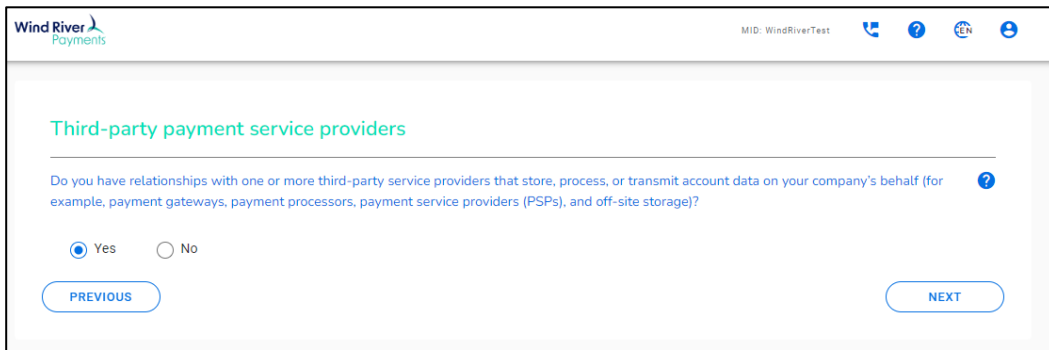
Does your compliance assessment require scanning?

Is quarterly scanning a requirement of your PCI DSS compliance assessment, otherwise referred to as an ASV External Vulnerability Scan?

Yes No

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

6. Answer the **Third-Party Payment Service Providers** question.



Wind River Payments MID: WindRiverTest

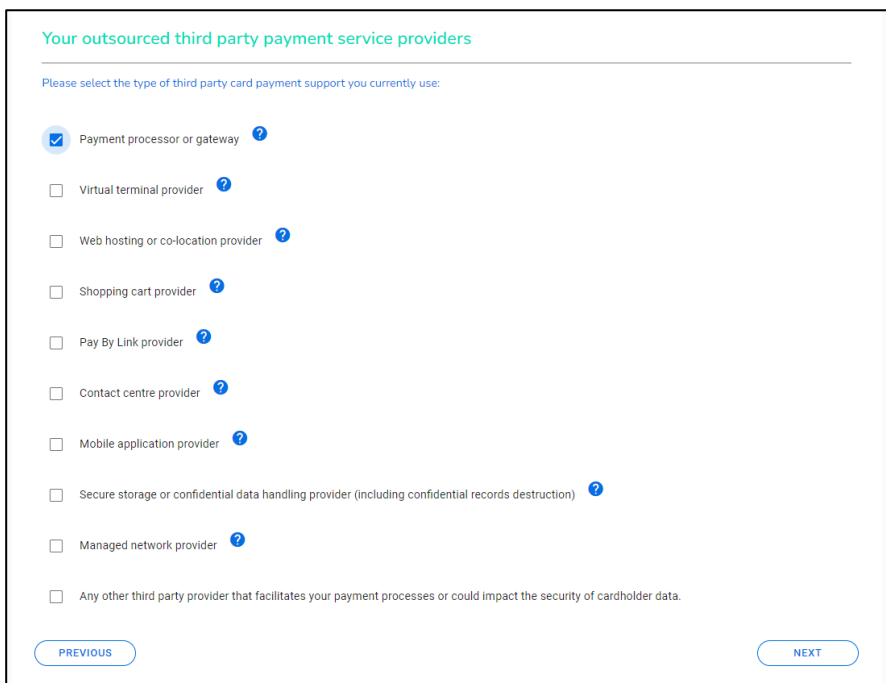
Third-party payment service providers

Do you have relationships with one or more third-party service providers that store, process, or transmit account data on your company's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)?

Yes No

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

7. Select **Payment Processor or Gateway**.



Your outsourced third party payment service providers

Please select the type of third party card payment support you currently use:

- Payment processor or gateway
- Virtual terminal provider
- Web hosting or co-location provider
- Shopping cart provider
- Pay By Link provider
- Contact centre provider
- Mobile application provider
- Secure storage or confidential data handling provider (including confidential records destruction)
- Managed network provider
- Any other third party provider that facilitates your payment processes or could impact the security of cardholder data.

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

8. Type **Network Merchants LLC** in the **Filter** box.

Your payment gateway/processor ?

Please select all of your payment gateway/processor(s) below

Filter

- 1 & 1 Internet AG
- 1 Link (Guarantee) Limited
- 1ShoppingCart.com
- 1st Americard Inc.
- 2000Charge Inc.
- 24 Solutions AB
- 2C2P (Thailand) Co. Ltd
- 2Checkout Inc.
- 3 Delta Systems Inc.
- 3C Payment Luxembourg S.A.

PREVIOUS NEXT

9. Select **Network Merchants LLC**.

Your payment gateway/processor ?

Please select all of your payment gateway/processor(s) below

Network Merchants

- Network Merchants LLC

PREVIOUS NEXT

10. Answer the **Password Policy** question.

Password policy

Do you enforce a minimum password length of seven characters, containing both numeric and alphabetic characters, for user accounts on all POS devices, computers and systems in your business? ?

Yes No

Please note: After 31st March 2025, you will need to enforce a minimum password length of twelve characters (where twelve characters are supported, otherwise a minimum of eight characters is required). This also applies to passwords used by all non-customer users and administrators with access to e-commerce websites/webservers.

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

11. Fill out the summary information then click **Next**.

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..) ?

Fill out this section

21/4000

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

Fill out this section

21/4000

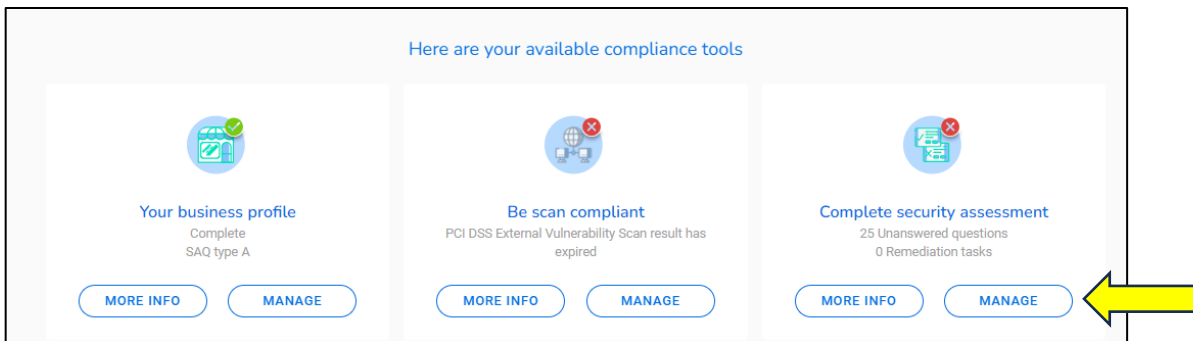
Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and webservers, include a description as to how they connect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

Fill out this section

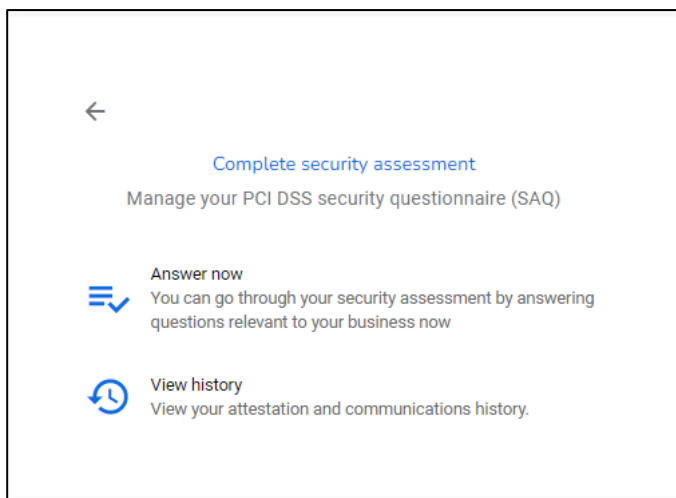
21/4000

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

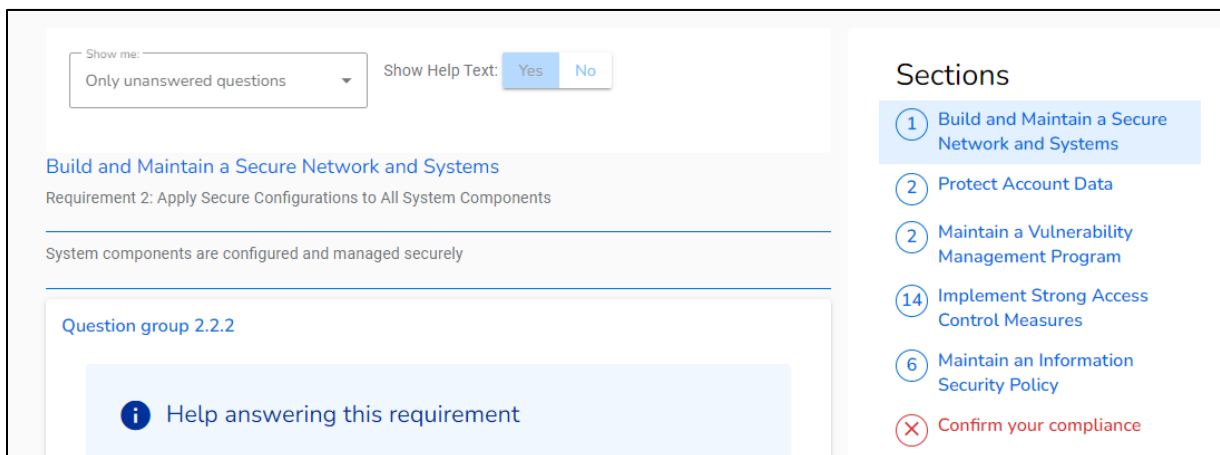
12. Click **Manage** in the **Complete Security Assessment** box.



13. Click **Answer Now**.



14. Answer all the unanswered questions (the number of questions may vary)



15. Click **Confirm Your Compliance** (if not already in that section).

Confirm your compliance

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

✓ Your organization information details

Company name Wind River Test - MX Team	Contact name** Test Account
Title	Telephone numbers 608.442.4223
Email address	Business address 65
Madison	Wisconsin

Sections

- ✓ Build and Maintain a Secure Network and Systems
- ✓ Protect Account Data
- ✓ Maintain a Vulnerability Management Program
- ✓ Implement Strong Access Control Measures
- ✓ Maintain an Information Security Policy
- ✗ **Confirm your compliance**

16. Click **Confirm Your Attestation**.

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ A

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✗ Attestation

✓ **Information for Submission.**

Based on the results noted in the SAQ A dated Mar 21, 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 21, 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.

CONFIRM YOUR ATTESTATION