Visa Asia Pacific AIS Service Tutorial

AIS Service Enrollment

1. Visit https://ap-ais.scanalert.com/

Click '**Asia-Pacific–AIS** or

'**Visa Asia Pacific AIS Validation Service**' links.

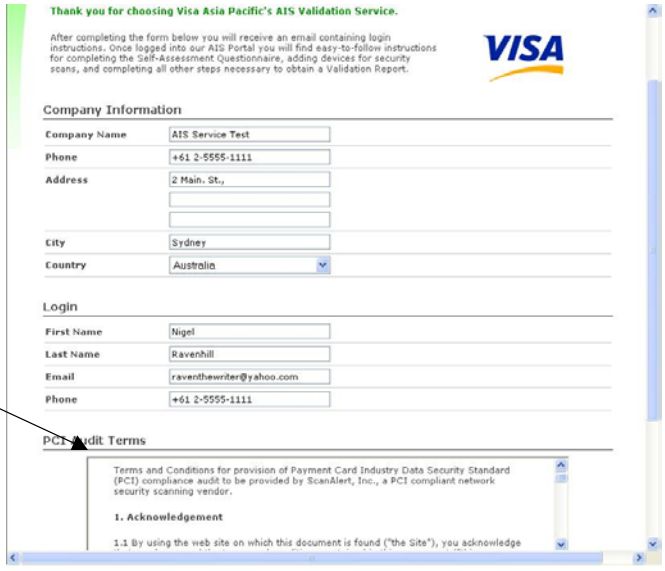
2. Page Title: "Welcome to the Visa Asia Pacific Account Information Security Portal"

Click '**Continue**'

3. Page Title: "Thank you for choosing Visa Asia Pacific's AIS Validation Service"

Enter the information for your organization.

Click '**Complete"** after completing the fields and agreeing to the PCI Audit Terms.

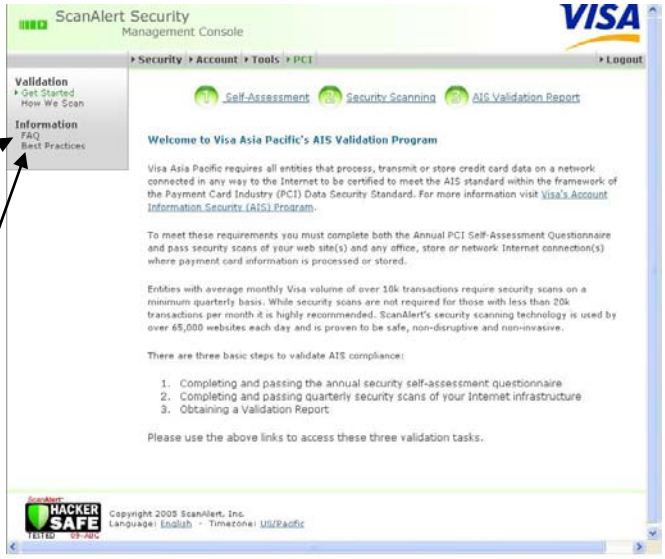


4. You will receive a welcome email.
Subject header is ScanAlert - FREE Asia Pacific AIS Validation.
Click on the link in the email and use the temporary password contained in the email to login to ScanAlert's AIS Portal.

5. You will have to change your password after logging in. You will then select and answer a security verification question for future identification. Once you have logged into your account please click the "PCI" menu tab for instructions on completing the steps necessary to meet the Visa AIS requirements using the internationally recognized Payment Card Industry (PCI) Data Security Standard.

6. Click '**FAQ**' for general information on the PCI standard

Click '**Best Practices**' for additional information on recommended IT security practices



Step 1: Self Assessment Questionnaire (SAQ)

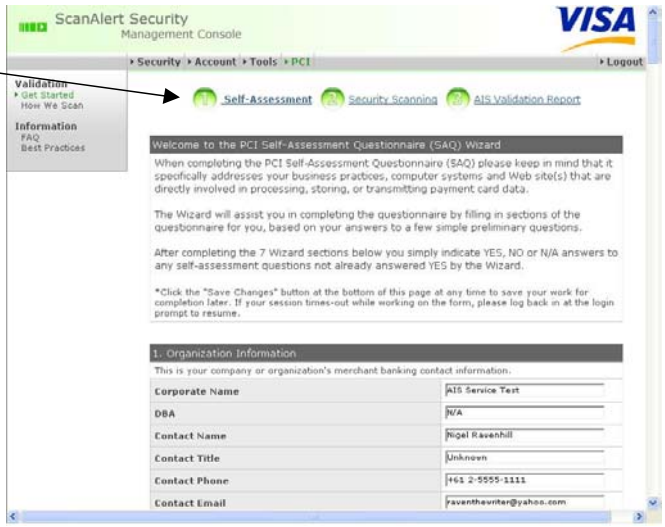
Click '**Self Assessment**'

The SAQ wizard will assist you in completing the SAQ by filling in sections of the questionnaire for you, based on your answers to a few simple preliminary questions.

The wizard will also help you download a PCI compliant privacy policy as well as designate a security officer for your organization.

The actual SAQ questions are 12 sections of the PCI Self-Assessment Questionnaire. Note: All questions must be answered either YES or N/A in order to receive an AIS Validation Report.

Some, or all, of the questions in each of the 12 sections may already be completed based on your answers to the Preliminary Questions above. These pre-completed sections have been "passed" with either YES or N/A answers based on your answers to those questions.



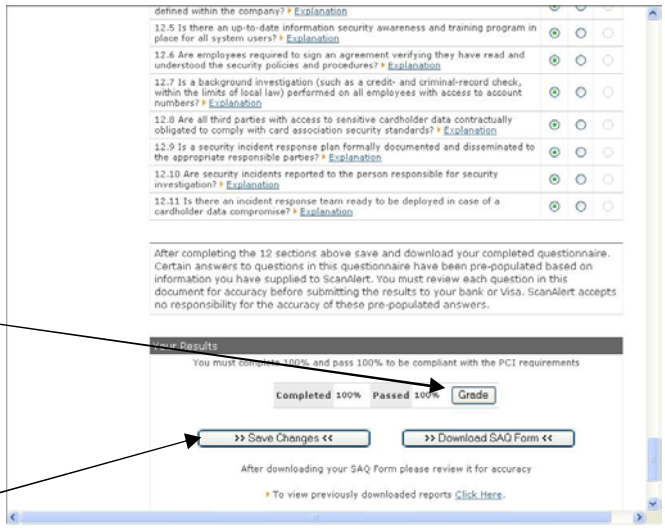
Click '**Save Changes**' at the bottom of this page at any time to save your work for completion later.

You can also view previously downloaded reports by clicking on the link at the bottom of the page.

Click 'Grade' at any time to see how close you are to finishing the SAQ.

You must complete 100% and pass 100% to be compliant with the PCI requirements.

Once you have completed all questions and received a 100% pass score, click '**Save Changes**' and download your SAQ for future reference.



Step 2: Security Scanning

Click '**Security Scanning**'

Security scanning is required for all Internet servers and network connection points involved in collecting, processing, transmitting or storing cardholder data. This includes office connections (dial-up modem, DSL, cable or wireless), store locations and Internet servers such as website(s), email, FTP, etc.

Click '**How We Scan**' if you have any questions regarding ScanAlert's scanning technology.

Click ''**Add Device'** to add a device to be scanned**.** Whenever you add a device, you must call a ScanAlert representative to "Activate" scanning.

Page Title: "Add Device"

Enter each domain or IP address that requires scanning. You must accept ScanAlert's Terms of Service. Click ''**Add Device'**

IMPORTANT:
To activate devices for scanning, merchants/IPSPs must contact ScanAlert.

Merchants/IPSPs in Taiwan or Hong Kong please call +886-2-2700-2207. You can also email aistaiwan@scanalert.com.

Merchants/IPSPs in Australia, New Zealand or other Asia Pacific countries please call +61-2-9922-6988 or +61-2-9929-0188. You can also email ais_au@scanalert.com.

Once your devices have been approved, they will be scanned within 24 hours, after which you can log into your account to view the scan results and patch or remediate any vulnerabilities that were found.

Step 3: Obtaining an AIS Validation Report

Note: To obtain an AIS Validation Report, you must meet the following requirements:

1. All SAQ questions must be answered either YES or N/A
2. All Internet servers and network connection points involved in collecting, processing, transmitting or storing cardholder data must pass a remote vulnerability scan with no vulnerabilities rated 3, 4 or 5.

You can choose either an English language HTML or PDF formatted report.

Click '**HTML**' or '**PDF**' to print a report.

Congratulations, you are now Validated to the PCI standard.