SECTIGO

Sectigo Hacker Guardian Migration Guide

SECTIGO

Table of Contents

Introduction..... 3
Portal Login..... 3
Adding IP Addresses..... 5
Deleting IP Addresses..... 6
Adding Domains..... 8
Starting Scans..... 9
Viewing Reports..... 11
Reporting False Positives..... 14
Generate Attestation of Scan Compliance, Detailed report and Executive Summary..... 14
Create a Scan Schedule..... 19
Update Account Details..... 22
Contact Support..... 24
License Purchase and Renewal..... 24

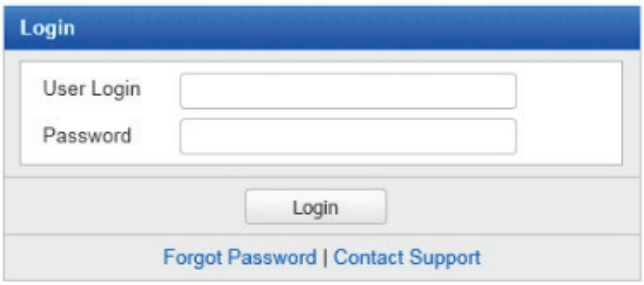
Introduction

This document is intended to guide existing HackerGuardian customers through changes to the HackerGuardian Portal and how to use the new portal.

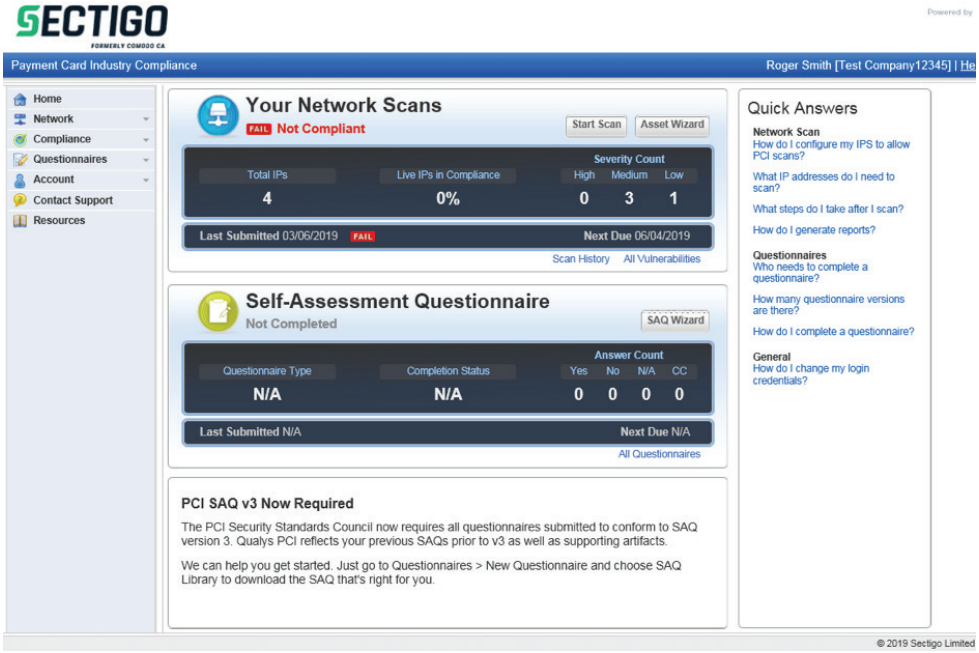
Portal Login

The old login was https://www.hackerguardian.com/sas/login.jsp.

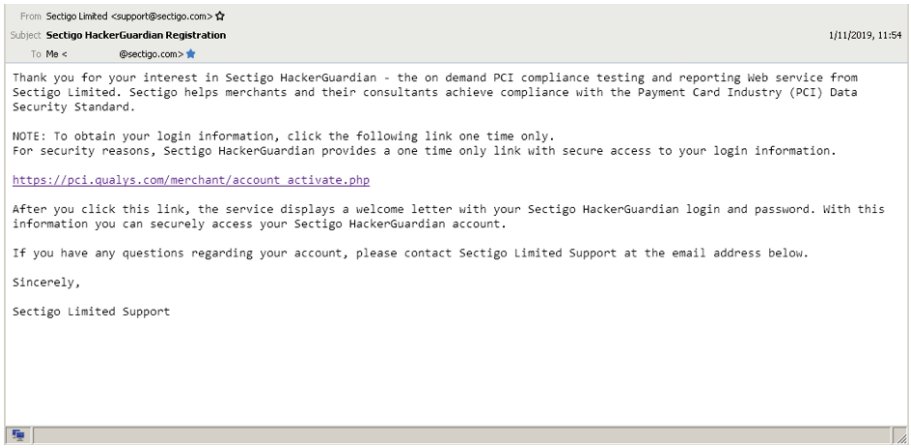
Please bookmark https://pci.qualys.com/merchant/, which is the login for the new portal.



Once logged in you will see the new portal with an overview of your status.



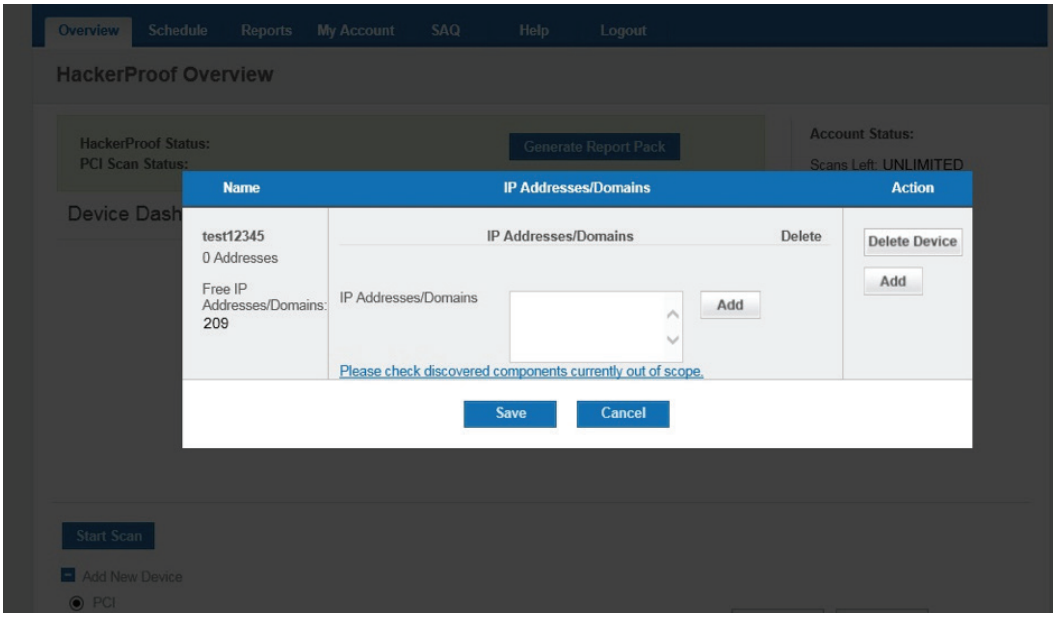
As we migrate existing customers over to the new portal you will be sent an account activation email. Clicking the activation link will provide you with a new username and password which can be used for the new portal.



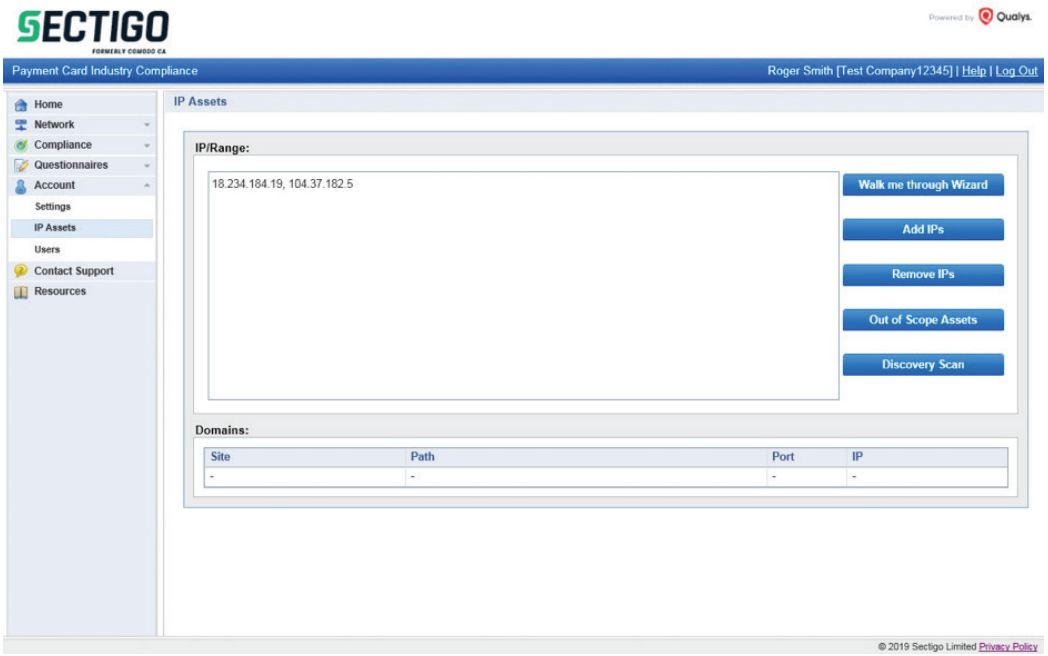
Previously Sectigo OMS username and password were the same as the HackerGuardian username and password. Now you will have a separate username and password for the new HackerGuardian portal. You should still use your Sectigo OMS username and password for purchasing new licenses and logging into OMS. HackerProof licenses will remain unchanged on the old portal with this release.

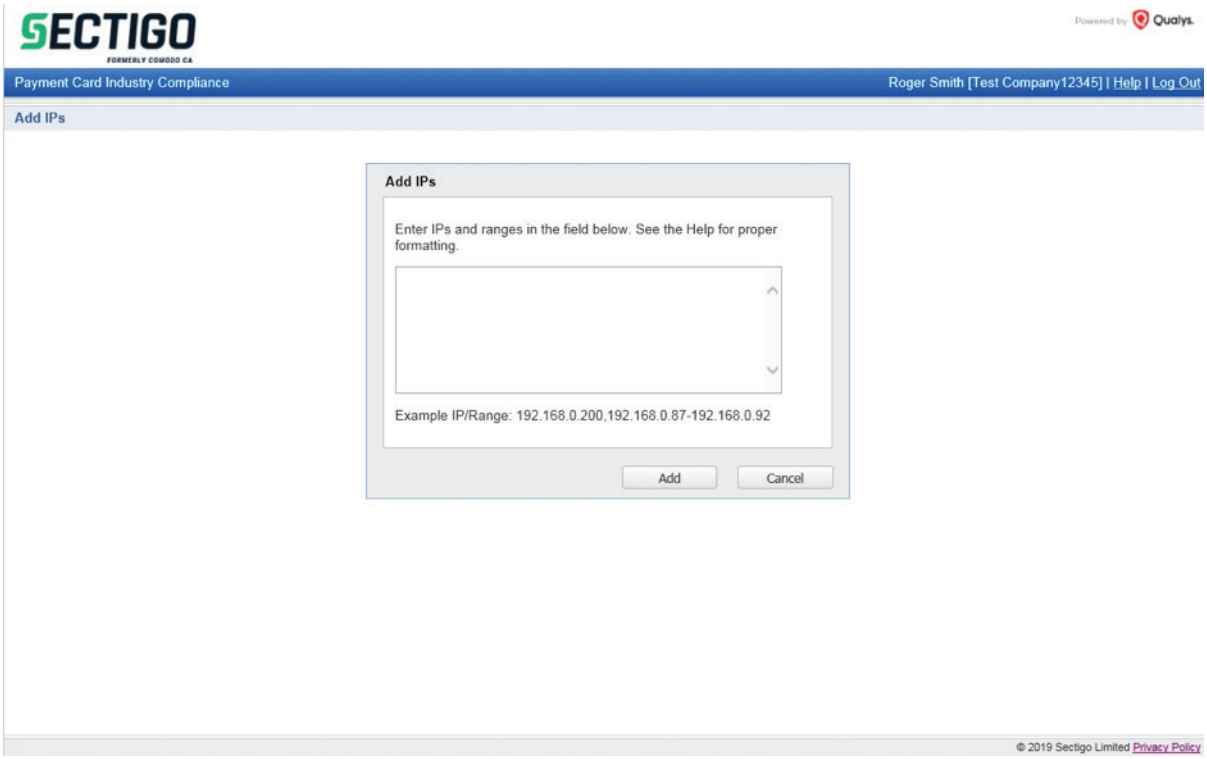
Adding IP Addresses

Previously you would navigate to the overview page and click Add New Device, set the device name and click continue. You could then add a single or multiple IP addresses, an IP Address range or a domain.



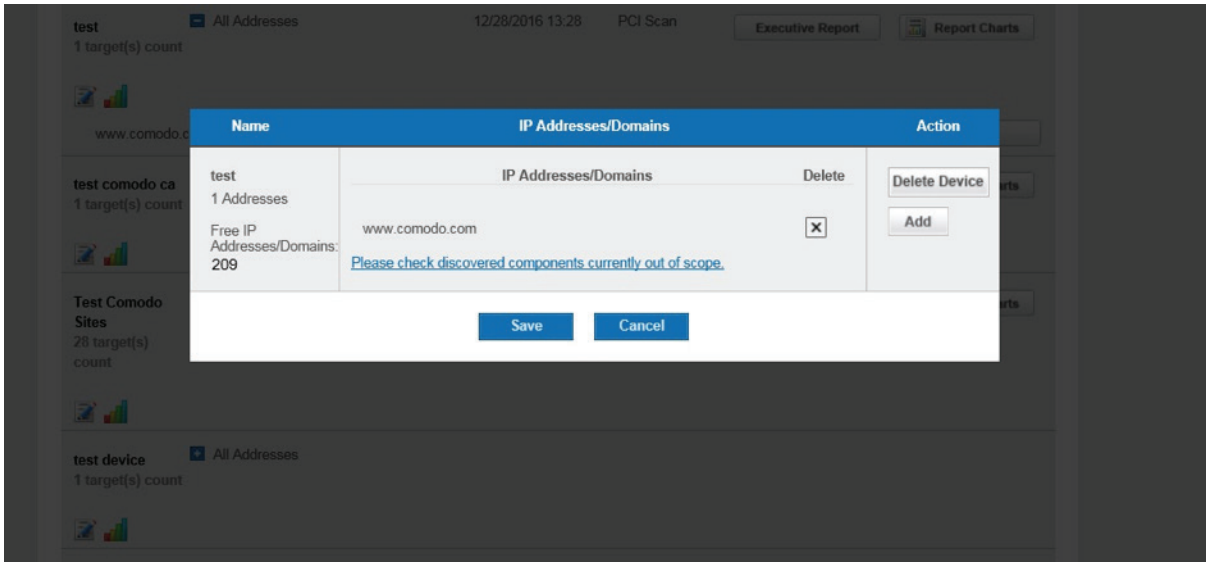
In the new portal click “Account” then “IP Assets”. Click “Add IPs” to add IP Addresses or IP Address ranges. IP Address can also be added automatically when running a new scan.



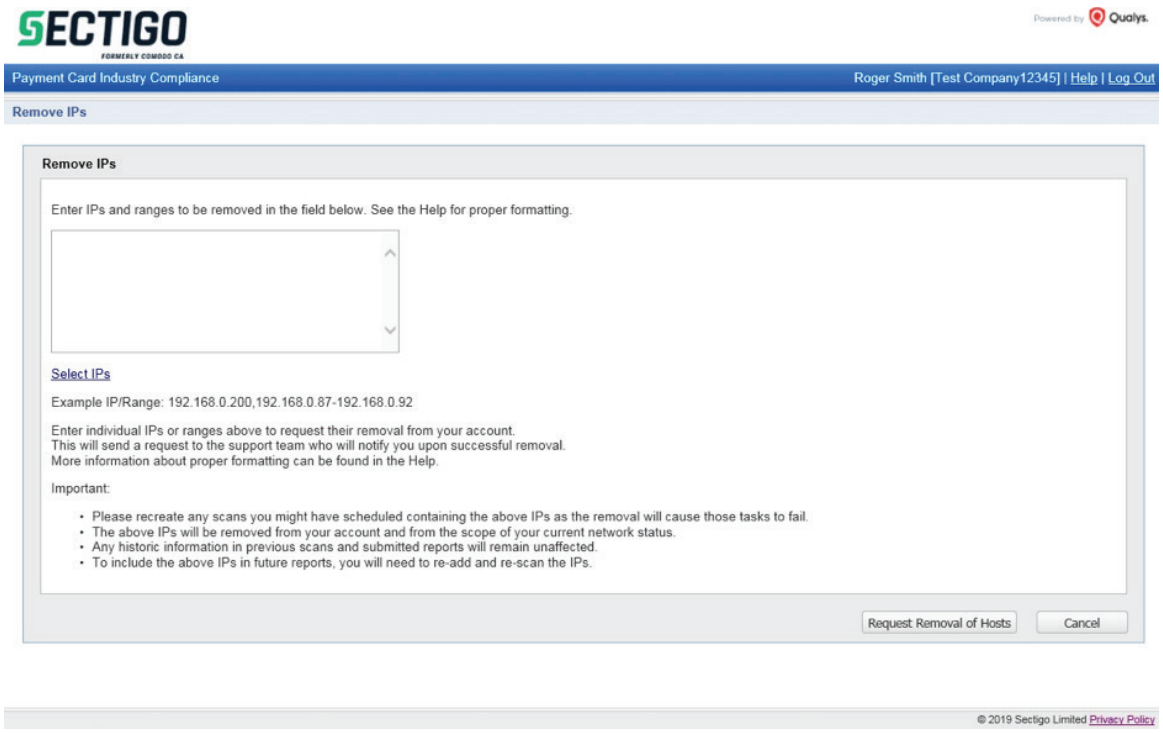


Deleting IP Addresses

In the old portal you clicked the edit device icon then remove IP Addresses/Domains by clicking the “X” button . Within minutes of the customer submitting the order form.

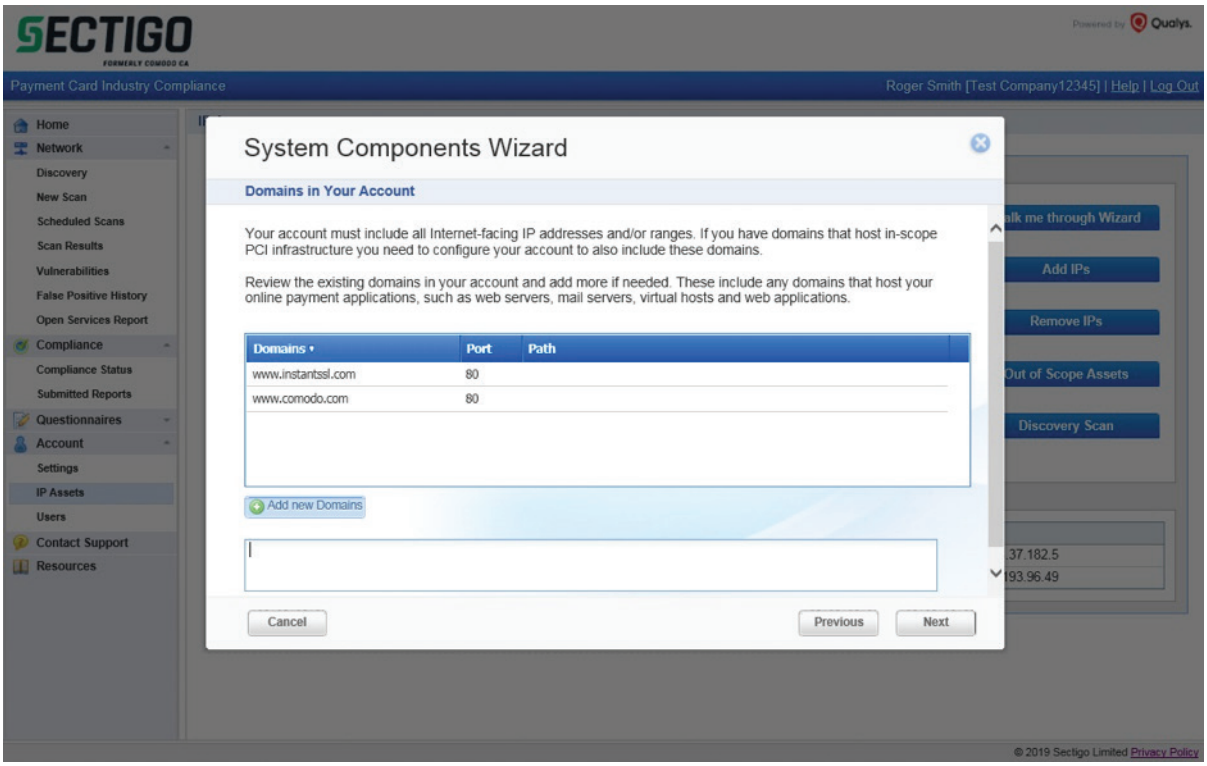


In the new portal click “Account” then “IP Assets”. Click “Remove IPs” and then enter the IP Addresses you wish to remove. The IP Addresses will be checked and removed by a Sectigo administrator. Domains are still listed but the IP Address associated with a domain may be removed and it will no longer be scanned.



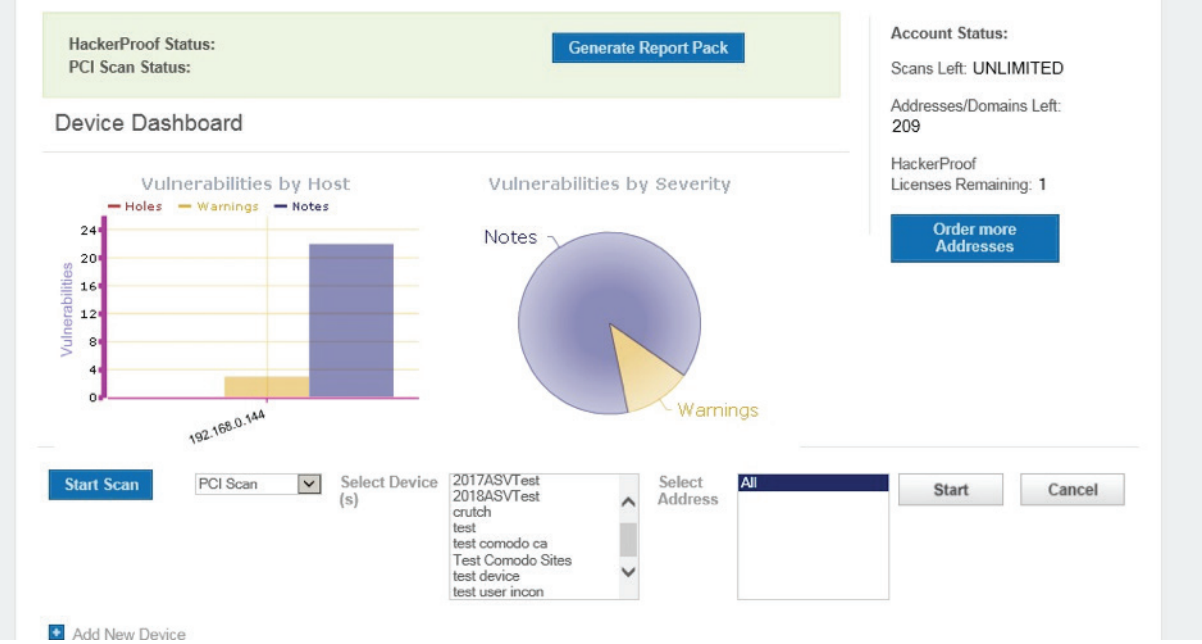
Adding Domains

To add domains click “Walk me through the Wizard” click “next” then “next” again. Then click “Add new domains” and set the domains you own. The IP Addresses of these domains are resolved and will be listed in the IP Address list. When starting a new scan the resolved IP Address is listed and not the domain as with the old portal. The path to a particular location which requires scanning can also be added such as www.example.com/index.html.



Starting Scans

Previously you would navigate to the overview page and click “Start Scan” then select the IP Addresses or domains to be scanned and click “Start”.

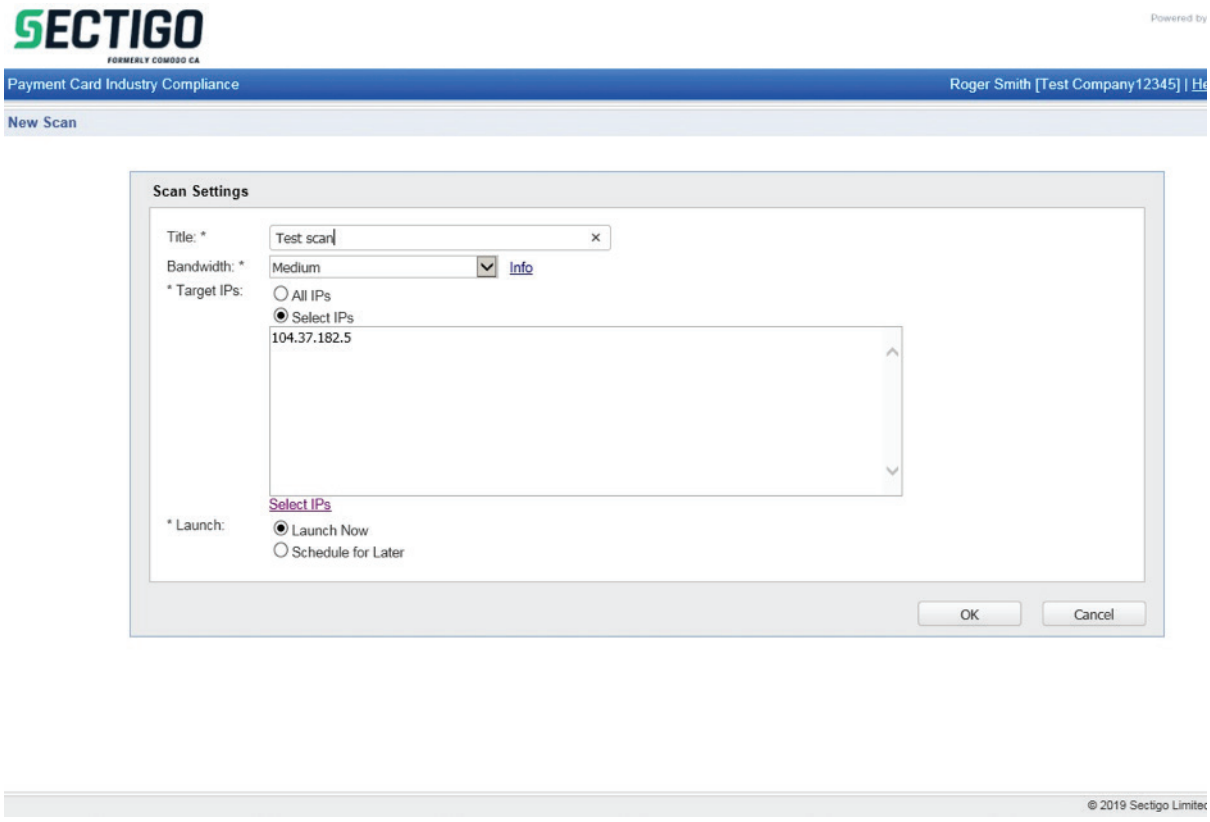


In the new portal click “Network” then “New Scan” to add new IP Addresses, select existing IP Addresses to scan or scan all IP Addresses. A title to identify the scan must be supplied. The bandwidth of the scan may be selected which can be used to increase the scan speed or reduce the load the scan generates on the server being scanned. You may also start the scan straight away (Launch Now) or schedule the scan for a later date (Schedule for Later). If you select “Launch Now” you will be redirected to the page displaying the scan progress.

The old scanner IP Address range was: 178.255.82.64/27 (178.255.82.64-178.255.82.95)

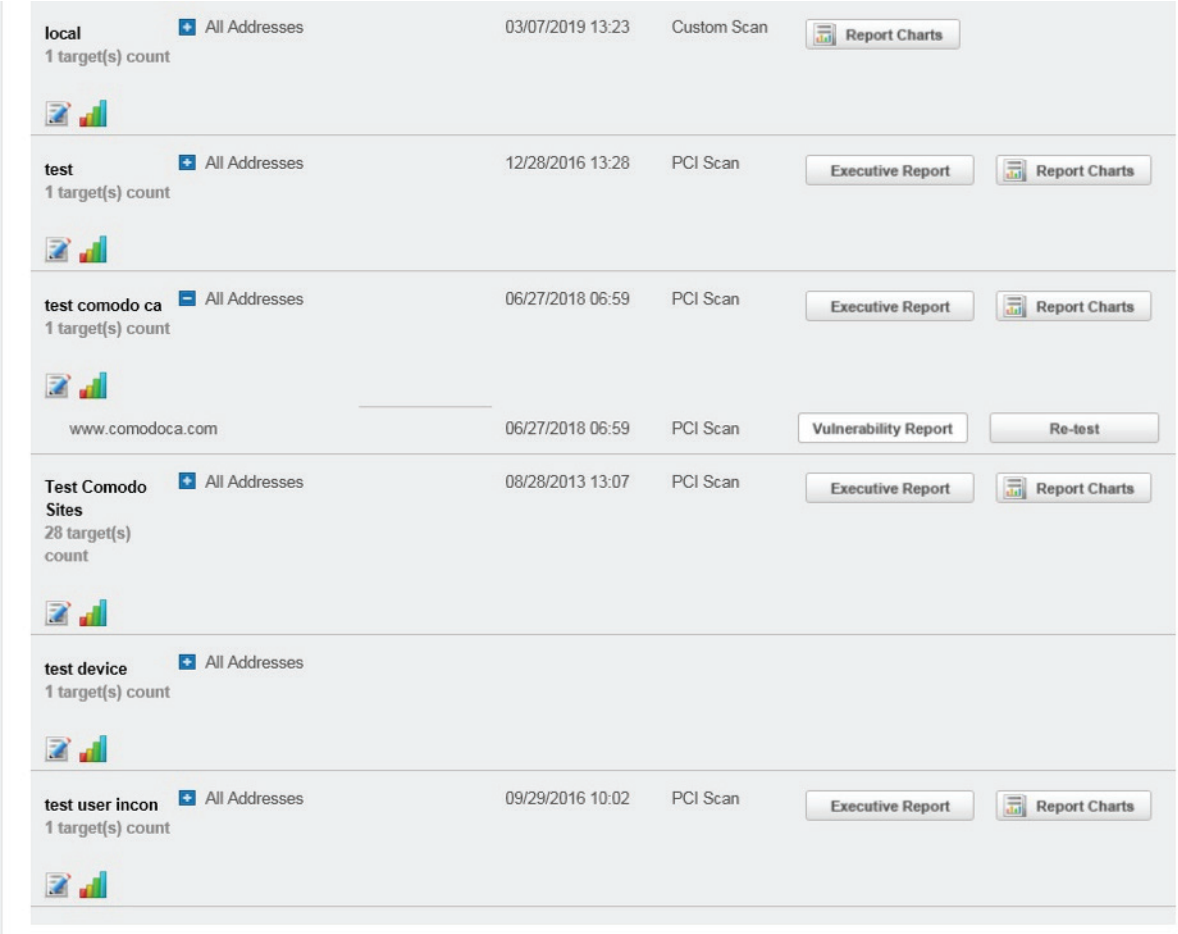
New scanner IP Address range: 64.39.96.0/20 (64.39.96.1-64.39.111.254)

The new scanner address range should be whitelisted when scanning through the new portal.

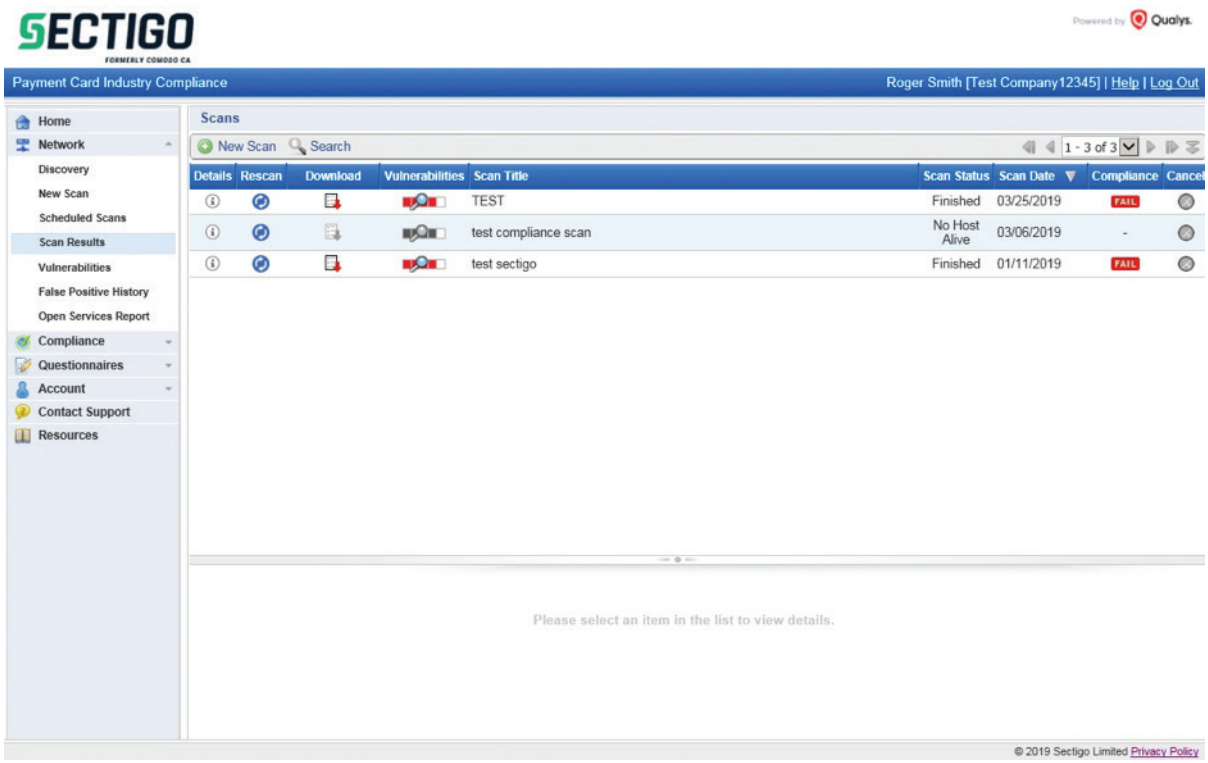


Viewing Reports

Previously you would navigate to the overview page or reports page then click the device you wanted to view the report for and click the “Executive Report” or “Vulnerability Report” button depending on which report you wanted to view.

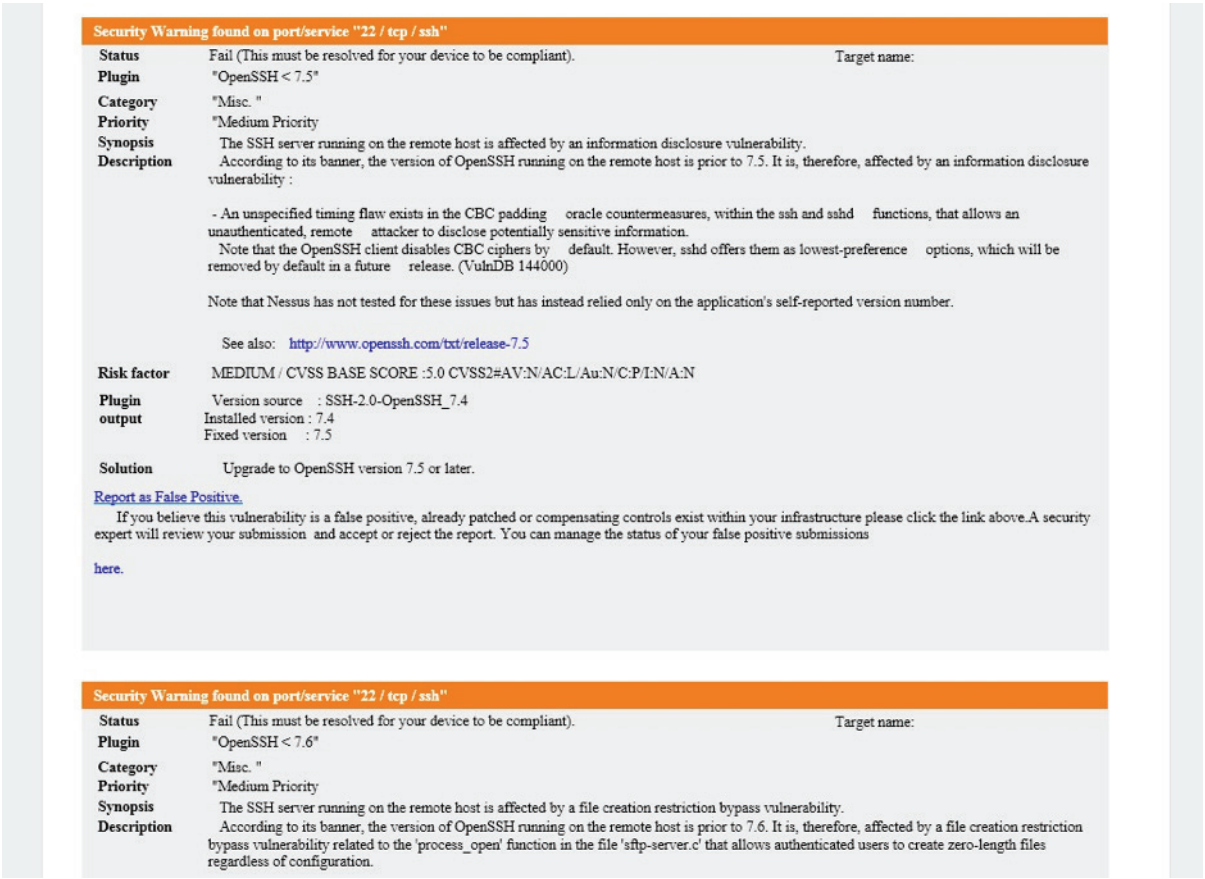


In the new portal click “Network” then “Scan Results”. The full report can be viewed as a PDF by clicking the download icon in the “Download” column of the table. To view a list of the vulnerabilities that require action click the icon in the “Vulnerabilities” column. The executive summary report is only available after submitting your attestation of scan compliance. Please see the “Generate Attestation of Scan Compliance, Detailed report and Executive Summary” section for details on how to do this.



Reporting False Positives

Previously false positives could be reported from within the detailed report view. After selecting a report to view each failing item shows a link which can be clicked to bring up the false positive submission form. The submitted information is reviewed by an ASV Qualified Employee before being accepted or rejected. If accepted the vulnerability no longer affects the report status. The false positive status and history could be viewed under “Reports” then “False Positive Tracker”.



Security Warning found on port/service "22 / tcp / ssh"

Status	Fail (This must be resolved for your device to be compliant).	Target name:
Plugin	"OpenSSH < 7.5"	
Category	"Misc. "	
Priority	"Medium Priority	
Synopsis	The SSH server running on the remote host is affected by an information disclosure vulnerability.	
Description	According to its banner, the version of OpenSSH running on the remote host is prior to 7.5. It is, therefore, affected by an information disclosure vulnerability : - An unspecified timing flaw exists in the CBC padding oracle countermeasures, within the ssh and sshd functions, that allows an unauthenticated, remote attacker to disclose potentially sensitive information. Note that the OpenSSH client disables CBC ciphers by default. However, sshd offers them as lowest-preference options, which will be removed by default in a future release. (VulnDB 144000) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. See also: http://www.openssh.com/txt/release-7.5	
Risk factor	MEDIUM / CVSS BASE SCORE :5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	
Plugin output	Version source : SSH-2.0-OpenSSH_7.4 Installed version : 7.4 Fixed version : 7.5	
Solution	Upgrade to OpenSSH version 7.5 or later.	

Report as False Positive.

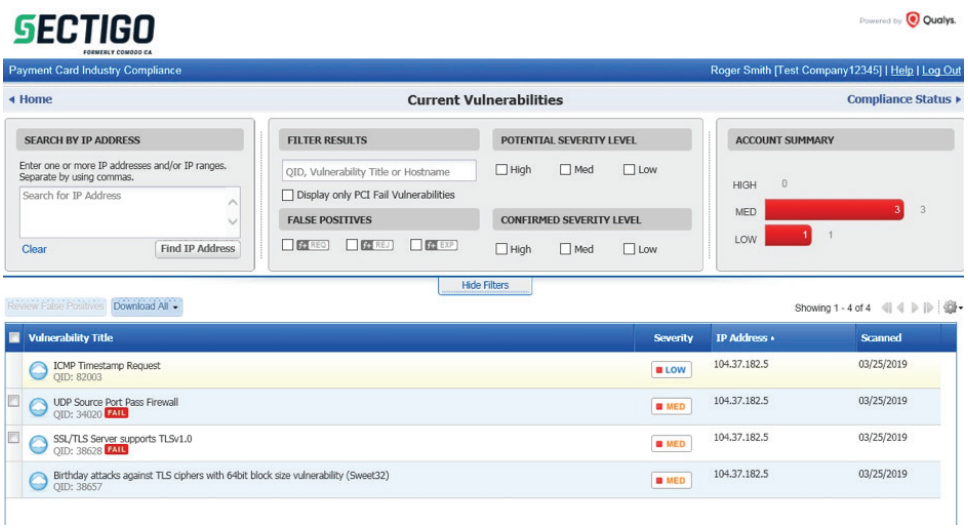
If you believe this vulnerability is a false positive, already patched or compensating controls exist within your infrastructure please click the link above.A security expert will review your submission and accept or reject the report. You can manage the status of your false positive submissions

here.

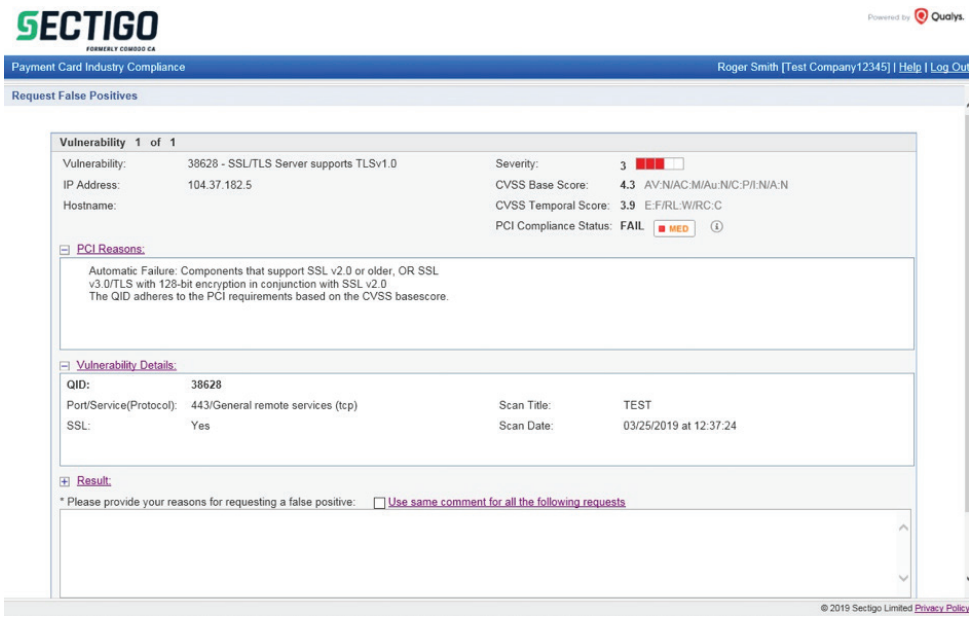
Security Warning found on port/service "22 / tcp / ssh"

Status	Fail (This must be resolved for your device to be compliant).	Target name:
Plugin	"OpenSSH < 7.6"	
Category	"Misc. "	
Priority	"Medium Priority	
Synopsis	The SSH server running on the remote host is affected by a file creation restriction bypass vulnerability.	
Description	According to its banner, the version of OpenSSH running on the remote host is prior to 7.6. It is, therefore, affected by a file creation restriction bypass vulnerability related to the 'process_open' function in the file 'sftp-server.c' that allows authenticated users to create zero-length files regardless of configuration.	

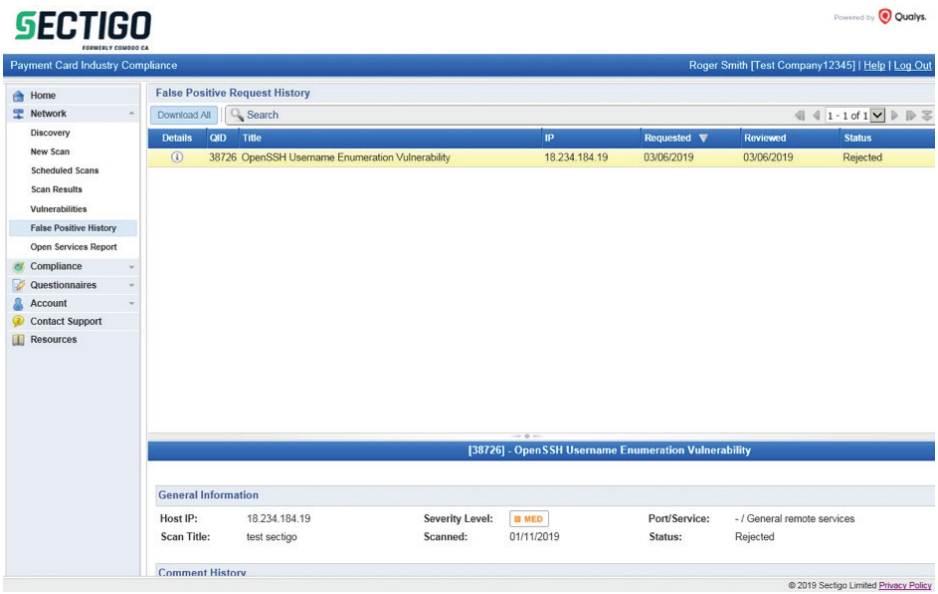
In the new portal either click “Network” then “Scan Results” then the vulnerabilities icon in the “Vulnerability” column of table to select an IP Address or click “Network” then “Vulnerabilities” for a full list. Use the far left checkbox to select the false positives you want to report and then click “Review False Positives”.



A detailed explanation as to why this is a false positive or description of the compensating controls implemented must be provided. The submitted information is reviewed by an ASV Qualified Employee before being accepted or rejected. If accepted the vulnerability no longer affects the report status.

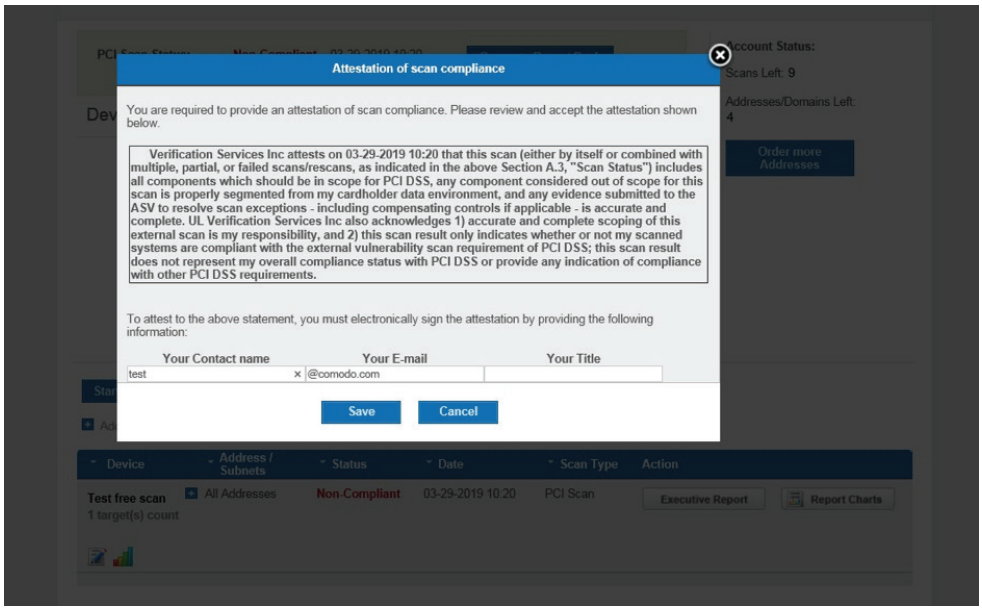


The false positive status and history could be viewed under “Network” then “False Positive History”.

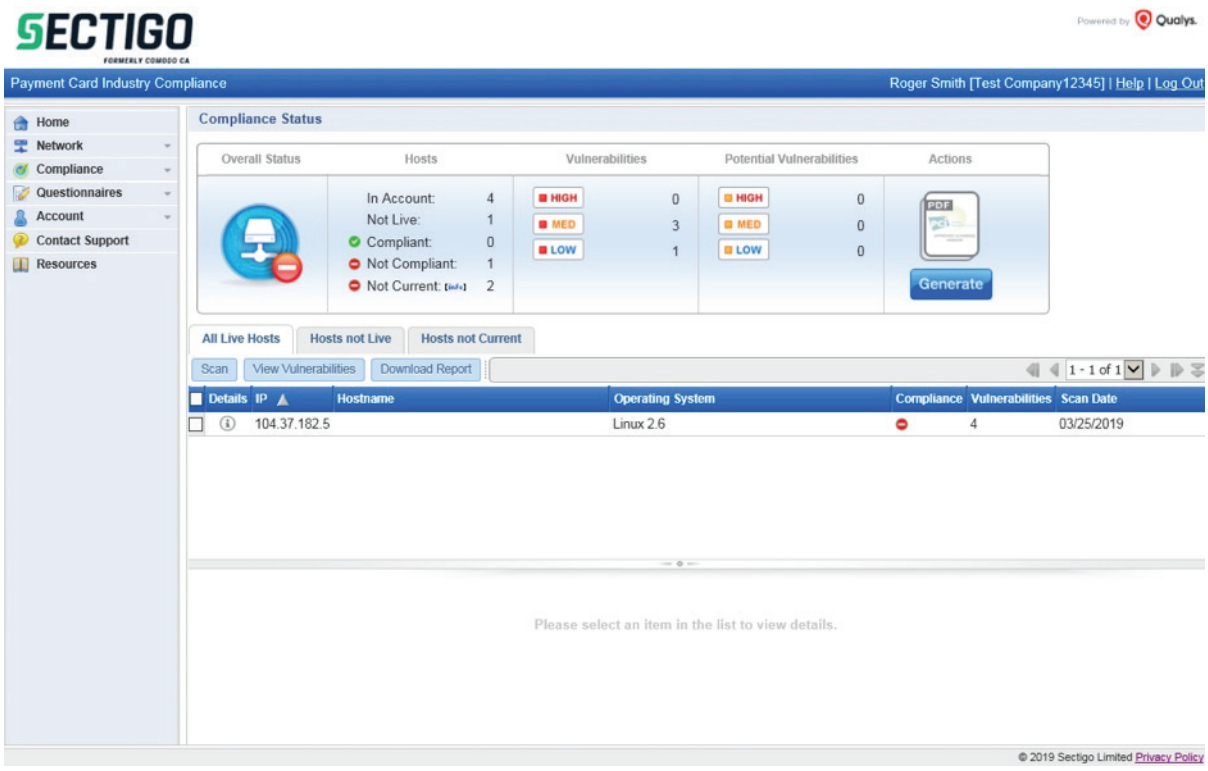


Generate Attestation of Scan Compliance, Detailed report and Executive Summary

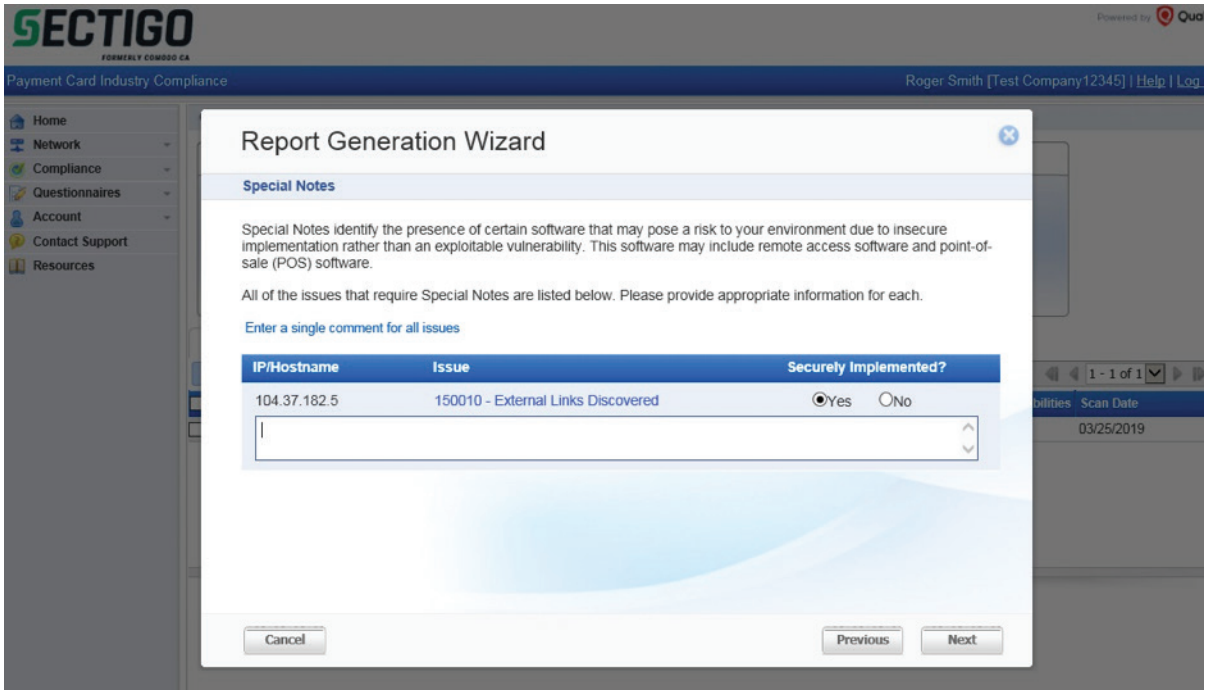
Previously the report pack which contained the compliance reports could be requested by clicking the “Generate Report Pack” button on the overview page. All IP Addresses were included in the generated report pack.



In the new portal click on “Compliance” and then “Compliance Status” then click the “Generate” button under “Actions”. The IP Addresses included in the report are listed in the table on this page. Previously a report could not be generated if all the IP Addresses were not scanned in the last 90 days. Now an IP Address will not gain a compliant status if it has not been scanned in the last 30 days. This is not a change in the compliance process but intended to follow PCI best practice.



The attestation process is similar to before, for each special note found a submission must be made to ensure the service is securely implemented. Optionally additional comments may be added for non-compliant IP Addresses. Out of scope IP Addresses may be confirmed on the final popup of the attestation. As previously the name and title to appear on the Attestation of Scan Compliance must be provided. Previously reports were automatically submitted for review, now you may decide to submit the report now or save it for later. Reports saved for later may be submitted by clicking “Compliance” then “Submitted Reports” and under “Next Action” click the “Request Review” link.



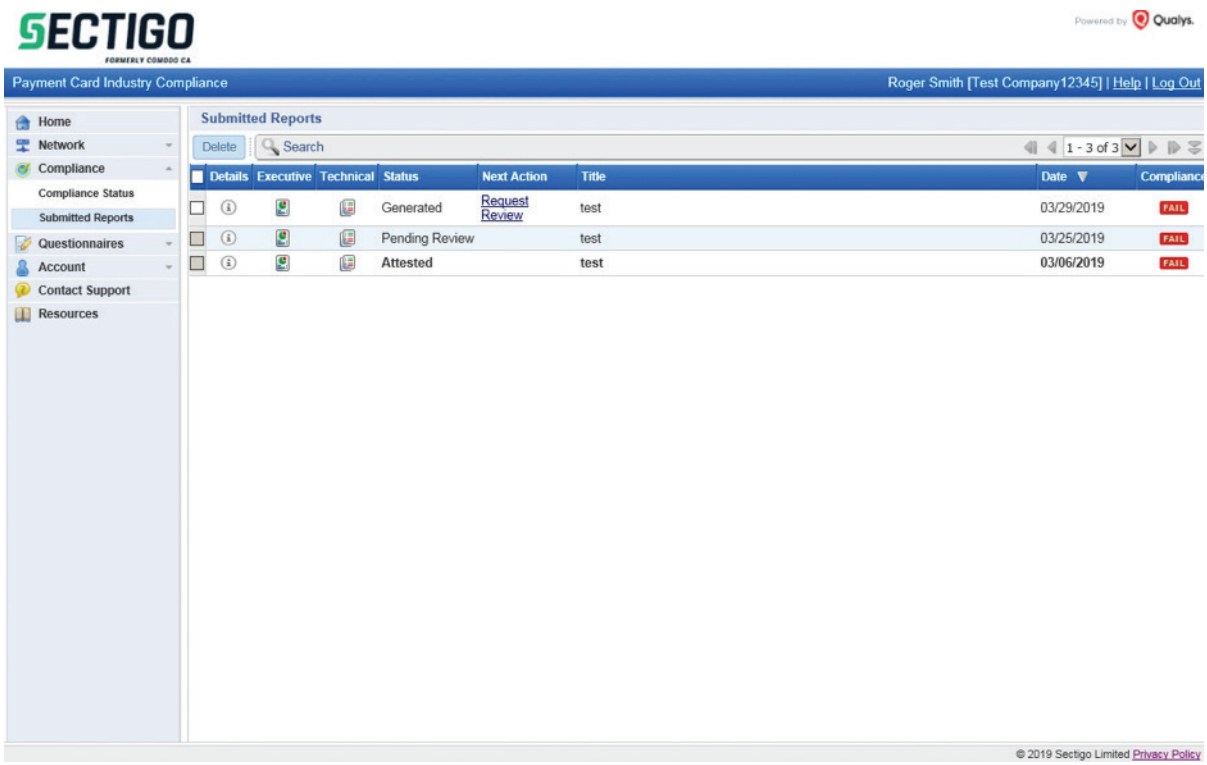
Once a report has been requested the status can be reviewed by clicking on “Compliance” then “Submitted Reports”. The status may be:

• Attested
The report has been reviewed and issued. The report may then be provided to your Acquirer to prove compliance with the PCI DSS ASV scan requirement.

• Pending Review
The report has not yet been reviewed by a Sectigo ASV qualified employee.

• Generated
The report has not yet been submitted for review.

• Rejected
An issue has been detected with the reports or information submitted during the attestation. The feedback on the rejection will be provided via email to account contact.



Previously the report pack contained three separate documents, the executive summary, detailed report and attestation of scan compliance. All three documents are now contained in a single PDF called the Technical report. A separate executive summary report is also available to download. The Technical report is broken down into the matching sections that were provided previously as separate documents. This document should be provided to your acquirer after approval. Most sections of the report match the formatting of the old reports. There is some small changes to the detailed report formatting but the same information is provided as previously.

SECTIGO

Powered by Qualys.

Payment Card Industry (PCI) Technical Report

03/06/2019

ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				A2. Approved Scanning Vendor Information			
Company:	Test Company12345			Company:	Sectigo Limited		
Contact Name:	Roger Smith	Job Title:	CFO	Contact Name:		Job Title:	
Telephone:	123455667	Email:		Telephone:	12345	Email:	
Business Address:				Business Address:	3rd Floor Building 26, Office Village Exchange Quay, Trafford Road		
City:		State/Province:	None	City:	Salford	State/Province:	None
ZIP/postal code:		Country:	United Kingdom	ZIP/postal code:	M5 3EQ	Country:	United Kingdom
URL:				URL:	https://sectigo.com/		

A3. Scan Status			
Date scan completed	N/A	Scan expiration date (90 days from date scan completed)	N/A
Compliance Status	FAIL	Scan report type	Full scan
Number of unique in-scope components scanned			0
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

Evaluation

A.4 Scan Customer Attestation

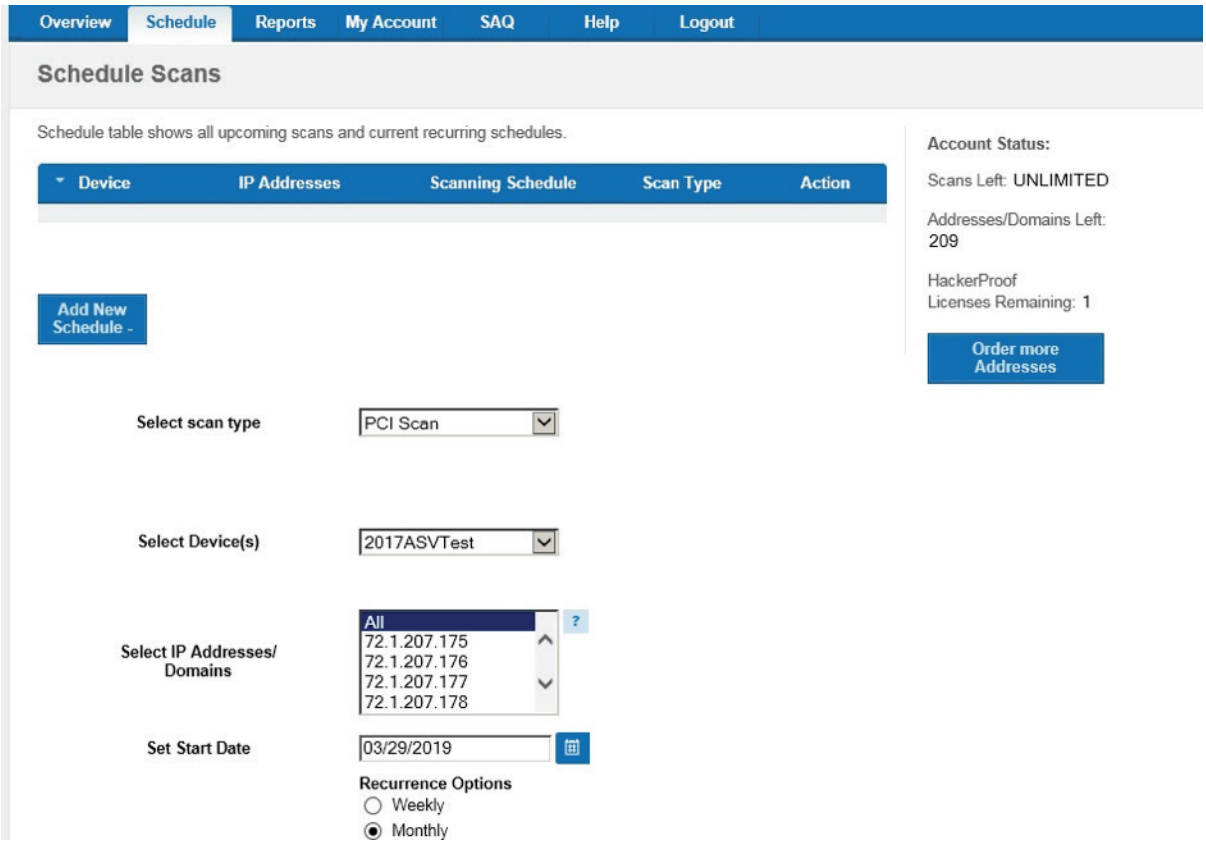
Test Company12345 attests on 03/06/2019 at 11:59:43 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions -including compensating controls if applicable- is accurate and complete.
Test Company12345 also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

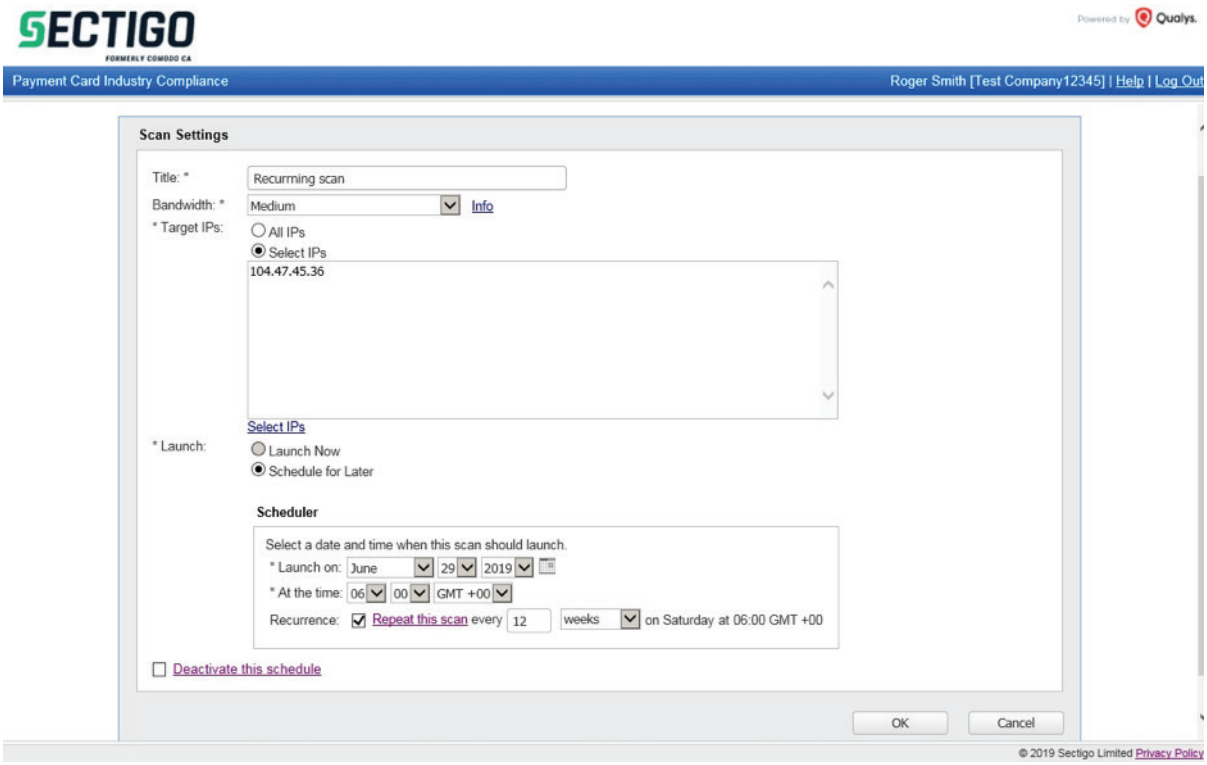
This scan and report was prepared and conducted by Sectigo Limited under certificate number 4172-01-12, according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.
Sectigo Limited attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by

Create a Scan Schedule

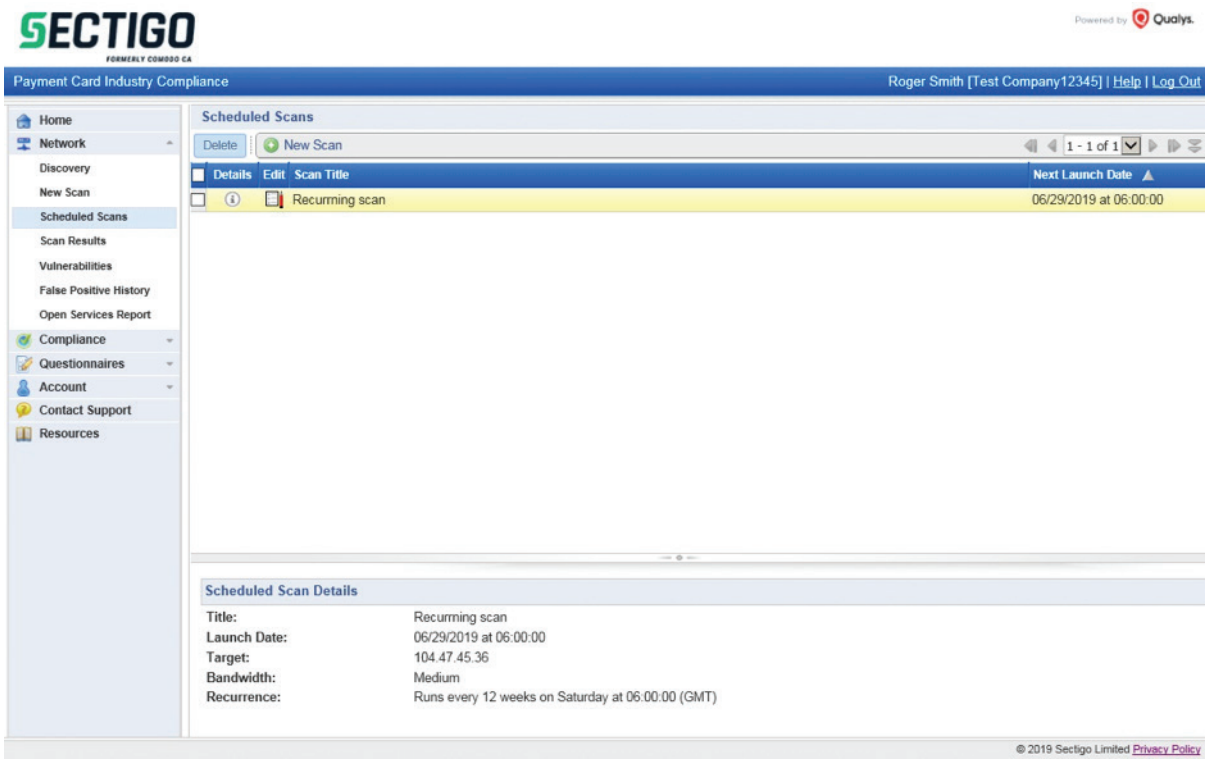
Previously scans could be scheduled via the “Schedule” tab at the top of the page. Clicking the “Add New Schedule” button allowed a recurring or one off scan to be scheduled on a weekly, monthly, quarterly or set number of days basis.



In the new portal a scan schedule can be created by either clicking on “Network” then “Scheduled Scans” then “New Scan” or by clicking on “Network” then “New Scan”. On the “New Scan” page the “Schedule for Later” must be selected to schedule the scan. The launch date and time must be specified and the scan can either be a single occurrence or scheduled to run over a recurring period. Previously individual schedules were required for each device now all IP Addresses can be run under a single schedule. A minimum recurring schedule is a daily scan and maximum is a scan every 13 weeks.

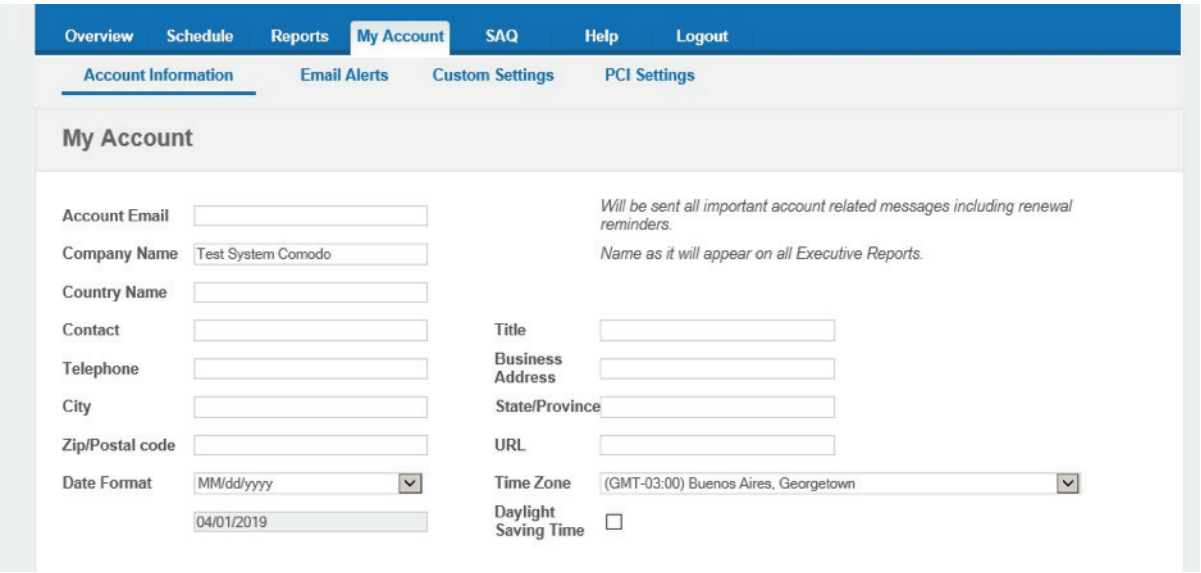


Existing scan schedules can be viewed, edited and deleted on the “Network”, “Scheduled Scans” page.

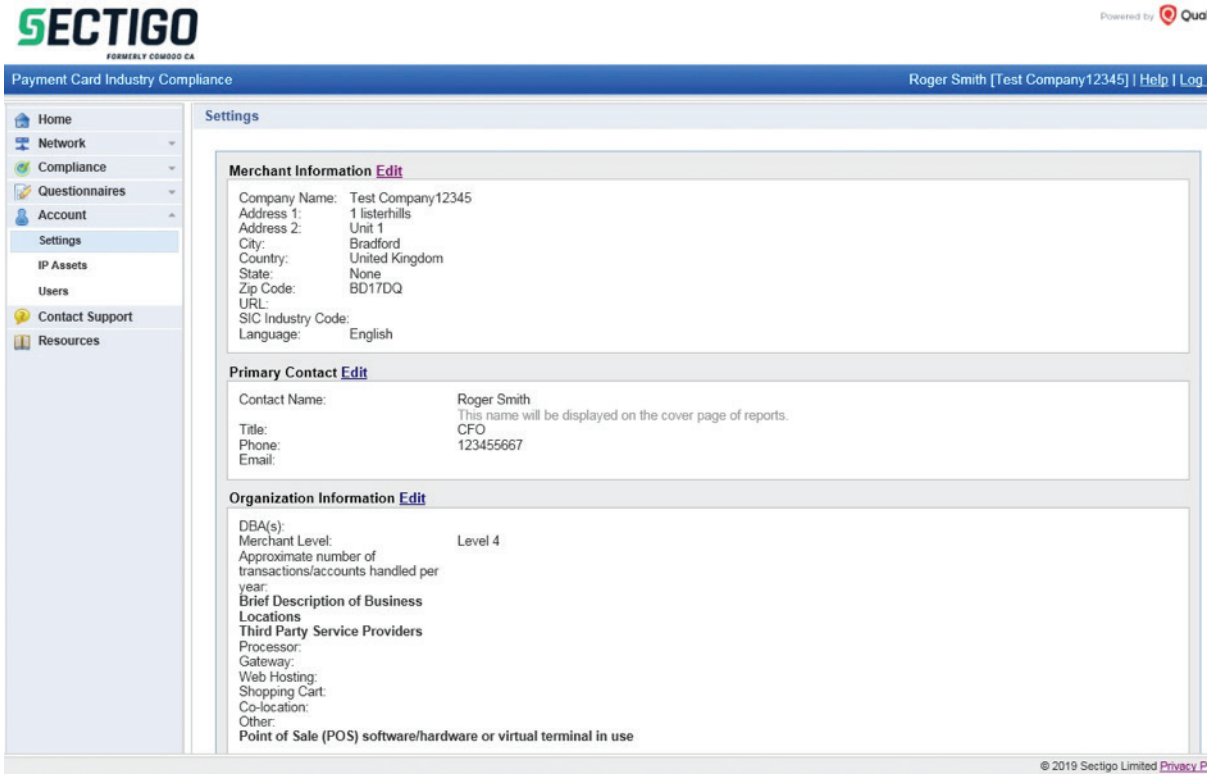


Update Account Details

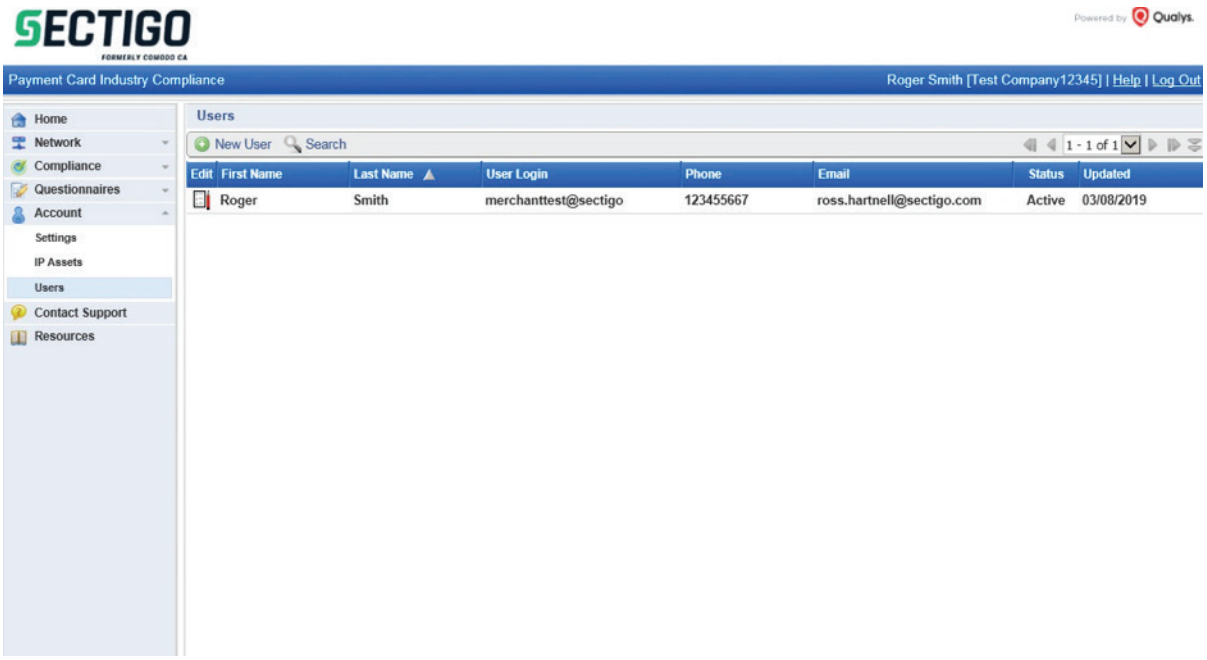
Previously account setting could be modified by clicking on “My Account” and “Account Information”.



In the new portal account settings can be altered by clicking on “Account”, “Settings” then the “Edit” link for the appropriate section. To alter the company name please contact support.



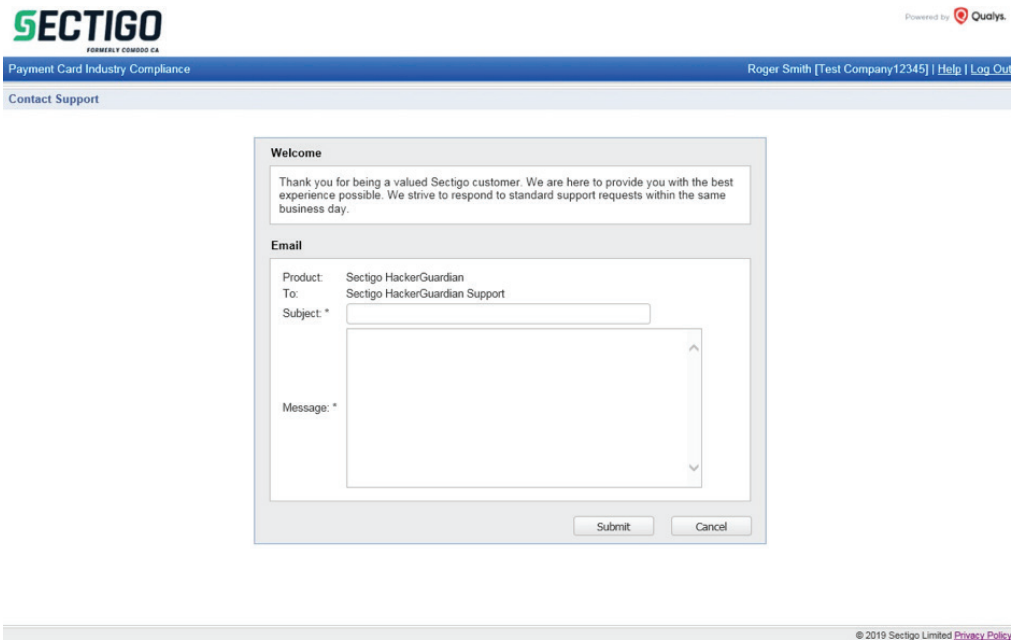
Previously only a single user could access an account, now you may create additional user logins for employees in your organization so they may also run scans and view the reports. An additional user may be added by clicking on “Account” and “User” then “New User”. After adding a new user an activation email will be sent to their email address. After activation the new user may access the portal using their credentials.



Contact Support

A support email can be sent to Sectigo support by clicking on “Contact Support”.
A support ticket can also be directly created here: https://sectigo.com/support-ticket.
Phone support can be reached at:

+1 (888) 266-6361 (US) +1 (703) 581-6361 (International)



License Purchase and Renewal

HackerGuardian can continue to be purchased through www.hackerguardian.com and the licenses and pricing are unchanged. The standard license will now allow an unlimited about of scans rather than the 10 per quarter as previously.

Licenses can only be renewed 30 days prior to the expiration of the existing license.

When renewing a license the number of IP Addresses on the account cannot be downgraded. Please contact support if you want to reduce the number of IP Addresses on your account when renewing.

The free trial license does not put limitations on the portal functionality. The same functionality is available on an account the with the trial license as with a full license. However the reports generated with the trial license contain an evaluation watermark and cannot be used to gain compliance with the PCI DSS ASV scan requirement.