



Sectigo HackerGuardian Version 2.0 User Guide

Table of Contents

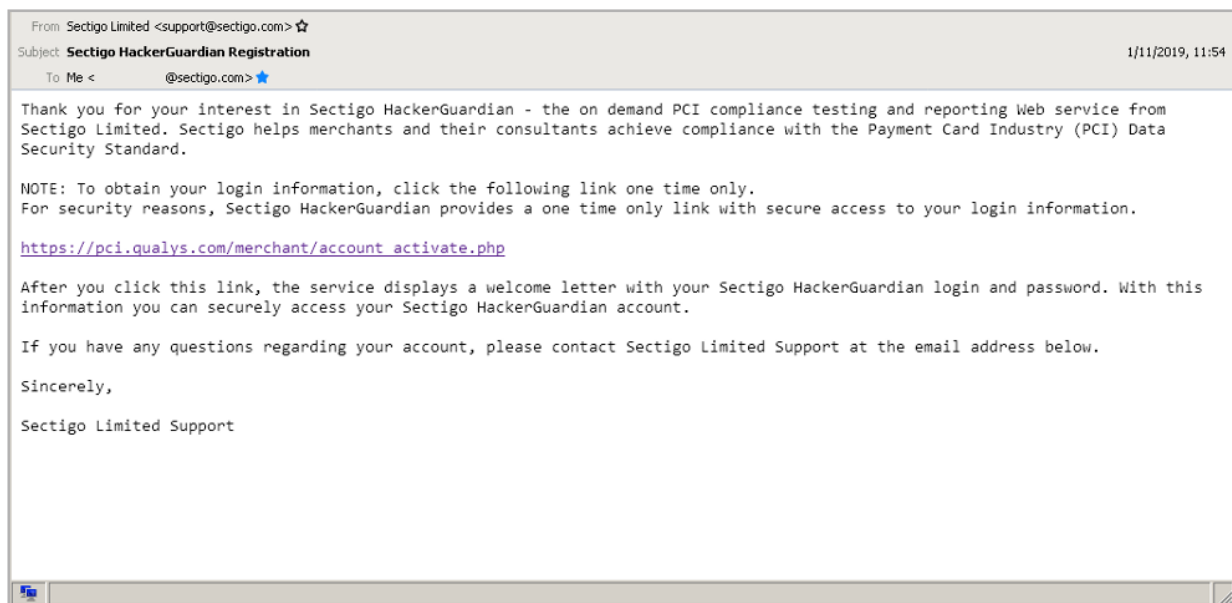
Introduction.....	03
Purchase and Account Activation.....	03
Portal Login.....	04
Adding IP Addresses.....	05
Deleting IP Addresses.....	06
Adding Domains.....	07
Deleting Domains.....	08
Starting Scans.....	09
Viewing Reports.....	10
Reporting False Positives.....	11
Generate Attestation of Scan Compliance, Detailed report and Executive Summary.....	12
Create a Scan Schedule.....	16
Update Account Details.....	17
Contact Support.....	18
License Purchase and Renewal.....	18

Introduction

This document is a guide for the new HackerGuardian version 2.0 portal.

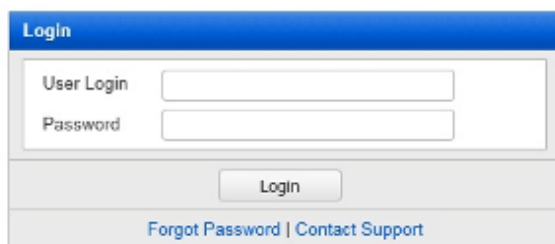
Purchase and Account Activation

After purchasing a new license at <http://store.hackerguardian.com> you will receive an account activation email like the one below. If you do not receive this email please check your spam folder before contacting support. Clicking on the link will activate your account and provide you with the credentials for the portal. Note that the credentials for store.hackerguardian.com and the HackerGuardian portal are different and the store credentials should be used when logging into <http://store.hackerguardian.com> for renewals and upgrades.



Portal Login

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



Login

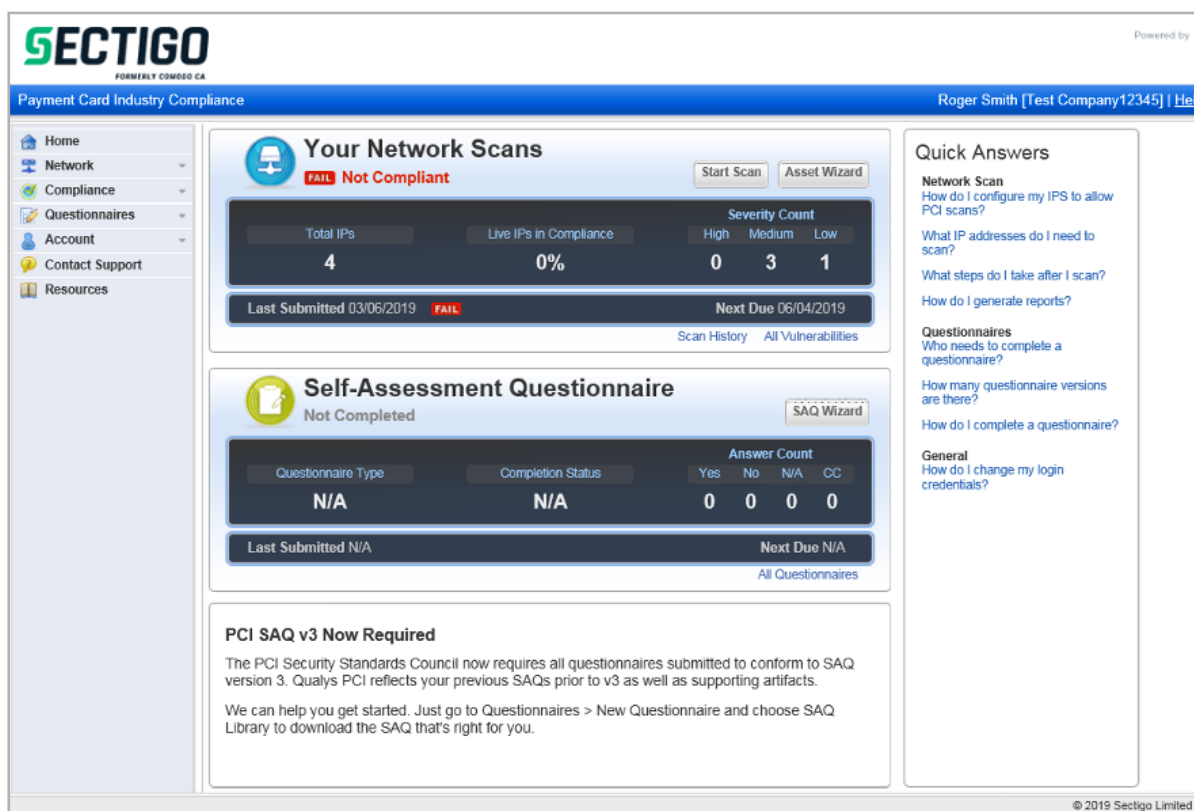
User Login

Password

Login

[Forgot Password](#) | [Contact Support](#)

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



SECTIGO
FORMERLY COMODO CA

Payment Card Industry Compliance

Roger Smith [Test Company12345] | Help

Home
Network
Compliance
Questionnaires
Account
Contact Support
Resources

Your Network Scans

FAIL Not Compliant Start Scan Asset Wizard

Total IPs	Live IPs in Compliance	Severity Count		
		High	Medium	Low
4	0%	0	3	1

Last Submitted 03/06/2019 **FAIL** Next Due 06/04/2019

Scan History All Vulnerabilities

Self-Assessment Questionnaire

Not Completed SAQ Wizard

Questionnaire Type	Completion Status	Answer Count			
		Yes	No	N/A	CC
N/A	N/A	0	0	0	0

Last Submitted N/A Next Due N/A

All Questionnaires

PCI SAQ v3 Now Required

The PCI Security Standards Council now requires all questionnaires submitted to conform to SAQ version 3. Qualys PCI reflects your previous SAQs prior to v3 as well as supporting artifacts.

We can help you get started. Just go to Questionnaires > New Questionnaire and choose SAQ Library to download the SAQ that's right for you.

Quick Answers

Network Scan
How do I configure my IPS to allow PCI scans?
What IP addresses do I need to scan?
What steps do I take after I scan?
How do I generate reports?

Questionnaires
Who needs to complete a questionnaire?
How many questionnaire versions are there?
How do I complete a questionnaire?

General
How do I change my login credentials?

© 2019 Sectigo Limited

Adding IP Addresses

Within the HackerGuardian 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. IP Addresses can also be added through the asset wizard.

The screenshot shows the Sectigo web interface. The top navigation bar includes the Sectigo logo, "Payment Card Industry Compliance", and user information "Roger Smith [Test Company12345] | Help | Log Out". A left sidebar contains links to Home, Network, Compliance, Questionnaires, Account, Settings, IP Assets (selected), Users, Contact Support, and Resources. The main content area is titled "IP Assets" and features a large text input field labeled "IP/Range:" containing the text "18.234.184.19, 104.37.182.5". To the right of this field are five buttons: "Walk me through Wizard", "Add IPs", "Remove IPs", "Out of Scope Assets", and "Discovery Scan". Below the input field is a section labeled "Domains:" containing a table with four columns: "Site", "Path", "Port", and "IP". The table has one row with dashes in each column. The footer of the page reads "© 2019 Sectigo Limited Privacy Policy".

The screenshot shows the "Add IPs" dialog box within the Sectigo interface. The dialog has a title bar "Add IPs" and contains the instruction "Enter IPs and ranges in the field below. See the Help for proper formatting." Below this is a large text input field. At the bottom of the dialog, it provides an example: "Example IP/Range: 192.168.0.200,192.168.0.87-192.168.0.92". There are two buttons at the bottom: "Add" and "Cancel". The background of the main interface is visible, showing the "Add IPs" link in the left sidebar and the "Add IPs" title in the main content area. The footer of the page reads "© 2019 Sectigo Limited Privacy Policy".

Deleting IP Addresses

Within the HackerGuardian portal click "Account" then "IP Assets". Click "Remove IPs" and then enter the IP Addresses you wish to remove. With a full license the IP Addresses will be automatically removed. If your using a trial account 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.

The screenshot shows the Sectigo HackerGuardian web interface. At the top, the Sectigo logo is on the left, and 'Powered by Qualys' is on the right. Below the logo, it says 'FORMERLY COMODO CA'. The main header bar is blue and contains 'Payment Card Industry Compliance' on the left and 'Roger Smith [Test Company12345] | Help | Log Out' on the right. The main content area is titled 'Remove IPs'. Inside this area, there's a sub-header 'Remove IPs' and a text box with the instruction: 'Enter IPs and ranges to be removed in the field below. See the Help for proper formatting.' Below this is a large, empty text input field with a vertical scrollbar. Under the input field, there's a link 'Select IPs' and an example: 'Example IP/Range: 192.168.0.200,192.168.0.87-192.168.0.92'. Further down, it says: 'Enter individual IPs or ranges above to request their removal from your account. This will send a request to the support team who will notify you upon successful removal. More information about proper formatting can be found in the Help.' Below this is a section titled 'Important:' followed by a bulleted list:

- Please recreate any scans you might have scheduled containing the above IPs as the removal will cause those tasks to fail.
- The above IPs will be removed from your account and from the scope of your current network status.
- Any historic information in previous scans and submitted reports will remain unaffected.
- To include the above IPs in future reports, you will need to re-add and re-scan the IPs.

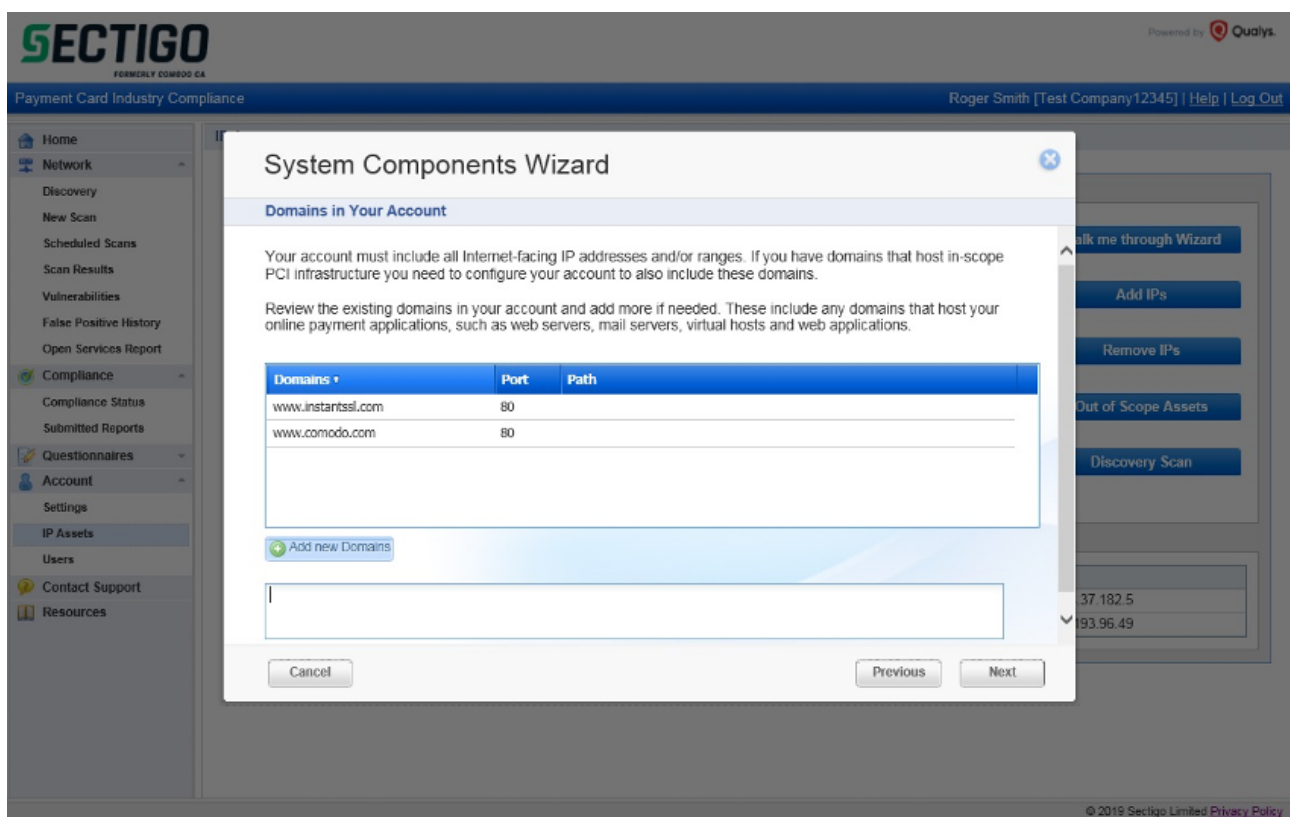
 At the bottom right of the form area are two buttons: 'Request Removal of Hosts' and 'Cancel'. The footer of the page contains '© 2019 Sectigo Limited Privacy Policy'.

Adding Domains

There are two methods of adding domains to an account. If you have multiple domains and use virtual hosting to serve them from a single IP Address you can use the wizard to resolve the domain name to an IP Address. When the IP Address is scanned the associated domains are listed in the report. Domains can also be scanned directly for cases such as a server using dynamic IP Addresses or the domain using a single IP Address.

To add domains which use virtual hosting 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. The path to a particular location which requires scanning can also be added such as `www.example.com/index.html`.

To add a domain which resolves to a single IP Address you can select "DNS" on the start scan page and select or add domains.



The screenshot shows the Sectigo web interface with the 'System Components Wizard' modal open. The wizard is titled 'System Components Wizard' and has a close button in the top right corner. The current step is 'Domains in Your Account'. The text explains that the account must include all Internet-facing IP addresses and/or ranges, and that domains hosting in-scope PCI infrastructure need to be configured. It also mentions reviewing existing domains and adding more if needed, including domains for online payment applications like web servers, mail servers, virtual hosts, and web applications.

Domains	Port	Path
www.instantssl.com	80	
www.comodo.com	80	

Below the table is an 'Add new Domains' button and a text input field. At the bottom of the wizard are 'Cancel', 'Previous', and 'Next' buttons. The background shows the Sectigo dashboard with a sidebar menu and a top navigation bar.

Deleting Domains

Within the HackerGuardian portal click "Account" then "DNS Hosts" or "Virtual host" depending on how you added the domain. Click the trash icon in the delete column to remove the domain.

The screenshot displays the HackerGuardian portal interface. At the top, the logo and "Powered by Qualys" are visible. Below the header, a navigation menu on the left includes options like Home, Network, Compliance, Questionnaires, Account, Settings, DNS Hosts (selected), Virtual Host, IP Assets, Users, Contact Support, and Resources. The main content area is titled "Display DNS Host" and features a table with columns for DNS, DATE MODIFIED, and Delete. The table lists six domains: www.comodo.com, app.hackerguardian.com, comodo.com, enterprisesssl.com, instantssl.com, and sectigo.com, each with a corresponding delete icon.

DNS	DATE MODIFIED	Delete
www.comodo.com	2020-05-21 11:17:18	
app.hackerguardian.com	2020-02-24 11:56:50	
comodo.com	2020-02-24 11:55:49	
enterprisesssl.com	2020-02-24 11:55:29	
instantssl.com	2020-02-24 11:55:02	
sectigo.com	2020-02-21 18:03:03	

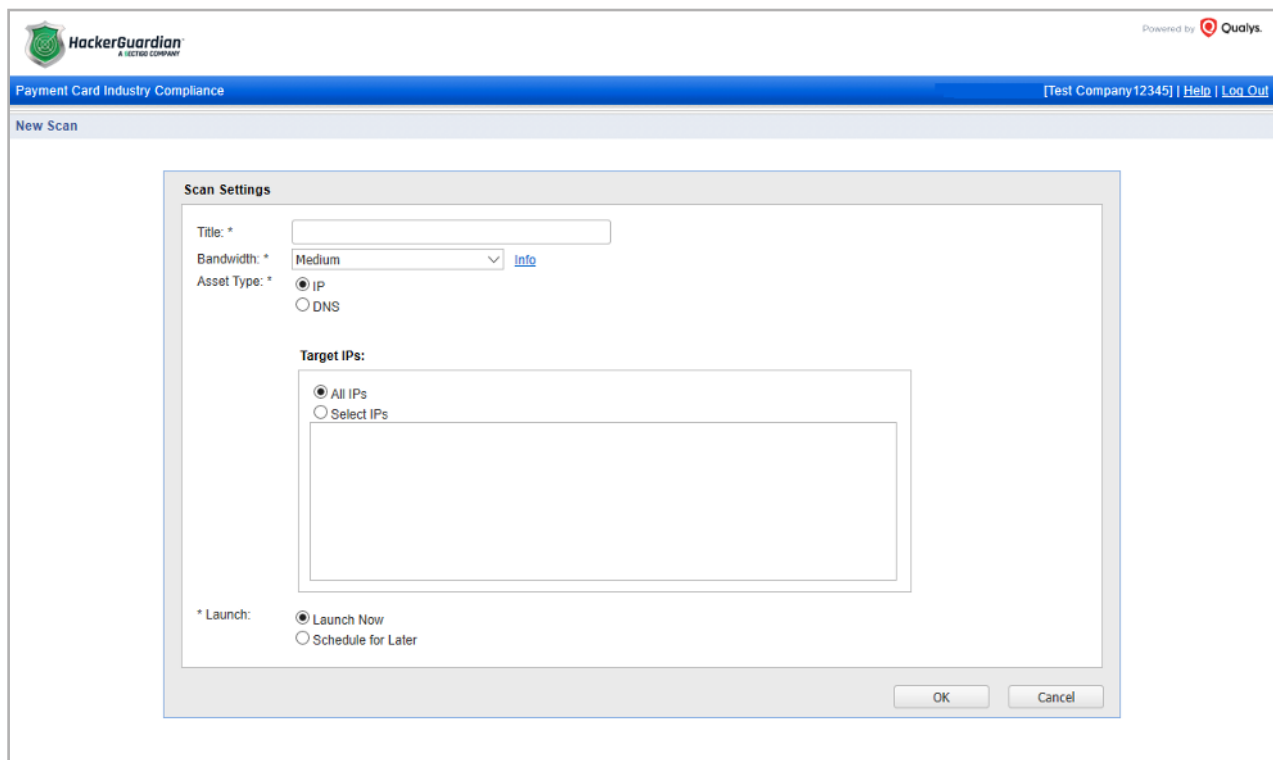
Starting Scans

Within the HackerGuardian 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.



The screenshot shows the 'New Scan' dialog box in the HackerGuardian portal. The dialog has a title bar with the HackerGuardian logo and 'Powered by Qualys'. Below the title bar is a blue header with 'Payment Card Industry Compliance' and '[Test Company 12345] | Help | Log Out'. The main content area is titled 'New Scan' and contains a 'Scan Settings' section. This section includes a 'Title' text field, a 'Bandwidth' dropdown menu set to 'Medium' with an 'info' link, and an 'Asset Type' section with radio buttons for 'IP' (selected) and 'DNS'. Below this is a 'Target IPs' section with radio buttons for 'All IPs' (selected) and 'Select IPs', followed by a large empty text area. At the bottom left is a '* Launch:' section with radio buttons for 'Launch Now' (selected) and 'Schedule for Later'. At the bottom right are 'OK' and 'Cancel' buttons.

Viewing Reports

Within the HackerGuardian 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.

The screenshot displays the Sectigo HackerGuardian portal interface. The top navigation bar includes the Sectigo logo, the text "Payment Card Industry Compliance", and the user name "Roger Smith [Test Company12345]". A sidebar on the left contains navigation links: Home, Network, Discovery, New Scan, Scheduled Scans, Scan Results (highlighted), Vulnerabilities, False Positive History, Open Services Report, Compliance, Questionnaires, Account, Contact Support, and Resources. The main content area is titled "Scans" and features a table with the following data:

Details	Rescan	Download	Vulnerabilities	Scan Title	Scan Status	Scan Date	Compliance	Cancel
				TEST	Finished	03/25/2019	FAIL	
				test compliance scan	No Host Alive	03/06/2019	-	
				test sectigo	Finished	01/11/2019	FAIL	

Below the table, a message states: "Please select an item in the list to view details." The footer of the page includes the copyright notice "© 2019 Sectigo Limited" and a link to the "Privacy Policy".

Reporting False Positives

Within the HackerGuardian 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".

SECTIGO FORMERLY COMODO CA Powered by Qualys

Payment Card Industry Compliance Roger Smith [Test Company12345] | Help | Log Out

Current Vulnerabilities Compliance Status ▶

SEARCH BY IP ADDRESS
Enter one or more IP addresses and/or IP ranges. Separate by using commas.
Search for IP Address
[Clear](#) [Find IP Address](#)

FILTER RESULTS
QID, Vulnerability Title or Hostname
☐ Display only PCI Fail Vulnerabilities

POTENTIAL SEVERITY LEVEL
☐ High ☐ Med ☐ Low

FALSE POSITIVES
☐ RED ☐ REJ ☐ EXP

CONFIRMED SEVERITY LEVEL
☐ High ☐ Med ☐ Low

ACCOUNT SUMMARY
HIGH 0
MED 3
LOW 1

[Review False Positives](#) [Download All](#) [Hide Filters](#) Showing 1 - 4 of 4

Vulnerability Title	Severity	IP Address	Scanned
ICMP Timestamp Request QID: 82003	LOW	104.37.182.5	03/25/2019
UDP Source Port Pass Firewall QID: 34020	MED	104.37.182.5	03/25/2019
SSL/TLS Server supports TLSv1.0 QID: 38628	MED	104.37.182.5	03/25/2019
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) QID: 38657	MED	104.37.182.5	03/25/2019

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.

SECTIGO FORMERLY COMODO CA Powered by Qualys

Payment Card Industry Compliance Roger Smith [Test Company12345] | Help | Log Out

Request False Positives

Vulnerability 1 of 1

Vulnerability: 38628 - SSL/TLS Server supports TLSv1.0
IP Address: 104.37.182.5
Hostname:

Severity: 3
CVSS Base Score: 4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 3.9 E:F/RL:W/RC:C
PCI Compliance Status: FAIL

PCI Reasons:
Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0
The QID adheres to the PCI requirements based on the CVSS basescore.

Vulnerability Details:
QID: 38628
Port/Service(Protocol): 443/General remote services (tcp)
SSL: Yes
Scan Title: TEST
Scan Date: 03/25/2019 at 12:37:24

Result:
* Please provide your reasons for requesting a false positive: ☐ [Use same comment for all the following requests](#)

© 2019 Sectigo Limited [Privacy Policy](#)

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

False Positive Request History

Details	ID	Title	IP	Requested	Reviewed	Status
	38726	OpenSSH Username Enumeration Vulnerability	18.234.184.19	03/06/2019	03/06/2019	Rejected

[38726] - Open SSH Username Enumeration Vulnerability

General Information

Host IP:	18.234.184.19	Severity Level:		Port/Service:	- / General remote services
Scan Title:	test sectigo	Scanned:	01/11/2019	Status:	Rejected

Comment History

© 2019 Sectigo Limited [Privacy Policy](#)

Generate Attestation of Scan Compliance, Detailed report and Executive Summary

Within the HackerGuardian 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. 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 which specifies a 90 day limit but is intended to follow PCI best practice.

Compliance Status

Overall Status	Hosts	Vulnerabilities	Potential Vulnerabilities	Actions
	In Account: 4 Not Live: 1 Compliant: 0 Not Compliant: 1 Not Current: 2	0 3 1	0 0 0	

Table:

Details	IP	Hostname	Operating System	Compliance	Vulnerabilities	Scan Date
	104.37.182.5		Linux 2.6		4	03/25/2019

Please select an item in the list to view details.

© 2019 Sectigo Limited [Privacy Policy](#)

For each special note found a submission must be made to ensure the service is securely implemented. This information requested must be provided for a Compliant report to be issued. 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. The name and title to appear on the Attestation of Scan Compliance must be provided. 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.

The screenshot shows the 'Report Generation Wizard' window in the Sectigo interface. The 'Special Notes' tab is active. The text explains that special notes identify software that may pose a risk due to insecure implementation. It instructs the user to provide appropriate information for each issue listed below. A table with one row is shown, containing an IP address, an issue description, and a 'Securely Implemented?' checkbox. The 'Yes' radio button is selected. Below the table is a text input field for a comment. The wizard has 'Cancel', 'Previous', and 'Next' buttons at the bottom.

Report Generation Wizard

Special Notes

Special Notes identify the presence of certain software that may pose a risk to your environment due to insecure implementation rather than an exploitable vulnerability. This software may include remote access software and point-of-sale (POS) software.

All of the issues that require Special Notes are listed below. Please provide appropriate information for each.

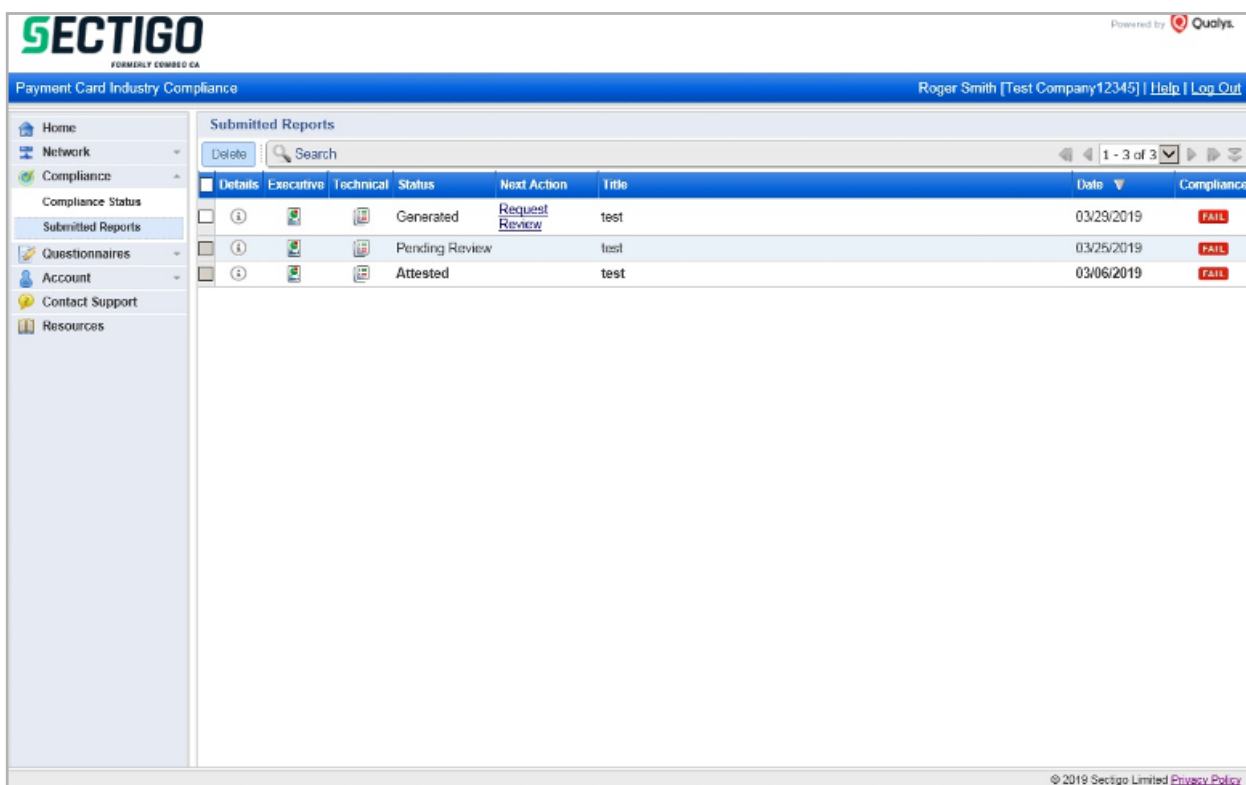
Enter a single comment for all issues

IP/Hostname	Issue	Securely Implemented?
104.37.182.5	150010 - External Links Discovered	<input checked="" type="radio"/> Yes <input type="radio"/> No

Cancel Previous Next

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.



The screenshot displays the Sectigo Payment Card Industry Compliance dashboard. The top navigation bar includes the Sectigo logo, the text "FORMERLY COMBOD CA", and a "Powered by Qualys" badge. The main header shows the user "Roger Smith [Test Company12345]" with links for "Help" and "Log Out". A left sidebar contains navigation links: Home, Network, Compliance (selected), Compliance Status, Submitted Reports (selected), Questionnaires, Account, Contact Support, and Resources. The main content area is titled "Submitted Reports" and features a table with columns: Details, Executive, Technical, Status, Next Action, Title, Date, and Compliance. The table contains three rows of data, all with a "FAIL" status.

Details	Executive	Technical	Status	Next Action	Title	Date	Compliance
<input type="checkbox"/> ⓘ			Generated	Request Review	test	03/29/2019	FAIL
<input type="checkbox"/> ⓘ			Pending Review		test	03/25/2019	FAIL
<input type="checkbox"/> ⓘ			Attested		test	03/06/2019	FAIL

© 2019 Sectigo Limited [Privacy Policy](#)

The executive summary, detailed report and attestation of scan compliance are contained in a single PDF called the Technical report. A separate executive summary report is also available to download. This document should be provided to your acquirer after approval as part of the PCI Compliance process.



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:	123455687	Email:		Telephone:	12345	Email:	
Business Address:				Business Address:	3rd Floor Building 28, 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		

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

Within the HackerGaurdian 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. A minimum recurring schedule is a daily scan and maximum is a scan every 13 weeks.

The screenshot shows the 'New Scan' configuration window in the Sectigo interface. The window has a title bar with the Sectigo logo and 'FORMERLY COMODO CA'. Below the title bar is a blue navigation bar with 'Payment Card Industry Compliance' and user information 'Roger Smith [Test Company12345] | Help | Log Out'. The main content area is titled 'Scan Settings' and contains the following fields:

- Title:** A text input field containing 'Recurring scan'.
- Bandwidth:** A dropdown menu set to 'Medium' with an 'Info' link.
- Target IPs:** Radio buttons for 'All IPs' and 'Select IPs'. 'Select IPs' is selected, and a text area below contains the IP address '104.47.45.36'.
- Launch:** Radio buttons for 'Launch Now' and 'Schedule for Later'. 'Schedule for Later' is selected.
- Scheduler:** A section titled 'Select a date and time when this scan should launch' containing:
 - Launch on:** Date pickers for 'June', '29', and '2019'.
 - At the time:** Time pickers for '06', '00', and a dropdown for 'GMT +00'.
 - Recurrence:** A checked checkbox for 'Repeat this scan' followed by 'every 12 weeks on Saturday at 06:00 GMT +00'.
- Deactivate this schedule:** An unchecked checkbox.

At the bottom right are 'OK' and 'Cancel' buttons. The footer of the window shows '© 2019 Sectigo Limited Privacy Policy'.

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

The screenshot shows the 'Scheduled Scans' page in the Sectigo interface. The page has a title bar with the Sectigo logo and 'FORMERLY COMODO CA'. Below the title bar is a blue navigation bar with 'Payment Card Industry Compliance' and user information 'Roger Smith [Test Company12345] | Help | Log Out'. The main content area is titled 'Scheduled Scans' and contains a table with the following columns: 'Details', 'Edit', 'Scan Title', and 'Next Launch Date'. The table has one row with the following data:

Details	Edit	Scan Title	Next Launch Date
<input type="checkbox"/>	<input type="checkbox"/>	Recurring scan	06/29/2019 at 06:00:00

Below the table is a section titled 'Scheduled Scan Details' with the following information:

- Title:** Recurring scan
- Launch Date:** 06/29/2019 at 06:00:00
- Target:** 104.47.45.36
- Bandwidth:** Medium
- Recurrence:** Runs every 12 weeks on Saturday at 06:00:00 (GMT)

The footer of the page shows '© 2019 Sectigo Limited Privacy Policy'.

Update Account Details

Within the HackerGuardian 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.

SECTIGO
FORMERLY COMODO CA

Payment Card Industry Compliance Roger Smith [Test Company12345] | Help | Log

Home Network Compliance Questionnaires Account Settings IP Assets Users Contact Support Resources

Settings

Merchant Information [Edit](#)

Company Name: Test Company12345
Address 1: 1 listerhills
Address 2: Unit 1
City: Bradford
Country: United Kingdom
State: None
Zip Code: BD17DQ
URL:
SIC Industry Code:
Language: English

Primary Contact [Edit](#)

Contact Name: Roger Smith
This name will be displayed on the cover page of reports.
Title: CFO
Phone: 123455667
Email:

Organization Information [Edit](#)

DBA(s):
Merchant Level: Level 4
Approximate number of transactions/accounts handled per year:
Brief Description of Business
Locations
Third Party Service Providers
Processor:
Gateway:
Web Hosting:
Shopping Cart:
Co-location:
Other:
Point of Sale (POS) software/hardware or virtual terminal in use

© 2019 Sectigo Limited Privacy P

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.

SECTIGO
FORMERLY COMODO CA

Payment Card Industry Compliance Roger Smith [Test Company12345] | Help | Log Out

Home Network Compliance Questionnaires Account Settings IP Assets Users Contact Support Resources

Users

[New User](#) Search

Edit	First Name	Last Name	User Login	Phone	Email	Status	Updated
	Roger	Smith	merchanttest@sectigo	123455667	ross.hartnell@sectigo.com	Active	03/08/2019

1 - 1 of 1

Contact Support

Please do not use the support form within the portal to contact support, instead create a support ticket 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

Thirty days before expiry you will be sent an invoice to renew your HackerGuardian account. You can login to <https://store.hackerGuardian.com> to pay the invoice and renew your account.

If you purchased HackerGuardian through a partner please contact them to renew your licence.

Licenses can only be renewed 180 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 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. IP Address removal requires approval on trial accounts and this does not apply to paid accounts.