The background features a dark blue gradient with three large, overlapping, perspective-view grids of green lines. The grids are composed of small squares and are oriented at different angles, creating a sense of depth and a digital or architectural aesthetic.

Sectigo HackerGuardian Version 2.0 User Guide

SECTIGO[®]

Table of Contents

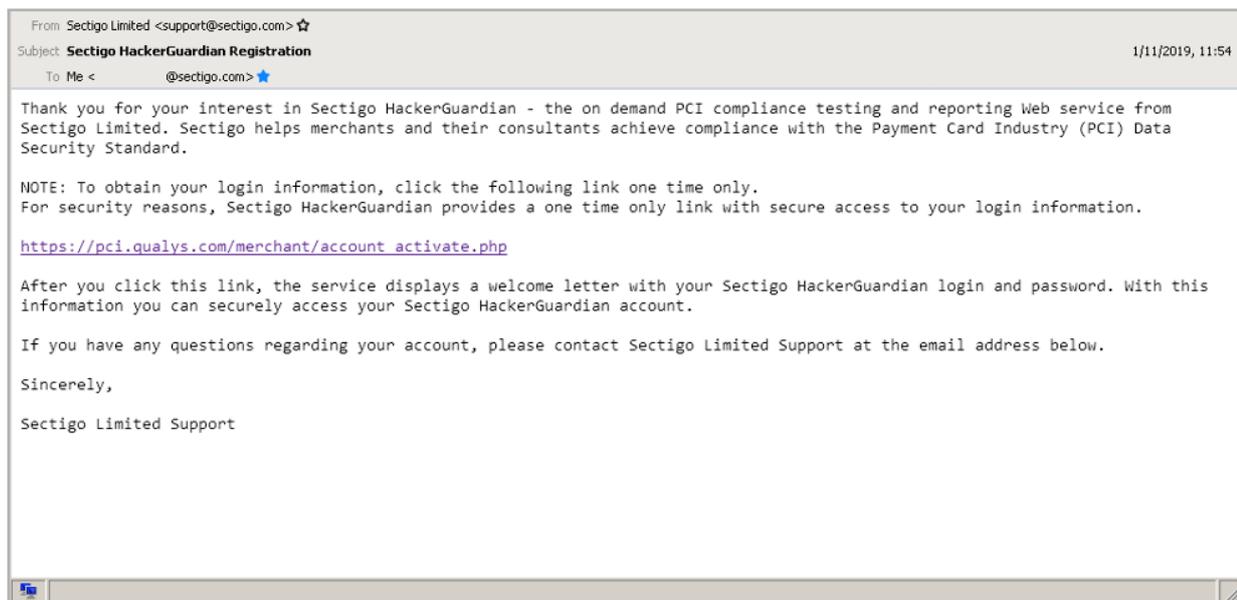
Introduction.....	03
Purchase and Account Activation.....	03
Portal Login.....	04
Adding IP Addresses.....	05
Deleting IP Addresses.....	06
Adding Domains.....	07
Deleting Domains.....	08
Starting Scans.....	09
Viewing Reports.....	10
Reporting False Positives.....	11
Generate Attestation of Scan Compliance, 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.

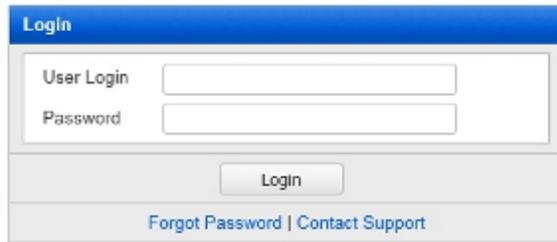
Purchase and Account Activation

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.



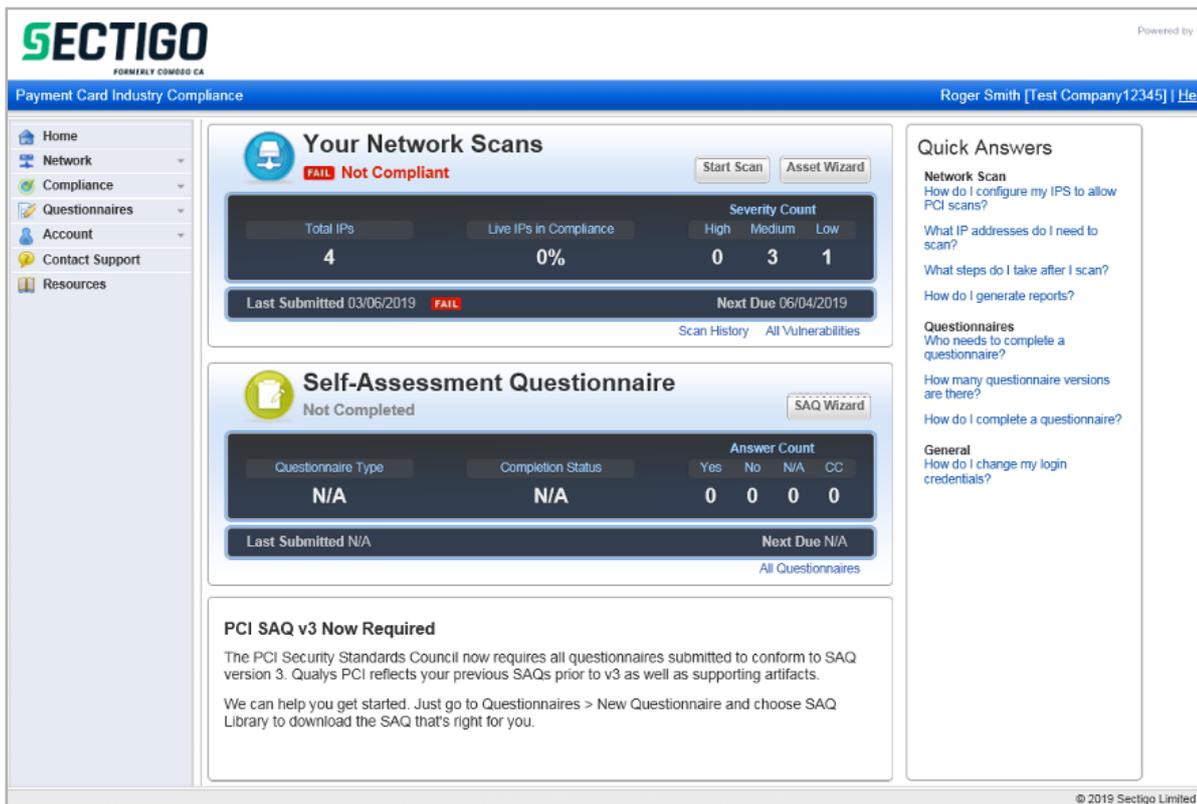
Portal Login

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



The screenshot shows a login form with a blue header labeled "Login". Below the header are two input fields: "User Login" and "Password". A "Login" button is positioned below the fields. At the bottom of the form, there are two links: "Forgot Password" and "Contact Support".

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



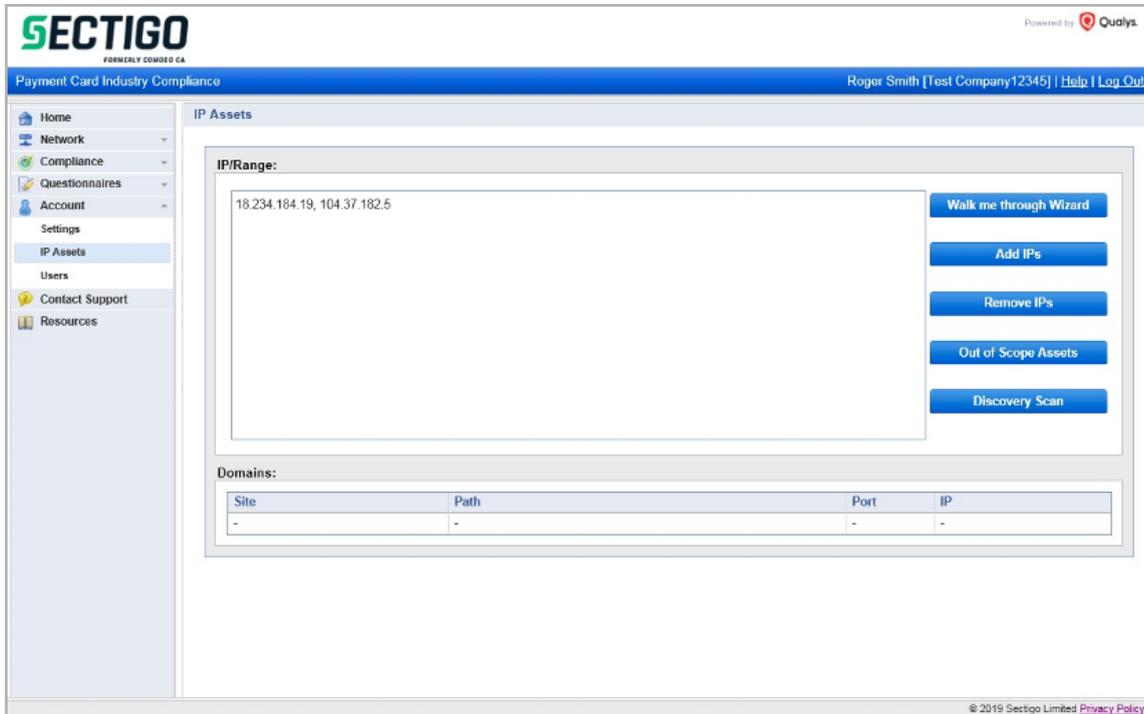
The screenshot displays the Sectigo PCI Compliance dashboard. The top navigation bar includes the Sectigo logo, the text "Payment Card Industry Compliance", and the user name "Roger Smith [Test Company12345] | Help". A left sidebar contains navigation links for Home, Network, Compliance, Questionnaires, Account, Contact Support, and Resources. The main content area is divided into three sections:

- Your Network Scans:** Shows a "FAIL Not Compliant" status. A table displays scan metrics: Total IPs (4), Live IPs in Compliance (0%), and Severity Count (High: 0, Medium: 3, Low: 1). It also shows the last submitted date (03/06/2019) and the next due date (06/04/2019).
- Self-Assessment Questionnaire:** Shows a "Not Completed" status. A table displays questionnaire metrics: Questionnaire Type (N/A), Completion Status (N/A), and Answer Count (Yes: 0, No: 0, N/A: 0, CC: 0). It also shows the last submitted date (N/A) and the next due date (N/A).
- PCI SAQ v3 Now Required:** A text-based announcement regarding the new PCI Security Standards Council requirements for SAQ version 3.

A "Quick Answers" sidebar on the right provides links to help topics for Network Scans, Questionnaires, and General user actions.

Adding IP Addresses

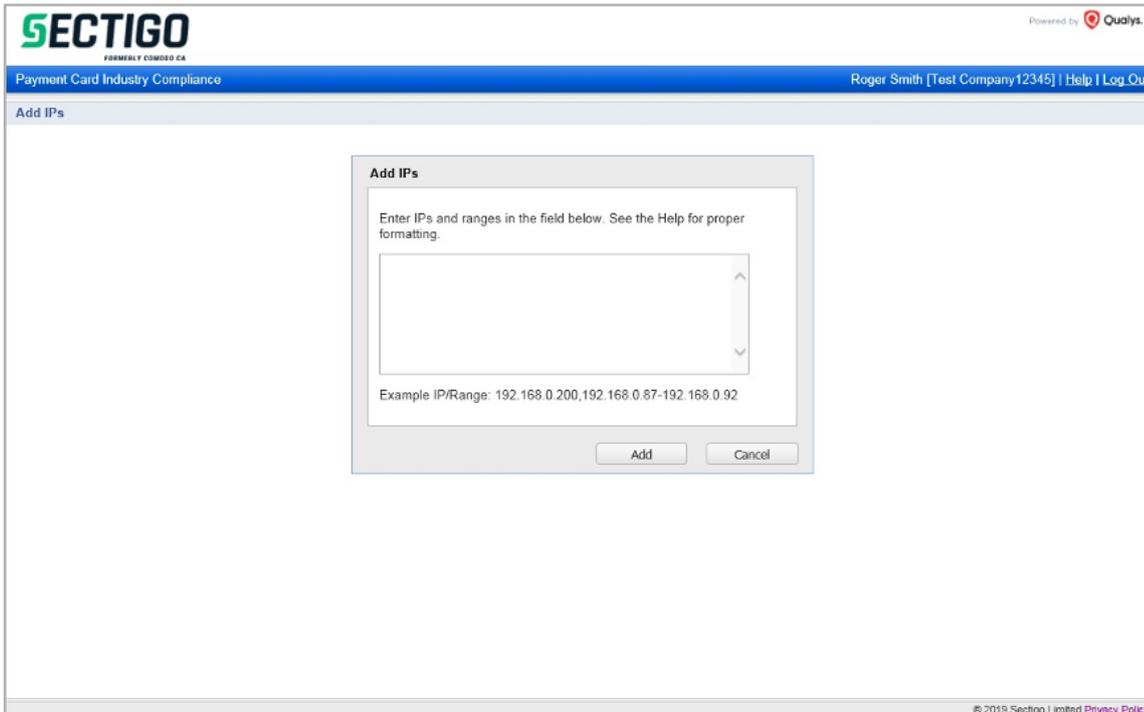
Within the HackerGuardian portal click "Account" then "IP Assets". Click "Add IPs" to add IP Addresses or IP Address ranges. IP Address can also be added automatically when running a new scan. IP Addresses can also be added through the asset wizard.



The screenshot shows the Sectigo web interface for managing IP Assets. The top navigation bar includes the Sectigo logo, the text "FORMERLY COMODO CA", and "Powered by Qualys". The main header displays "Payment Card Industry Compliance" and the user "Roger Smith [Test Company12345] | Help | Log Out". A left sidebar contains navigation options: 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 blue buttons: "Walk me through Wizard", "Add IPs", "Remove IPs", "Out of Scope Assets", and "Discovery Scan". Below the input field is a "Domains:" section with a table:

Site	Path	Port	IP
-	-	-	-

At the bottom right of the interface, there is a copyright notice: "© 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 following text: "Enter IPs and ranges in the field below. See the Help for proper formatting." Below this text is a large text input field. Underneath the input field, an example is provided: "Example IP/Range: 192.168 0.200,192.168 0.87-192.168 0.92". At the bottom of the dialog are two buttons: "Add" and "Cancel". The background of the main interface is visible, showing the "Add IPs" header and the same navigation and header elements as the previous screenshot. At the bottom right, the copyright notice "© 2019 Sectigo Limited Privacy Policy" is visible.

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 left is the Sectigo logo with the text 'FORMERLY COMODO CA'. At the top right, it says 'Powered by Qualys'. Below the logo is a blue navigation bar with '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 is a sub-section also titled 'Remove IPs' 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. Underneath the input field is a link that says 'Select IPs'. Below the link is an example: 'Example IP/Range: 192.168.0.200,192.168.0.87-192.168.0.92'. This is followed by instructions: '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:' with 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.

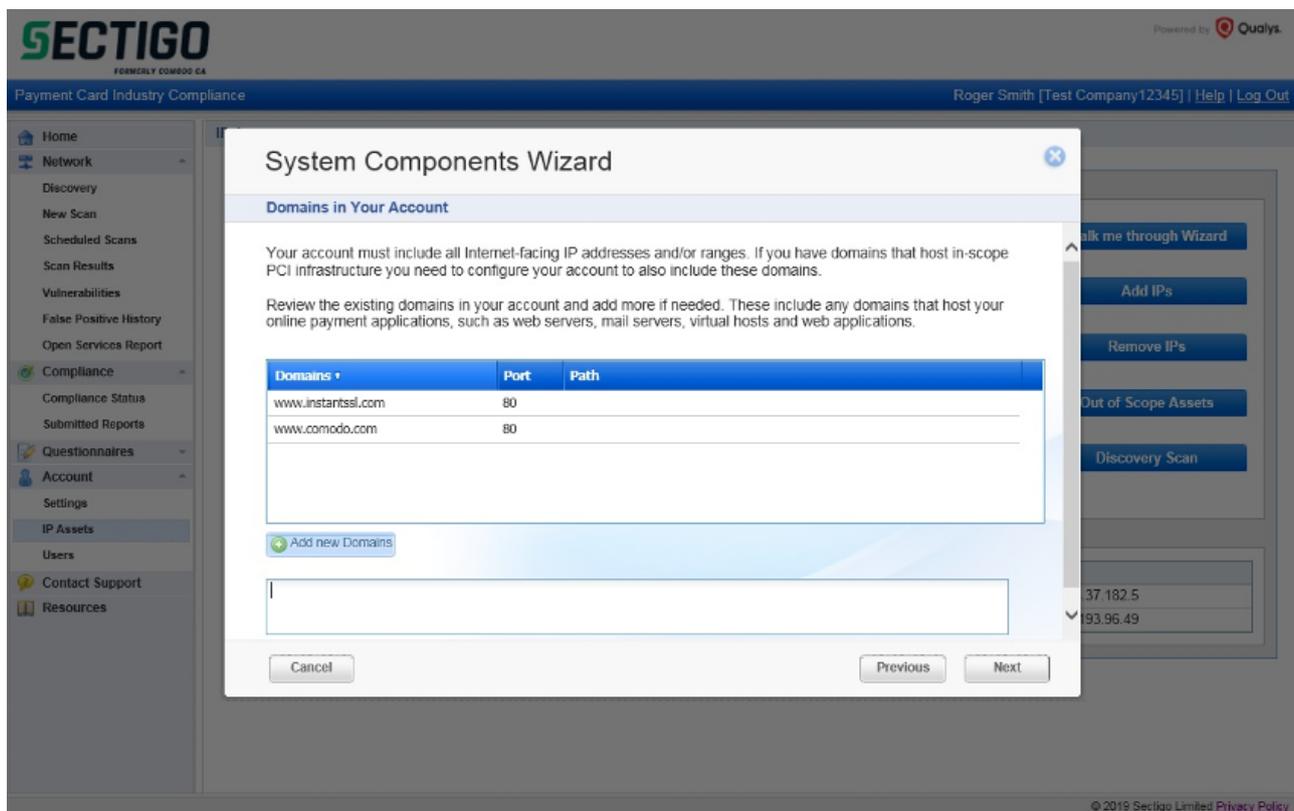
 At the bottom right of the form are two buttons: 'Request Removal of Hosts' and 'Cancel'. At the very bottom of the page, there is a footer: '© 2019 Sectigo Limited [Privacy Policy](#)'.

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 System Components Wizard interface. The wizard is titled "System Components Wizard" and is currently on the "Domains in Your Account" step. The interface includes a navigation menu on the left, a main content area with instructions, a table of domains, and a "Add new Domains" button. The table lists two domains: `www.instantssl.com` and `www.comodo.com`, both with port `80`. The wizard also features "Previous" and "Next" buttons at the bottom.

System Components Wizard

Domains in Your Account

Your account must include all Internet-facing IP addresses and/or ranges. If you have domains that host in-scope PCI infrastructure you need to configure your account to also include these domains.

Review the existing domains in your account and add more if needed. These include any domains that host your online payment applications, such as web servers, mail servers, virtual hosts and web applications.

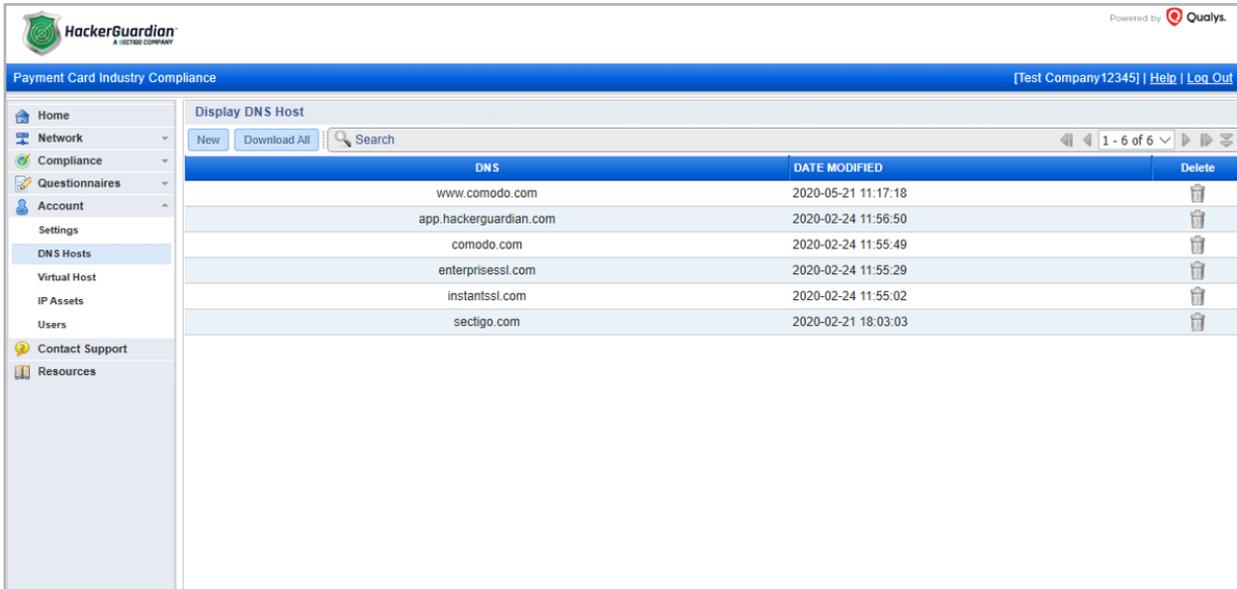
Domains	Port	Path
<code>www.instantssl.com</code>	80	
<code>www.comodo.com</code>	80	

[Add new Domains](#)

Cancel Previous Next

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 shows the HackerGuardian portal interface. The top navigation bar includes the HackerGuardian logo, the text "Payment Card Industry Compliance", and the user information "[Test Company12345] | Help | Log Out". The left sidebar contains a menu with items: Home, Network, Compliance, Questionnaires, Account, Settings, DNS Hosts, Virtual Host, IP Assets, Users, Contact Support, and Resources. The main content area is titled "Display DNS Host" and features a search bar and a table of DNS hosts.

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	

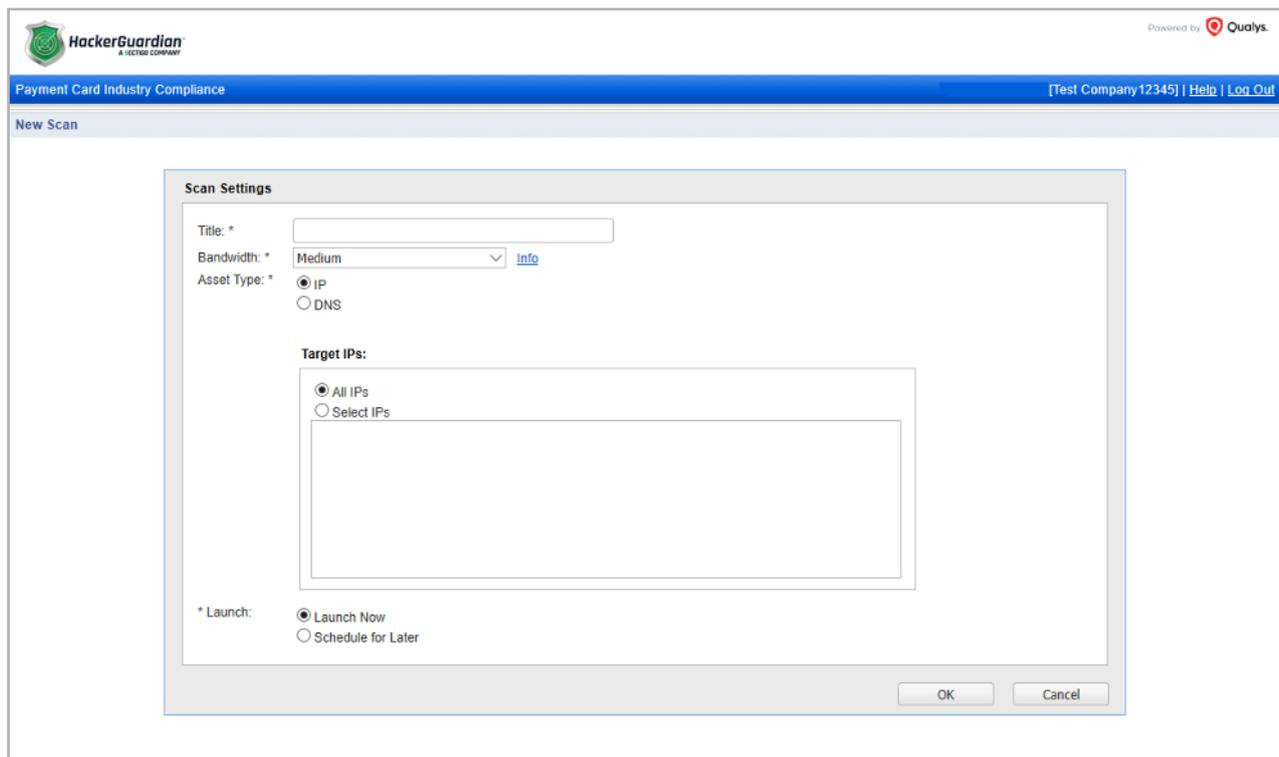
Starting Scans

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.



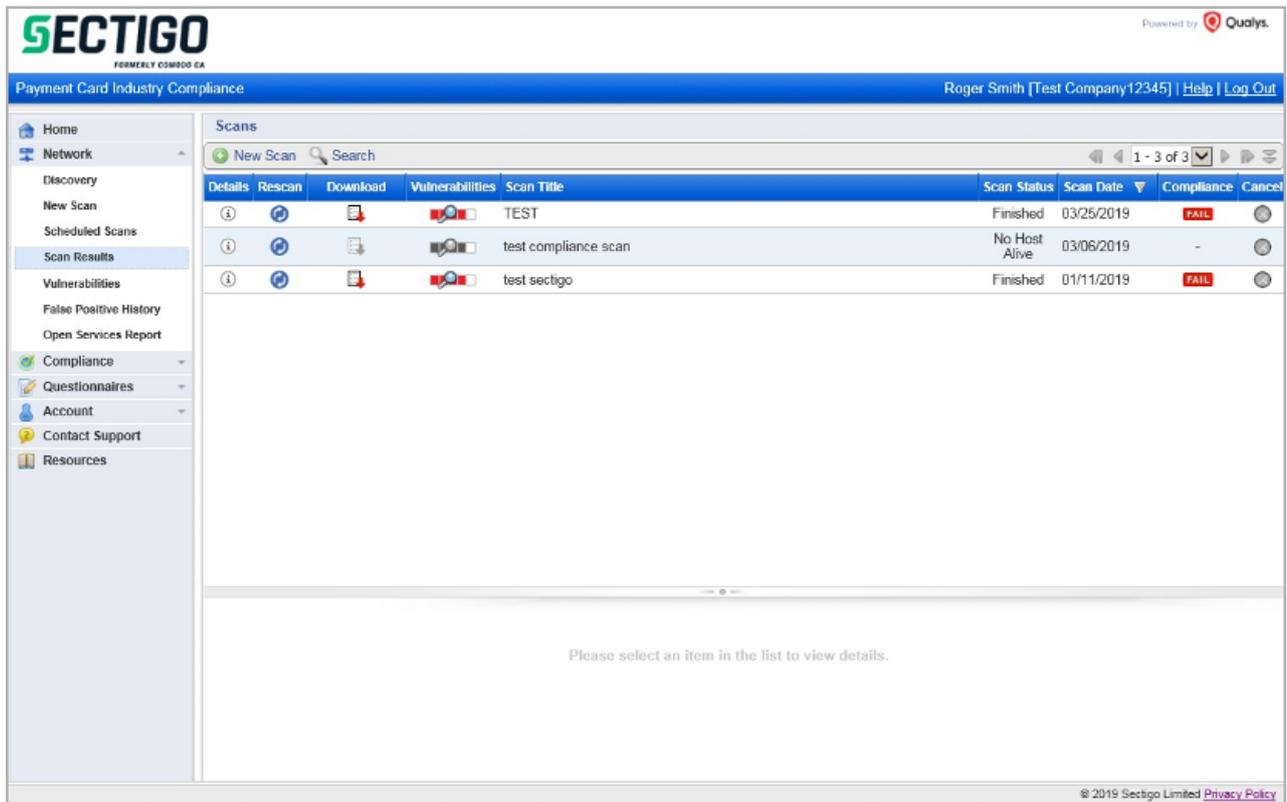
The screenshot shows the 'New Scan' configuration window in the HackerGuardian portal. The window is titled 'New Scan' and is part of the 'Payment Card Industry Compliance' section. It is powered by Qualys. The configuration options are as follows:

- Title:** * [Text input field]
- Bandwidth:** * Medium (dropdown menu) [info]
- Asset Type:** *
 - IP
 - DNS
- Target IPs:**
 - All IPs
 - Select IPs
- * Launch:**
 - Launch Now
 - Schedule for Later

Buttons for 'OK' and 'Cancel' are located at the bottom right of the window.

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 interface. The top navigation bar includes the Sectigo logo (formerly OSWEGO CA) and the text "Powered by Qualys". The main header shows "Payment Card Industry Compliance" and the user "Roger Smith [Test Company12345] | Help | Log Out".

The left sidebar contains a navigation menu with the following items: Home, Network (selected), Discovery, New Scan, Scheduled Scans, Scan Results (selected), Vulnerabilities, False Positive History, Open Services Report, Compliance, Questionnaires, Account, Contact Support, and Resources.

The main content area is titled "Scans" and features a "New Scan" button and a search field. Below this is a table with the following columns: Details, Rescan, Download, Vulnerabilities, Scan Title, Scan Status, Scan Date, Compliance, and Cancel. The table contains three rows of scan 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 reads: "Please select an item in the list to view details." The footer of the page contains the copyright notice: "© 2019 Sectigo Limited 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".

The screenshot displays the 'Current Vulnerabilities' interface. It includes a search bar for IP addresses, filter options for severity levels (High, Med, Low) and PCI Fail vulnerabilities, and an account summary showing 3 Medium severity vulnerabilities. A table lists four vulnerabilities:

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 FAIL	MED	104.37.182.5	03/25/2019
SSL/TLS Server supports TLSv1.0 QID: 38628 FAIL	MED	104.37.182.5	03/25/2019
Birthday attacks against TLS ciphers with 64-bit 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.

The screenshot displays the 'Request False Positives' interface for a specific vulnerability:

- 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:MAu/N/C:P/I:N/A:N
- CVSS Temporal Score:** 3.9 E:F/RL:W/R/C:C
- PCI Compliance Status:** FAIL (MED)

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

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

False Positive Request History

Details	QID	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:	MED	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	HIGH : 0 MED : 3 LOW : 1	HIGH : 0 MED : 0 LOW : 0	

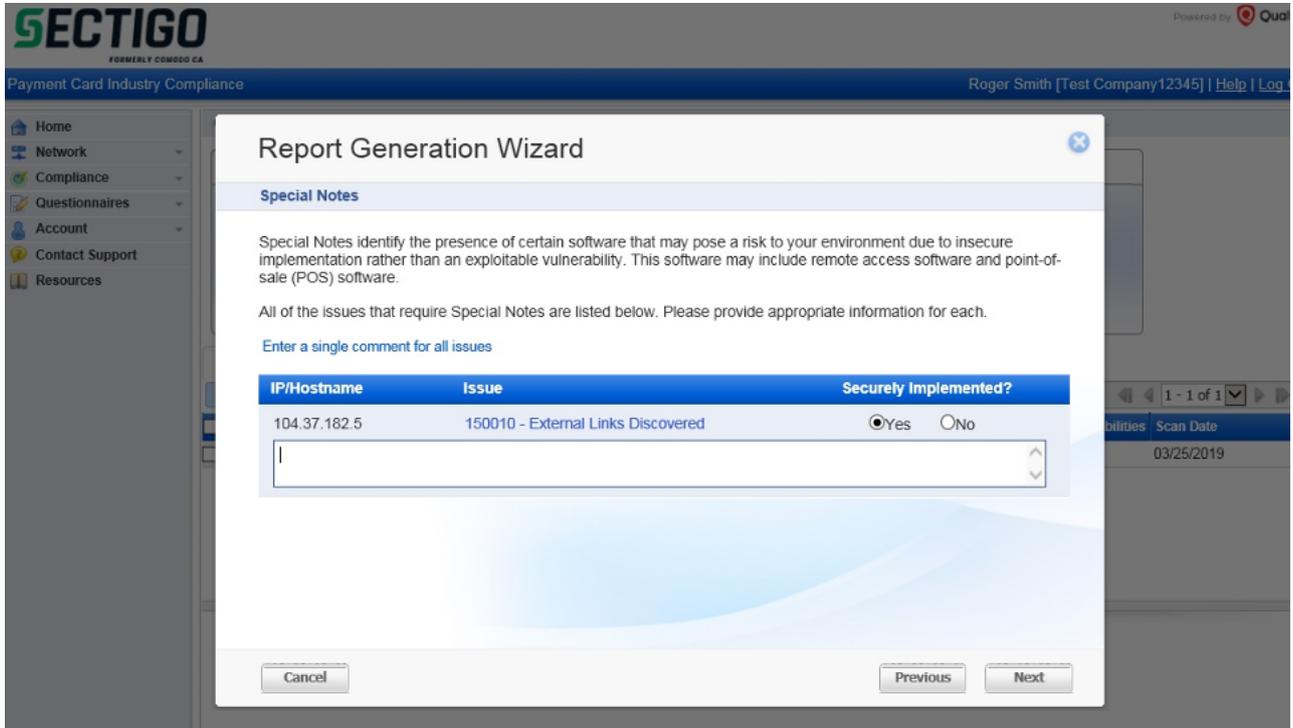
Table:

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.



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 "Powered by Qualys". The main header shows "Payment Card Industry Compliance" and the user "Roger Smith [Test Company12345] | Help | Log Out".

The left sidebar contains a navigation menu with the following items: Home, Network, Compliance, Compliance Status, Submitted Reports, Questionnaires, Account, Contact Support, and Resources. The "Submitted Reports" item is currently selected.

The main content area is titled "Submitted Reports" and features a table with the following columns: Details, Executive, Technical, Status, Next Action, Title, Date, and Compliance. The table contains three rows of data:

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

At the bottom right of the dashboard, there is a copyright notice: "© 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 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 HackerGuardian 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 'Scan Settings' form in the Sektigo interface. The form is titled 'Scan Settings' and contains the following fields and options:

- 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'. The 'Select IPs' option is chosen, and a text area below contains the IP address '104.47.45.36'.
- Launch:** Radio buttons for 'Launch Now' and 'Schedule for Later'. The 'Schedule for Later' option is chosen.
- Scheduler:** A section titled 'Scheduler' with the instruction 'Select a date and time when this scan should launch'. It includes:
 - 'Launch on: June 29 2019' with a calendar icon.
 - 'At the time: 06:00 GMT +00'.
 - 'Recurrence: Repeat this scan every 12 weeks on Saturday at 06:00 GMT +00'.
- A checkbox labeled 'Deactivate this schedule' is unchecked.
- Buttons for 'OK' and 'Cancel' are at the bottom right.

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

The screenshot shows the 'Scheduled Scans' page in the Sektigo interface. The page has a sidebar on the left with navigation options: Home, Network, Discovery, New Scan, Scheduled Scans, Scan Results, Vulnerabilities, False Positive History, Open Services Report, Compliance, Questionnaires, Account, Contact Support, and Resources. The main content area is titled 'Scheduled Scans' and includes a 'Delete' button and a 'New Scan' button. Below these is a table with the following data:

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

Below the table is a 'Scheduled Scan Details' section 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)

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.

The screenshot shows the Sectigo account settings page. The left sidebar contains navigation links: Home, Network, Compliance, Questionnaires, Account, Settings, IP Assets, Users, Contact Support, and Resources. The main content area is titled "Settings" and contains three sections:

- 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 (Note: 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.

The screenshot shows the Sectigo account users page. The left sidebar contains navigation links: Home, Network, Compliance, Questionnaires, Account, Settings, IP Assets, Users, Contact Support, and Resources. The main content area is titled "Users" and contains a table with one user entry:

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 license.

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.