COMODO
Creating Trust Online®

Comodo HackerGuardian

Software Version 10.0

Administrator Guide

Guide Version 10.0.031913

Comodo CA Limited
3rd floor, Office Village Exchange Quay
Trafford Road, Salford, Manchester M5 3EQ
United Kingdom

Table of Contents

1. Introduction to HackerGuardian

1.1. Overview

HackerGuardian is a fully configurable vulnerability assessment and reporting service for networks and web servers. Our remote audits run over 28,000 individual security tests on your organization's servers then provide expert advice to help you fix any vulnerabilities.

Because Comodo is PCI Approved Scanning Vendor (ASV), our 'HackerGuardian Scan Control Center' range provides everything a merchant needs to become compliant with the PCI vulnerability scanning guidelines. Comodo also offers two other scanning services - 'HackerProof and 'SiteInspector'. 'HackerProof' is the daily vulnerability scanning and certification service that builds consumer trust into your website. 'Site Inspector' connects to your website from a customer's point of view to determine whether or not your website contains malicious content that could harm your customer's machines.

HackerGuardian also offers a web-based Internal Scanning feature to run vulnerability scans on the individual devices connected to your network and protected by a firewall or other network security devices.

- **Free PCI Scan** is valid for 90 days and allows merchants to achieve PCI scan compliancy free of charge.
- **PCI Scan Compliancy Service** on-demand security auditing service. Allows merchants to meet the quarterly scan requirements of the PCI regulations. Produces compliance reports that can be submitted to acquiring banks.
- **PCI Scan Compliancy Service Enterprise** - as above but allows 100 PCI scans per quarter on up to 20 IP addresses and includes advanced reporting and configuration options.
- **Site Inspector Scanning**, the next dimension of website security scanning. SiteInspector acts as a vulnerable customer, visits your website, and views all pages. It then determines if your webcontent is malicious and reports the suspect to the website owner.

1.2. HackerGuardian PCI Scan Compliancy Service

The PCI Scan Compliancy Service is an on-demand, vulnerability assessment scanning solution to enable merchants and service providers to achieve PCI scan compliance.

After each scan, users receive a comprehensive vulnerability report detailing any security issues alongside remediation advice and advisories to help fix them.

Following a successful scan (no vulnerabilities with a CVSS base score greater than 4.0), merchants are provided with an official PCI compliance report that can be sent to an acquiring bank.

The **Standard** version enables merchants to run 10 PCI scans per quarter on up to 5 IP addresses using the full complement of over 24,000 individual vulnerability tests.

The **Enterprise** version is a more powerful and flexible service which provides for up to 100 scans per quarter on 20 IP addresses.

The IP ranges that HackerGuardian scans originate from are:

199.66.200.32/28 (which translates as 199.66.200.32 through 199.66.200.48) and

91.209.196.32/28 (which translates as 91.209.196.32 through 91.209.196.48).

1.3. Free Vulnerability Scan

Available to website owners, network operators and home users free of charge, the service enables users to run HackerGuardian PCI scans to identify potential security threats. The free service is limited to 5 scans over 3 IP addresses and is non user customizable.

2.PCI Scanning Service

2.1.Starting up with HackerGuardian PCI Scanning Service

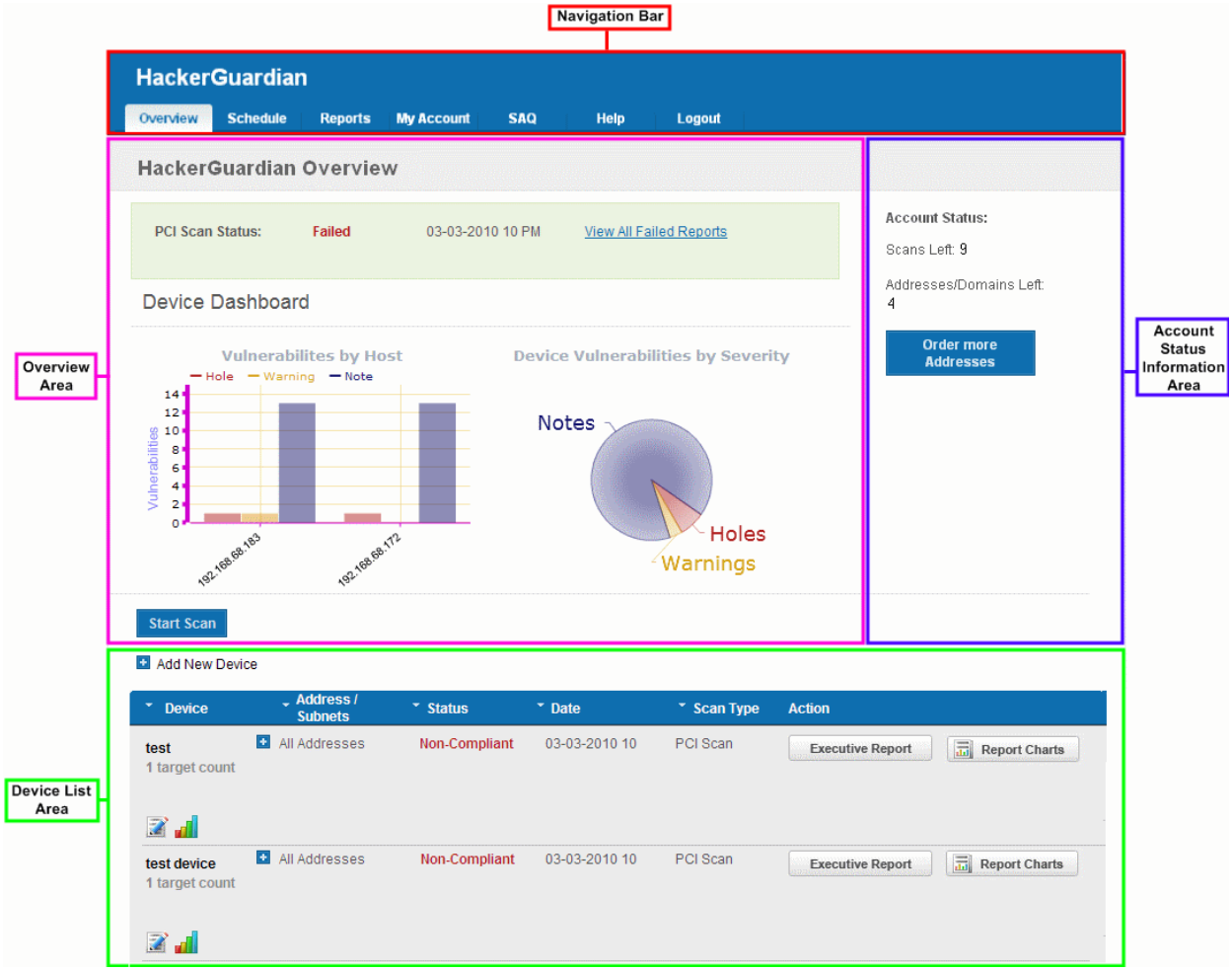
This section explains how to configure and run your first scanning task using the HackerGuardian PCI Scanning Service.

Click the links below for detailed explanations:

- Introduction to the Interface
- Running your first PCI Scan
- Accessing Self Assessment Questionnaire

2.1.1. Introduction to the Interface

The streamlined web-based main management interface provides easy access to each functional area of the HackerGuardian interface.



2.1.1.1. Navigation Bar

The navigation bar contains tabs to access each major functional area:

- Overview - Displays the 'Overview' and 'Device List' areas.

  The 'Overview' area provides the administrator with a summary of the last scan and serves as a launchpad for starting a new scan on the selected device.

As the name suggests, the 'Device List' area contains a list of all devices created and a summary of the last scan that was run on that device. It also allows the administrator to add, edit and configure devices and to view scan reports.

Clicking the bar chart icon  , underneath a device name will display statistics for that device in the main 'Overview' area.

- Schedule - Displays a list of existing scans, allows to add new schedule of scanning.
- Reports - Enables the administrator to view the summary and complete scan reports.
- My Account - Enables the administrator to configure account settings, view license information, configure email alerts, configure scan options, choose which plug-ins are to be deployed during a scan etc.
- SAQ - Allows the administrator to access the Self Assessment Questionnaire (SAQ) for their self-evaluation on compliance with the Payment Card Industry Data Security Standard (PCI DSS)
- Help - Contains links to the user Guide and to the Comodo support ticketing system. Also enables the administrator to launch a simple setup wizard for PCI Scanning.

2.1.1.2. Overview Area

The 'Overview' area displays the status of the HackerProof and PCI Scans and a dashboard summary of the scan reports from last performed scan on the device selected from the 'Device List' area. Click here for more details.

2.1.1.3. Device List Area

The Device List area displays a list of devices added to HackerGuardian and provides an at-a-glance summary of the status of each device. This area also allows the administrators to create a new device, edit a device, add IP's to a device and open device reports. Click here for more details.

2.1.1.4. Account Status Information Area

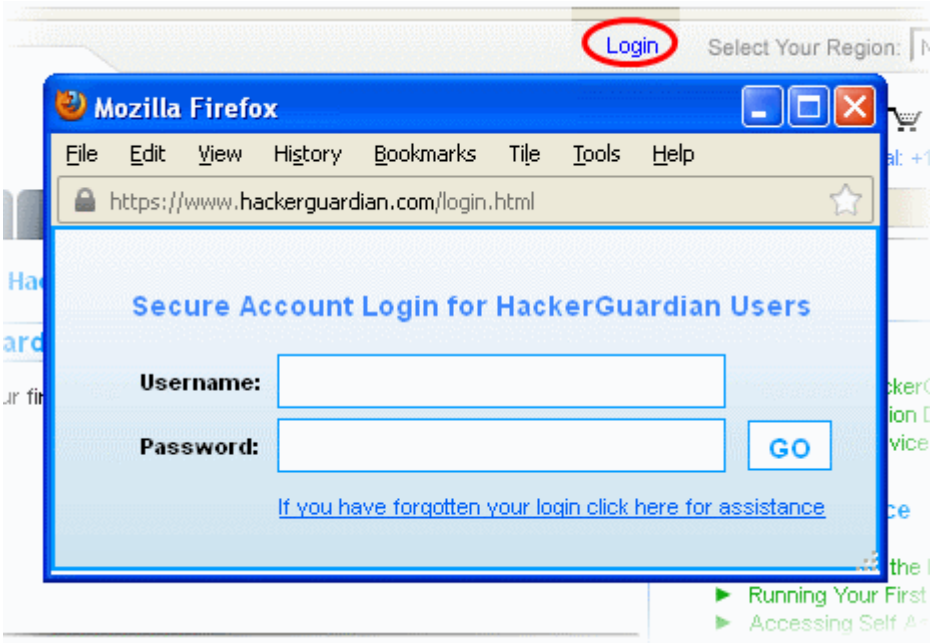
The Account Status Information Area displays the number of scans and IPs/Domains that remain on the license. It also allows the administrator to purchase additional IPs. Click here for more details.

2.1.2. Running Your First PCI Scan

Comodo HackerGuardian features a built-in Setup wizard for PCI scanning that provides the fastest and easiest way to add devices and to commence a PCI scan. The wizard is accessible from the interface after you login to your account.

1. Log in To HackerGuardian:

First step in configuring HackerGuardian PCI Scanning Service is to log into the online interface at http://www.hackerguardian.com . Enter the username and password you created during sign up in the 'Secure Account Login' box.

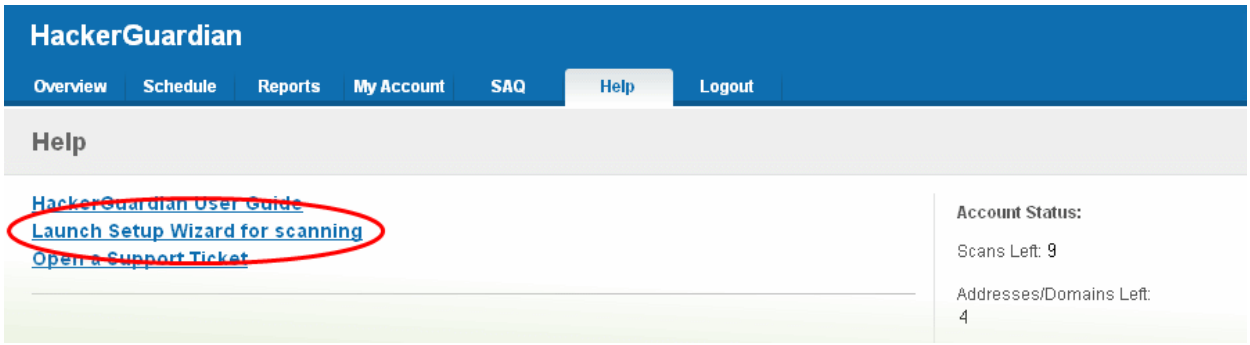


Note: During signup you created a Comodo account with a Username and Password. This Username and Password has dual functionality as it allows you to log into the HackerGuardian interface and your Comodo account. In order to log into HackerGuardian to configure the service, use the login box on **www.hackerguardian.com** (highlighted above). To login into your Comodo account, please use the login box at **www.comodo.com**.

After your username /password has been verified, you will be logged into the HackerGuardian administrators interface.

2. Launch Setup Wizard for PCI Scanning

Click the 'Help' tab from the Navigation bar to access the 'Help area'...

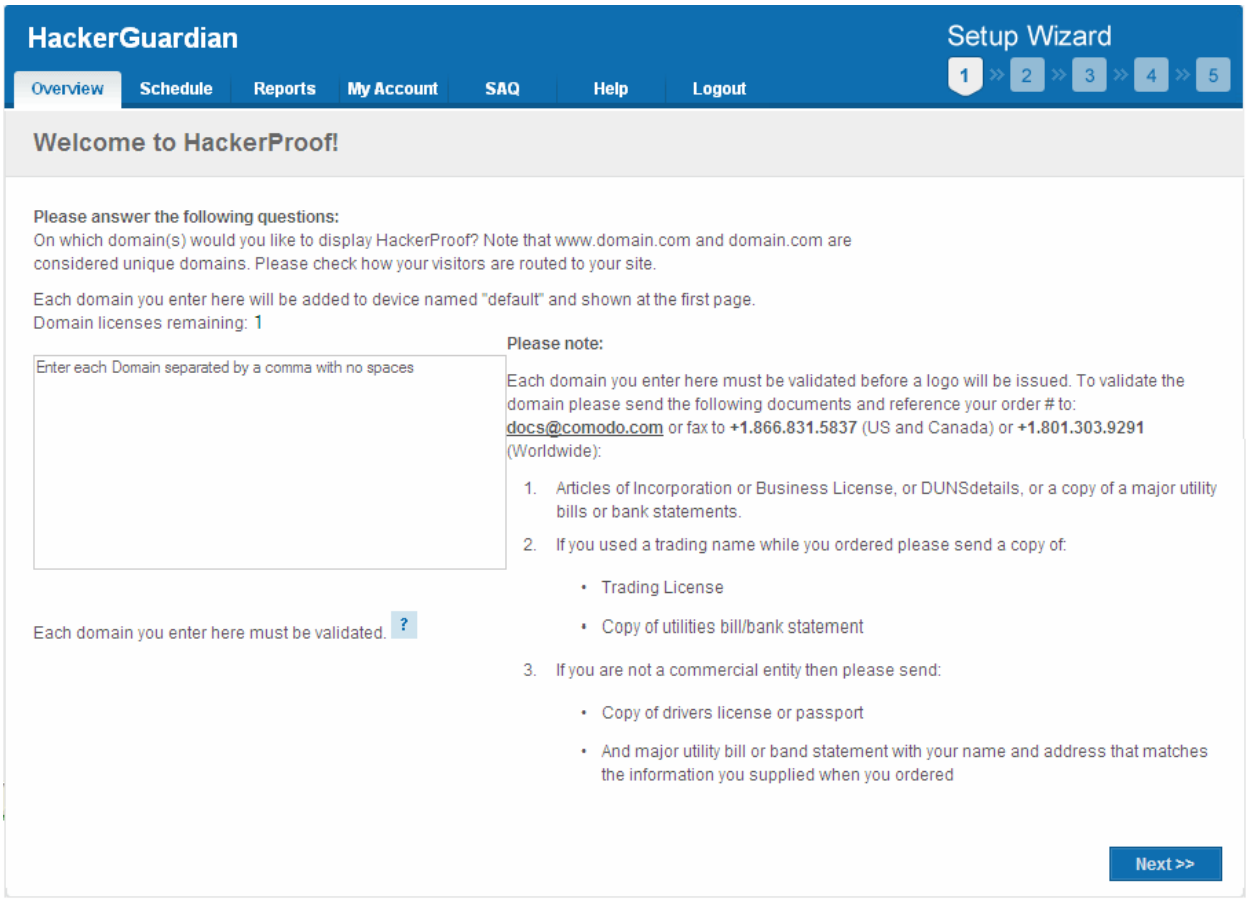


...and then click the link 'Launch Setup Wizard for scanning'. The wizard allows you to configure and start the scan in just five simple steps.

Step 1 - Enter the name of domain to be scanned

Note: This step applies only to HackerProof setup and will be visible only if you have a HackerProof License. If you do not have a HackerProof license, this step will be skipped and the wizard automatically starts from '**Step 2 - Add Device to Scan**' .

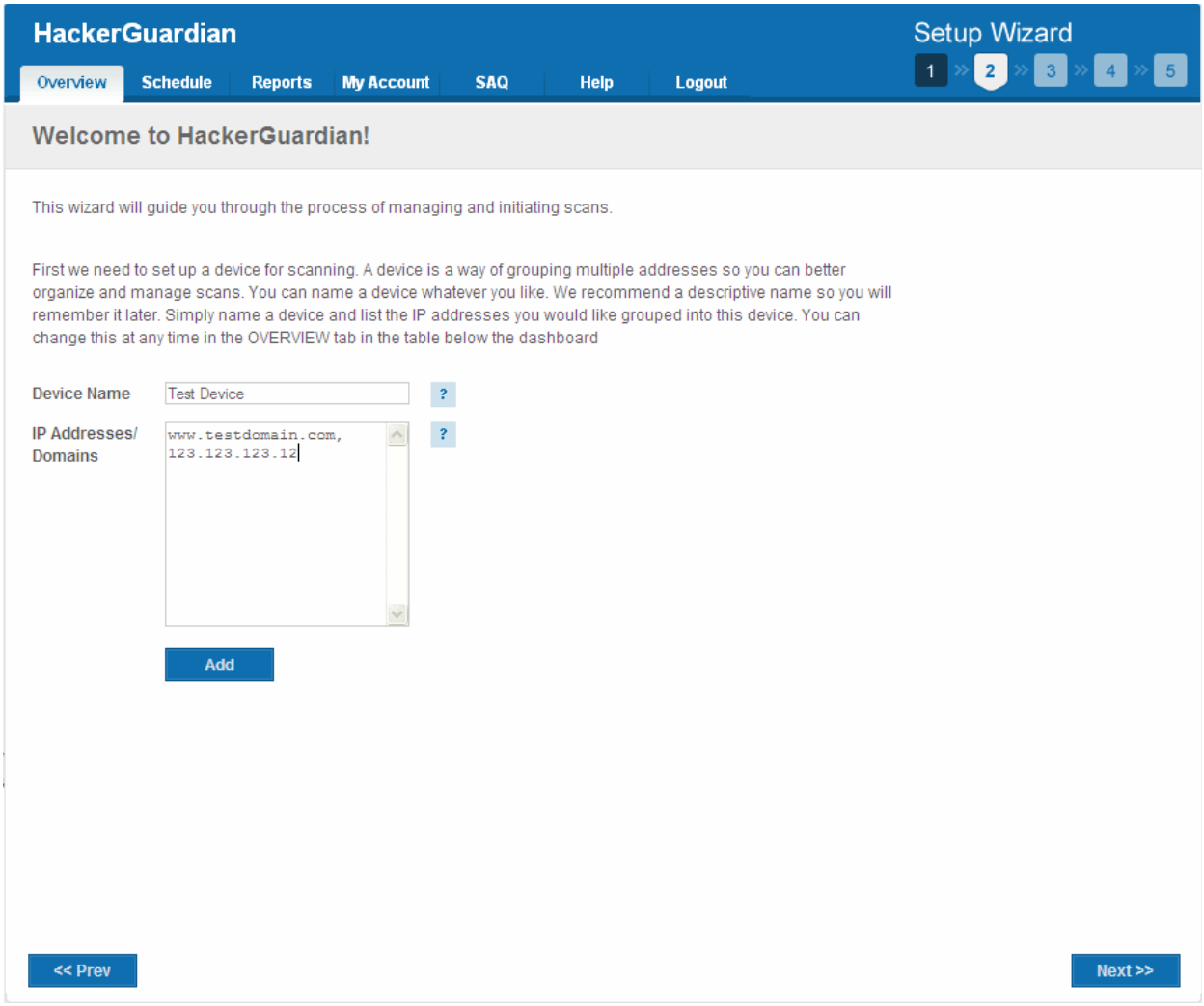
If you do not wish to setup a HackerProof scan at this point then you can ignore this step and skip straight to '**Step 2 - Add Device to Scan**' by clicking the 'Next' button.



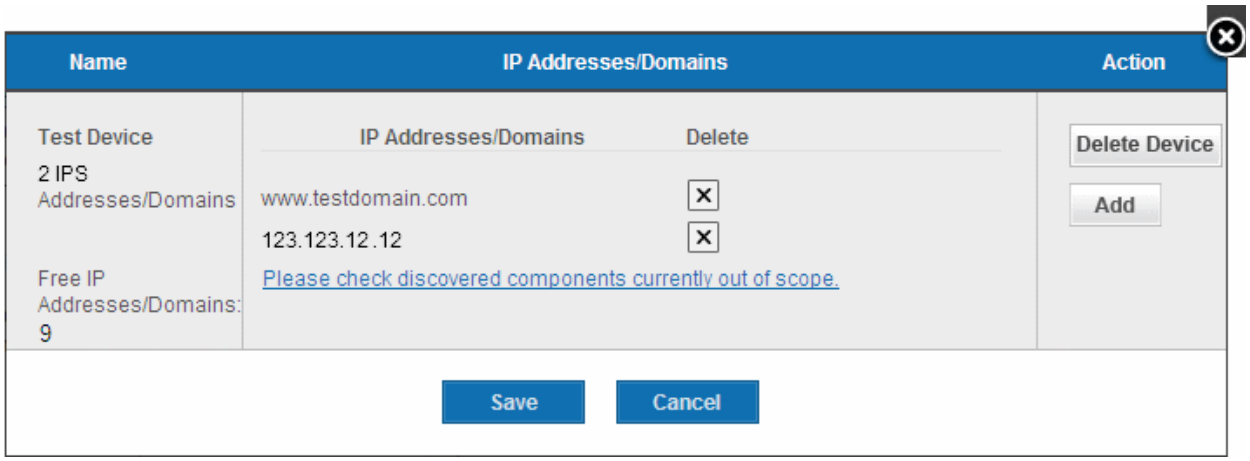
Step 2 - Add Device to Scan

In order to run a PCI (or HackerProof) scan, you must first create a **Device**.

A HackerGuardian 'Device' is an umbrella term that describes a grouping of IP addresses and/or domains that are to be used as the target for a PCI, HackerProof or SiteInspector scan. HackerGuardian 'Devices' can be used to 'mirror' a real life device. For example, a single machine in your organization's infrastructure may have multiple IP addresses (and domains) which host different services. The PCI DSS guidelines state that all these IP addresses and services must be scanned. By associating multiple IP addresses and domains to a single HackerGuardian 'Device', you can simulate your real-life device and scan it for **PCI compliance** in one pass. All customers must create a 'device' before PCI scanning can commence.



- When creating a device, HackerGuardian requires that you specify all the externally facing IP addresses/Domains belonging to your target server, host or other device.



Note: You can check for the IP addresses and the domains, which have been previously entered and deleted, or the IP Addresses that were detected through reverse lookups on the domains or common hostnames for the domains included previously, by clicking the link 'Please check discovered currently out of scope'. This helps you to identify the out of the scope components to be scanned and add to the created device.

- Click 'Save'

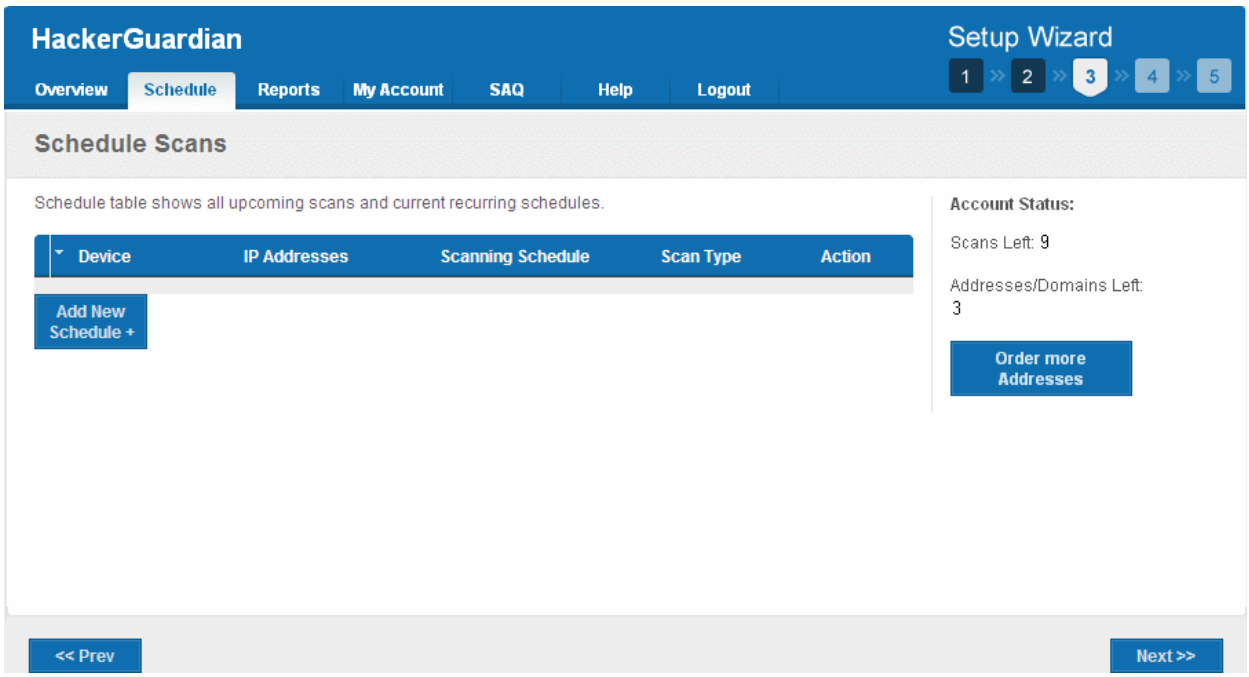
  The device will be added to your HackerGuardian account and accessible from the Overview area.

- Click 'Add' if you want to add the next device. The device will be added to your HackerGuardian account and accessible from the Overview area.
- If you have finished adding new devices, click 'Next' to continue the wizard.

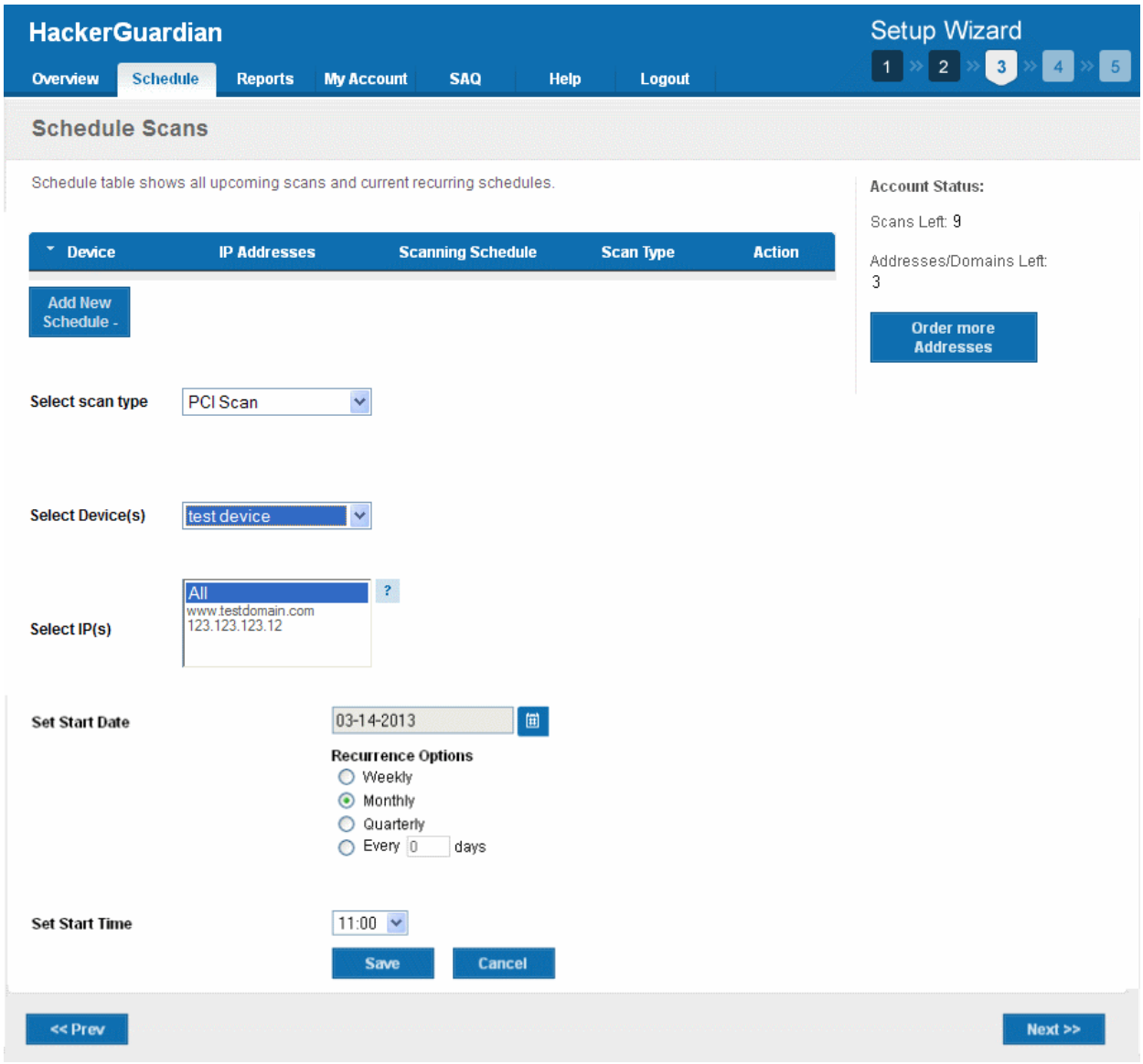
Note: You can also add new devices and edit existing devices from the Overview area of the interface. Click here for more details.

Step 3 - Schedule the PCI Scan

The next step is to schedule the scan if you wish to run the scan at a later time or periodically. This is optional. If you do not want to schedule the scan and want to run the scan instantly, just click 'Next' button to skip this step and go to Step 4.



If you want to schedule the scan, click 'Add New Schedule +' button.

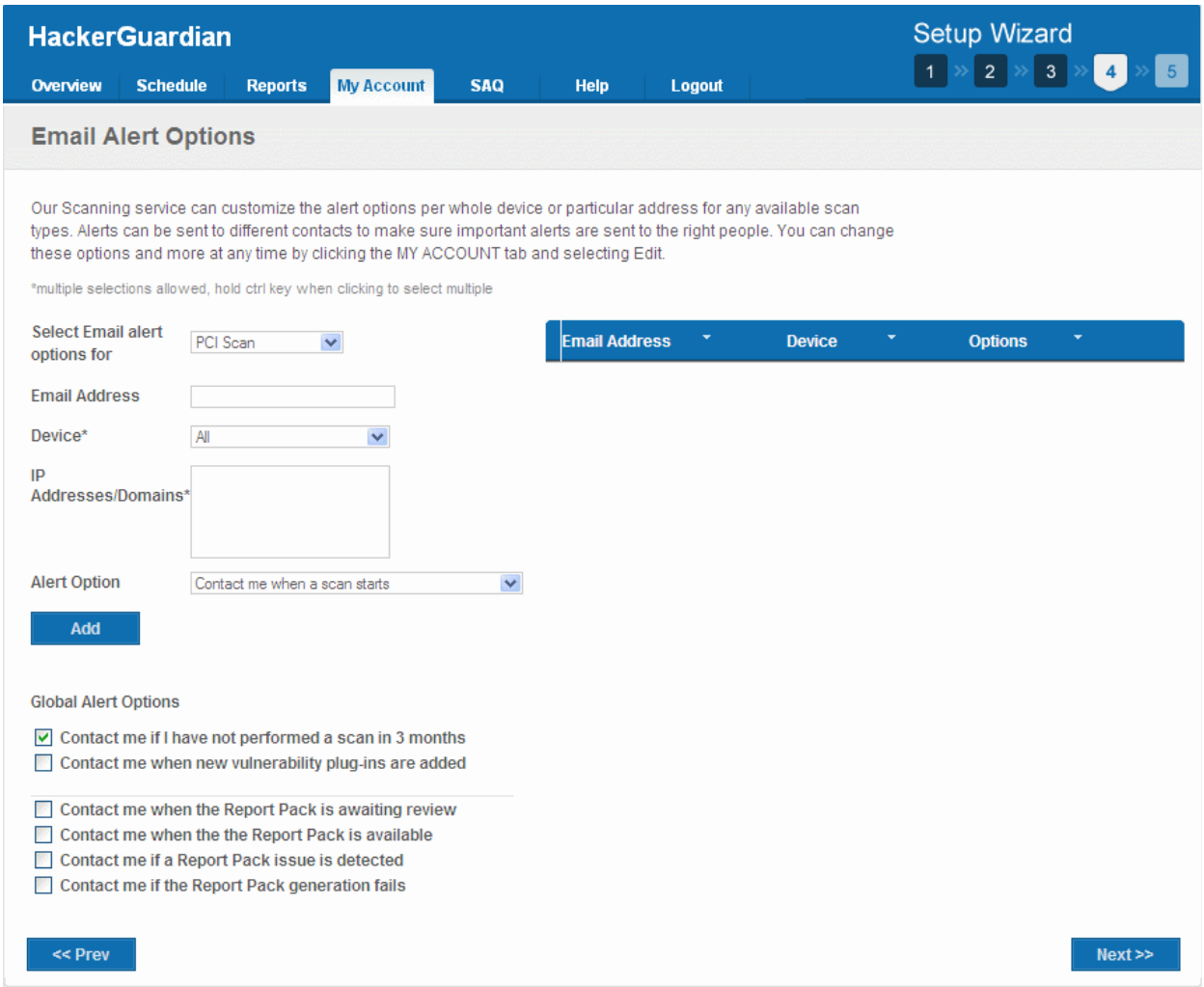


1. Select the device on which you wish to schedule the scan from Select Device(s) drop-down box.
2. Select the IPs/Domain pertaining to the selected device from Select IP(s) box. If you wish to scan all the IPs/Domains, select 'All'.
3. Select the start date for the scan schedule by clicking the calendar icon beside 'Set Start Date' text box.
4. Select the recurrence period.
    - Daily - The scan will be performed once per day on the specified time.
    - Weekly - The scan will be performed once in a week on the specified day and time.
    - Monthly - The scan will be performed once in a month on the specified date and time.
    - Quarterly - The scan will be performed once in three months on the specified date and time.
    - Every N days - Scan will be performed once for every n days from the start date. For example, if you specified 2 then the scan will be performed on alternate days.
5. Select the start time from the 'Set Start Time' drop-down combo box and select your time zone from the Time Zone drop-down box. The scan will be started on the set time at the scheduled dates according to your time zone.
6. Click 'Save' to to apply your schedule.
7. Click 'Next' to continue the wizard.

Note: You can always view/modify/delete the schedules from the Scheduled Scans area of HackerGaurdian interface. Click here for more details.

Step 4 - Configure PCI Scan Email Alert Options

HackerGuardian sends automated email notifications to administrators on events like commencement of manual/scheduled scans, results of scan and failure of scans. You can set your preferences for receiving the emails as you wish. If you do not want to have email alerts at this moment, Click 'Next' to go to Step 5. You can configure the alert notifications later by accessing the My Account area.



1. Select the Email Alert Options as given in the table below:

Form Element	Description
Select Email alert options for	Select the option 'PCI Scan' from the drop-down
Email Address	Enter the email address to which you wish to receive the scan alert message in the text box below 'Email Address'. This address can be different from the Account Email and can belong to the administrator for the specific device/domain.
Device	Select the Device for which you wish to receive the scan alert message from the drop-down box below 'Device'. If you wish to have the alert message for all the devices, select 'All'.
IP	Select the IPs/Domains pertaining to the device selected, for which you wish to receive the scan alert

Addresses/Domains	message from the text box below 'IP Addresses'. If you wish to have the alert message for all the IPs/Domains, select 'All'.
Alert Option	Select the event for which you wish to have email notification from the drop-down box below 'Options'.

2. Select the Global Alert Options

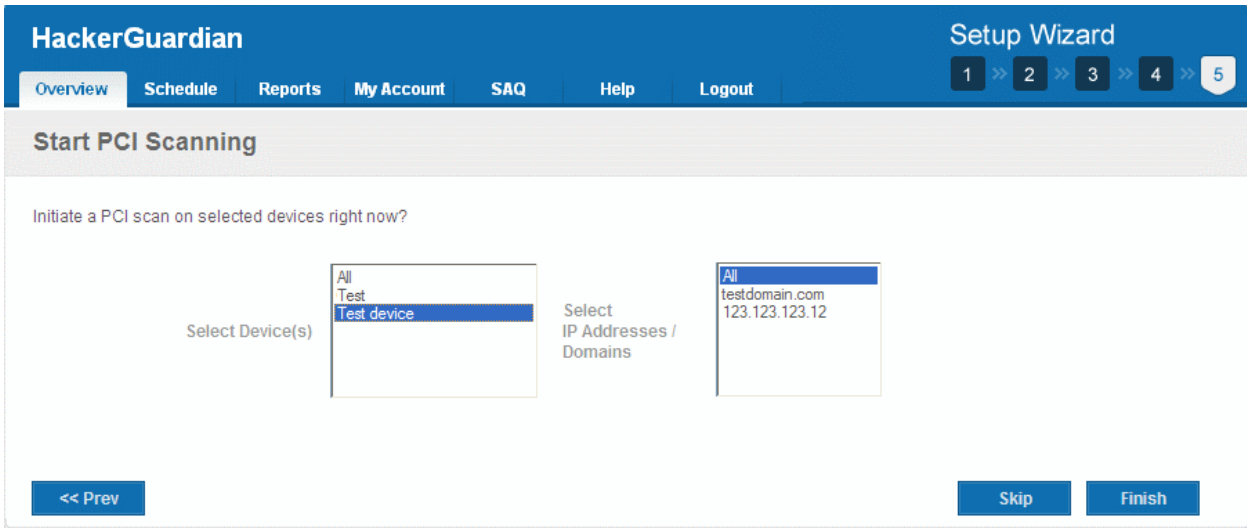
- **Contact me if I have not performed a scan in 3 months** - Selecting this option instructs HackerGuardian to send a remainder message for an on-demand scan to the Account Email address if the administrator has missed to perform a scan for three months.
- **Contact me when new vulnerability plug-in are added** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever a new vulnerability plug-in is added to HackerGuardian, enabling the Administrator to deploy the plug-in in future scans.
- **Contact me when the Report Pack is awaiting review** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report is under review by a PCI DSS approved staff of Comodo. The Report will be available for download upon completion of the Review and approval by the Comodo staff. Refer to **Downloading Report Pack** for more details.
- **Contact me when the Report Pack is available** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report is ready for download after review by a PCI DSS approved staff of Comodo. Refer to **Downloading Report Pack** for more details.
- **Contact me if a Report Pack issue is detected** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area, Report has been reviewed by a PCI DSS approved staff of Comodo and an issue has been detected in the generated report. Refer to **Downloading Report Pack** for more details.
- **Contact me if a Report Pack generation fails** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report generation has failed for some reasons. Refer to **Downloading Report Pack** for more details.

3. Click 'Add' if you want to configure email settings more devices/events.
4. Click 'Next' to continue the wizard.

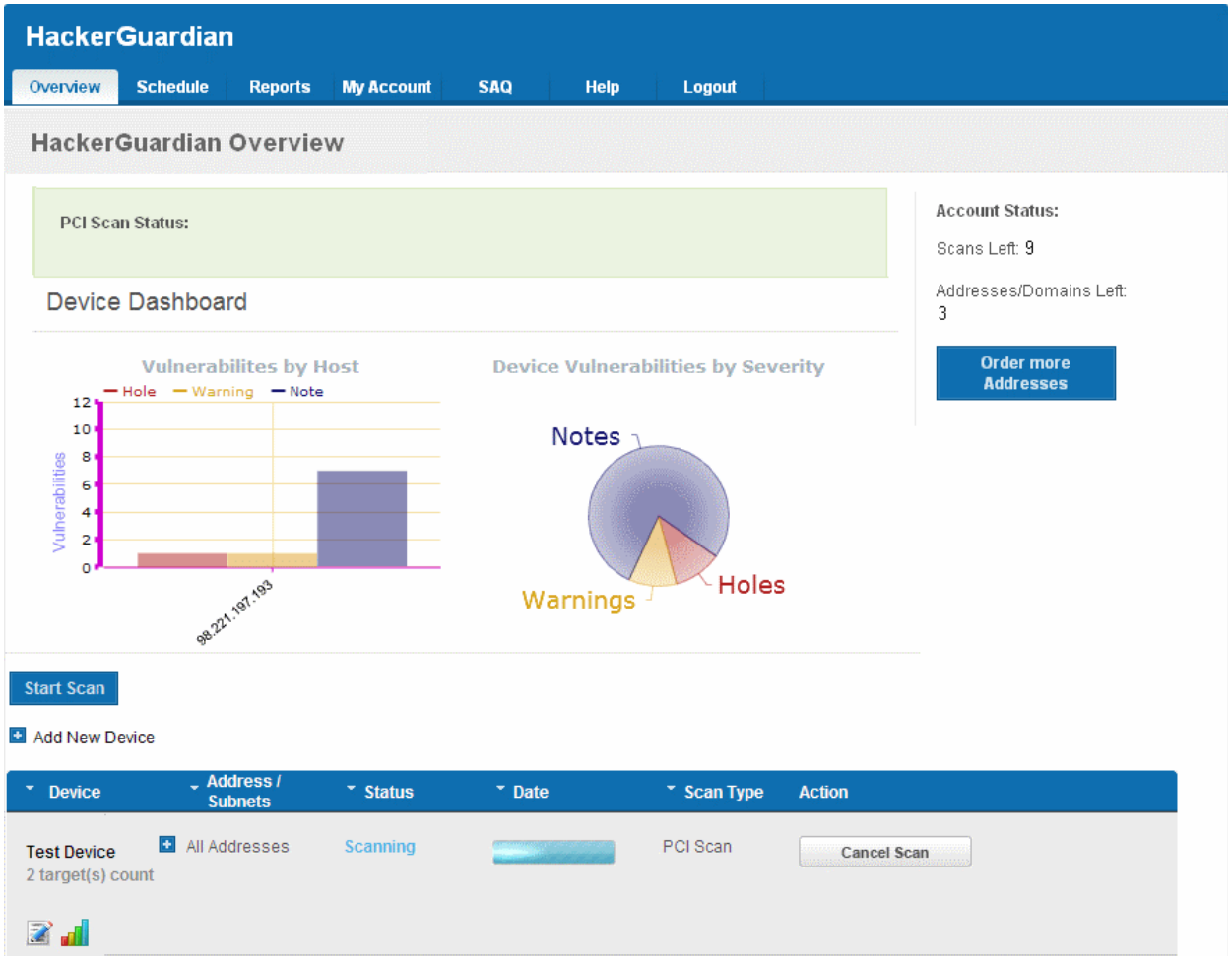
Note: You can always view/modify the email alert options from the My Account area of HackerGaurdian interface. **Click here for more details**.

Step 5 - Start PCI Scanning

The next step is to commence the PCI scan on a device.



1. Select the device on which you wish to commence the scan from the 'Select Device(s)' box. If you want to run the scan for all the devices at once, select 'All'.
2. Select the IPs/Domains in the next box. If you want to run the scan for all the IPs/Domains associated with the selected device at once, select 'All'.
3. Click Finish to commence the scan. The scan will be initiated and you can see the progress in the 'Overview' area.



Note: You can also start scanning on any existing device from the 'Overview' area of the interface. Click here for more details.

2.1.3. Viewing Executive Report, Charts and Vulnerability Reports

- To view the Executive scan Report, click the Executive Report button beside the device name.
- To view the Charts page that contains at-a-glance summary of the scan results on the device and graphical representations of proportions of identified vulnerabilities according to their categories , click the charts page button  in the row of the Device.
- To view the Vulnerability Report, click the Vulnerability Report button beside the IP/domain name from the list of IPs/domain names displayed by clicking the '+' button beside the Device name.

The Administrator can also download a Report Pack containing the pdf files of the reports for submitting to the acquiring bank from the Reports area, after a successful scan. Refer to HackerGuardian Reports for more details.

2.1.4. Accessing the Self Assessment Questionnaire

The PCI Data Security Standard Self Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

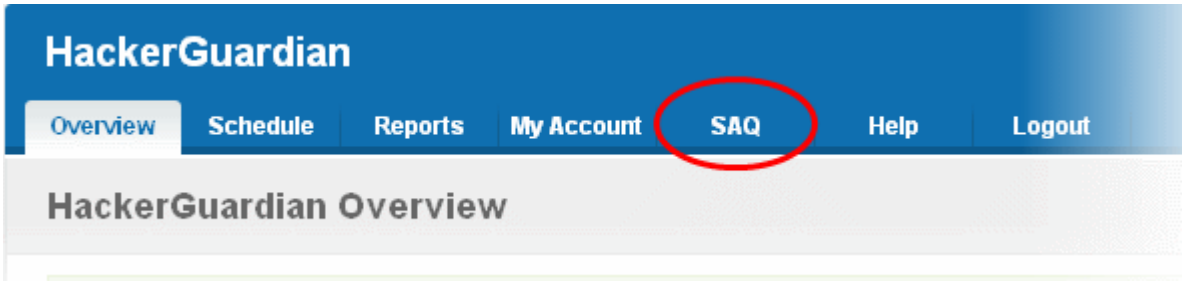
Comodo has simplified this often confusing process with the HackerGuardian PCI Compliance Wizard - an intuitive web-based application guides merchants through every step of the PCI Self Assessment Questionnaire. Each question is accompanied by expert advice to help the merchant interpret and appropriately answer each question. At the end of the wizard you will find out immediately whether or not your answers qualify your organization as PCI compliant.

The wizard will provide:

- A Questionnaire Summary - Listing security control areas on which you failed compliance
- A custom 'Remediation Plan' for your company containing:
  - A comprehensive list of remedial actions that you need to take to attain full PCI compliance
  - A remediation planning tool enabling task prioritization and project management
  - Links to recommended products and services that will help you cost-effectively resolve non-compliant areas
- A 'ready-to-submit' PCI DSS Self Assessment Questionnaire

To access the wizard

- Click the SAQ tab in the Navigation bar of the HackerGuardian interface.

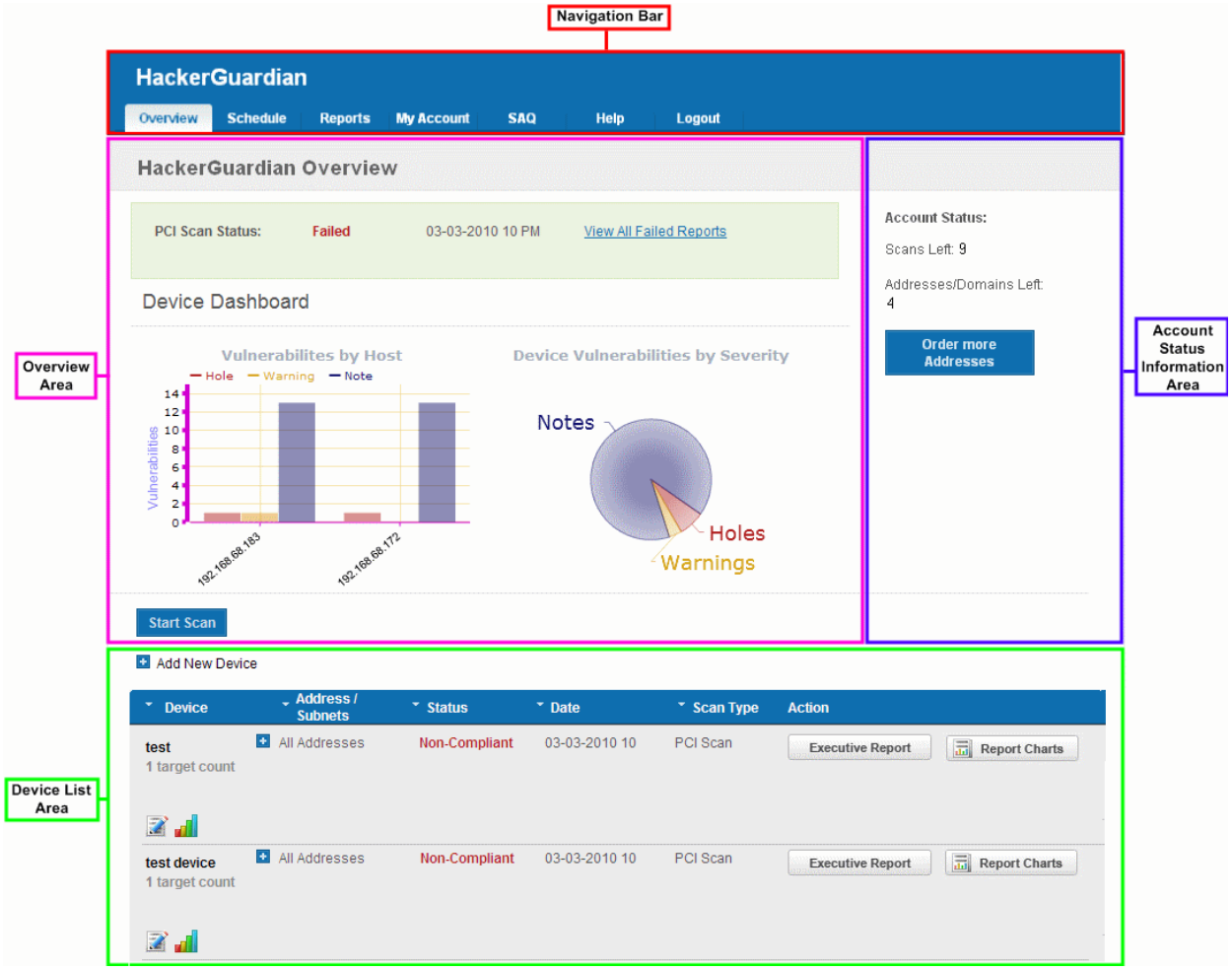


The wizard is a four-step process, where you have to register, select the SAQ type and complete the questionnaire. The final step provides the summary of SAQ.

Your progress is automatically saved after each question - allowing you to log out and return at a later date to complete the questionnaire. Your free account and responses are retained, giving you an opportunity to revise and modify any of your answers. This also allows you to update, schedule and track the progress of outstanding remediation tasks.

2.2. PCI Scanning Service - Infrastructure

The streamlined web-based main management interface provides easy access to all the functions of HackerGuardian. The navigation bar at the top has tabs to access different functional areas to add new devices, initiate scans, view reports, schedule scans, modify your account and scan settings etc. in simple steps. The account status displayed in the right pane informs your remaining scans, remaining IPs/Domains that you deserve and also enables you to purchase the service for more IP's and Domains.



2.2.1. Navigation Bar

- **Overview** - Displays the Overview area that provides the administrator with a report summary of last scan and serves as a launchpad for starting scans and the 'Device List area' that allows the administrator to add, edit and configure target devices; view scan reports.
- **Schedule** - Displays a list of existing scans, allows to add new schedule of scanning.
- **Reports** - Enables the administrator to view the summary and complete scan reports.
- **My Account** - Enables the administrator to configure account settings, view license, scan options and to choose which plug-ins are to be deployed during a scan.
- **SAQ** - Allows the administrator to access the Self Assessment Questionnaire (SAQ) for their self-evaluation on compliance with the Payment Card Industry Data Security Standard (PCI DSS)
- Help - Contains links to the download user guide and to the Comodo knowledgebase. Also enables the

administrator to launch a simple setup wizard for PCI Scanning.

2.2.2. Overview Area

The 'Overview' area displays the status of the HackerProof and PCI Scans and a dashboard summary of the scan reports from last performed scan on the device selected from the 'Device List' area. Click here for more details.

2.2.3. Device List Area

The Device List area displays a list of devices added to HackerGuardian and provides an at-a-glance summary of the status of each device. This area also allows the administrators to create a new device, edit a device, add IP's to a device and open device reports. Click here for more details.

2.2.4. Account Status Information Area

The Account Status Information Area displays the number of scans and IPs/Domains that remain on the license. It also allows the administrator to purchase additional IPs. Click here for more details.

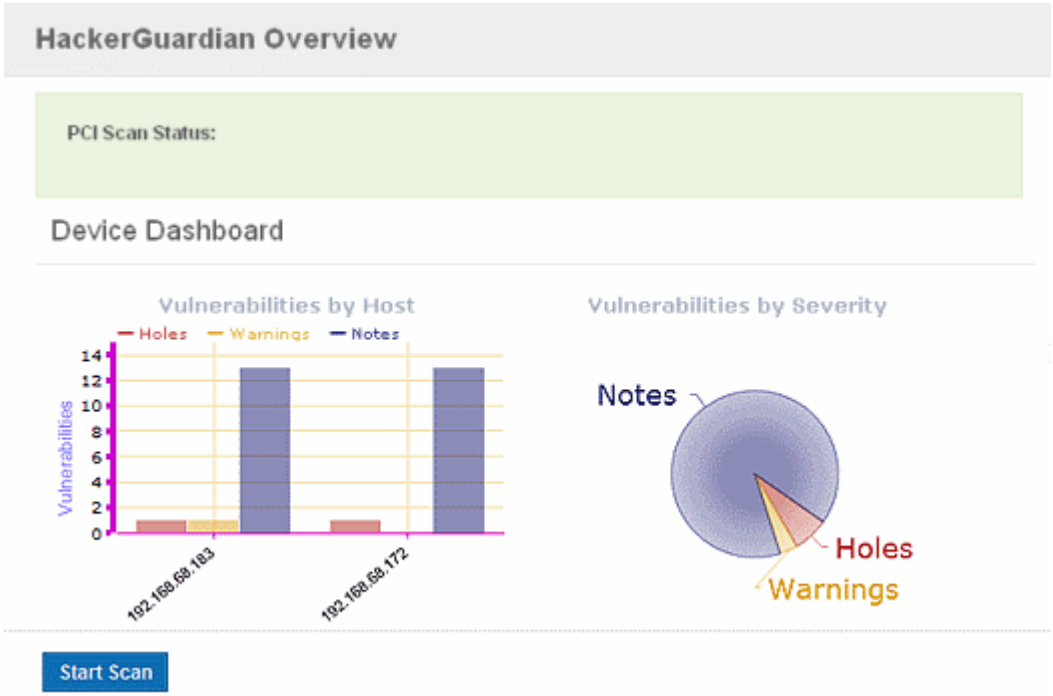
2.3. PCI Scan

Once you login to your account, the main configuration area of the HackerGardian interface is displayed. It contains two areas namely:

- Overview
- List of Devices

2.3.1. Overview

The 'Overview' area displays the status of the last run HackerProof and PCI Scans and a dashboard summary of the scan reports from the last scan performed on the device selected from the device list area.



Vulnerabilities by Host - A graphical representation of the information regarding the security holes found, security warnings, and security notes per host. Each category is represented by a different color. Pointing the mouse cursor over a bar in the graph displays the count of the respective item found.

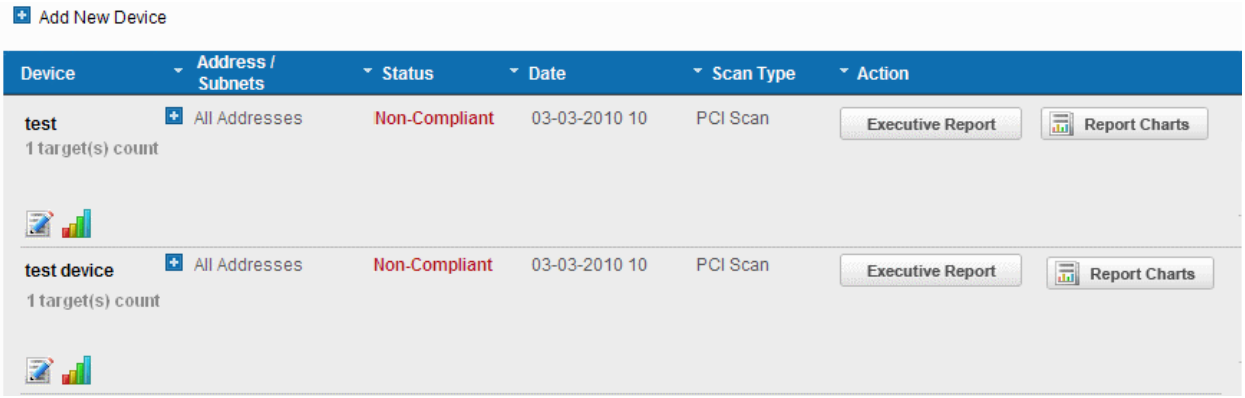
Vulnerabilities by Severity - A pie-diagram representation of information regarding the security holes, security warnings, and security notes found. Pointing the mouse cursor over a sector in the diagram displays the percentage proportion of the respective item found.

Definitions of Terms

Term	Description
Holes	A vulnerability, whose severity level according to PCI Severity Rating, is more than three or 'High', is identified as a Security Hole by HackerGuardian. To pass a PCI Compliance scan, no holes are to be found during the scan. If any holes are found, the merchant or the service provider must re mediate the identified problems and re-run the scan until the compliance is achieved. Click here for more details.
Warnings	A vulnerability, whose severity level, is more two or 'Medium', is indicated as a Security Warning by HackerGuardian. To pass a PCI Compliance scan, no warnings are to be found during the scan. If any warnings are found, the merchant or the service provider must re mediate the identified problems and re-run the scan until the compliance is achieved. Click here for more details.
Notes	A vulnerability, whose severity level, is more one or 'Low', is indicated as a Security Note by HackerGuardian. Click here for more details.

2.3.2. List of Devices

The 'Device List' area displays a list of existing devices for PCI/Custom/HackerProof/SiteInspector scanning.



The following table provides description of information columns in this area.

Column	Possible Values	Description
Device	Text	Displays the device name (a friendly name which was given by administrator when creating the device) and the total number of IPs/Domains associated with the device.
Address/Subnets	Text	Displays all the associated domains (e.g. www.domain.com) or IP addresses that administrator specified for the device. Click the '+' button beside All IPs to view the list of IPs and the Domains.
Status	'Compliant'	Indicates that the device/IP/domain is PCI scan Compliant as per the last run PCI scan.
	'Non - Compliant'	Indicates that the device/IP/domain is not PCI scan Compliant as per the last run PCI scan.

	'Passed'	Indicates that the device/IP/domain has passed the last run HackerProof or SiteInspector scan
	'Failed'	Indicates that the device/IP/domain has failed the last run HackerProof or Site Inspector scan
Date	Numeric	Displays the date of last run scan for the device/IP/domain.
Scan Type	'PCI Scan'	Indicates that the device/IP/domain is PCI Scan enabled.
	'Custom Scan'	Indicates that the device/IP/domain is Custom Scan enabled.
	'HackerProof'	Indicates that the device/IP/domain is HackerProof Scan enabled.
	'Site Inspector'	Indicates that the device/IP/domain is SiteInspector Scan enabled.
Action	'Executive Report' button	Enables the Administrator to view executive scan report of the last scan run on the device. Available only for the devices and not for the individual IPs and Domains associated with the device. Click here for more details.
	Chart button	Enables the Administrator to view the Charts Page contains at-a-glance summary of the scan results on the device at the top and graphical representations of proportions of identified vulnerabilities according to their categories. Click here for more details.
	'Vulnerability Report' button	Enables the Administrator to view vulnerability report of the last run scan on the device/IP/domain. Available only for the individual IPs and Domains associated with a device. Click here for more details.
	Retest	Enables the Administrator to re-run the scan on the device/IP/domain that has failed any of the scans.

Note: Clicking on the up or down arrows beside each column heading sorts the list of devices in ascending order based on the category.

From this area, you can:

- Create new device to enable PCI scanning;
- Manage existing devices;
- View a dashboard summary of scan results from a specific device
- View Executive Summary and Vulnerability Reports after running an on-demand scan.

2.3.3. Devices

In order to run a PCI (or HackerProof/SiteInspector) scan, the administrator must first create a Device.

A HackerGuardian 'Device' is an umbrella term that describes a grouping of IP addresses and/or domains that are to be used as the target for a PCI, Custom, HackerProof or SiteInspector scan. HackerGuardian 'Devices' can be used to 'mirror' a real life device. For example, a single machine in your organization's infrastructure may have multiple IP addresses (and domains) which host different services. The PCI DSS guidelines state that all these IP addresses and services must be scanned. By associating multiple IP addresses and domains to a single HackerGuardian 'Device', you can simulate your real-life device and scan it for PCI compliance in one pass. All customers must create a 'device' before PCI, HackerProof or SiteInspector scanning can commence.

- *PCI Customers*. When creating a device, HackerGuardian requires that you specify all the IP addresses belonging to your target server, host or other device.
- *HackerProof (or/and SiteInspector) Customers*. When creating a HackerGuardian device you need to specify the domain name of the website which you would like to display the HackerProof logo on.

Once a PCI device has been created, it will become available for selection in the 'Device List' area.

Important Notes

We recommend that you create separate devices for each type of scan. I.e. separate devices for HackerProof and PCI scans. You can use the same domains/IP addresses across multiple devices.

If you create PCI only devices (only PCI compliance scans will be run for these device):

- You must have at least one PCI scan compliancy license;
- You can add and scan as many IP's as allowed by your PCI license. (These IP's can be spread across as many devices as required.)
- At least one IP address or at least one domain name that you wish to scan for PCI compliancy has been added to the device. If you only specify a domain name then the PCI scan will actually take place on the IP address that this domain resolves to.
- IP address do not need validation. PCI compliance scans on IP's can begin immediately.

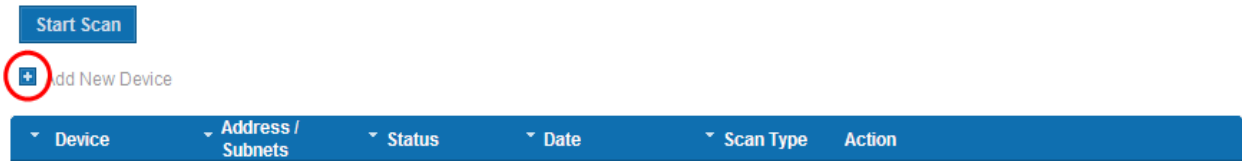
If you create PCI + HackerProof Devices (both daily and PCI compliance scans will be run for these devices):

- You must have at least one PCI scan compliancy license and HackerProof (daily) scan license.
- At least one domain that you wish to be daily and PCI scanned must be added to a PCI + HackerProof device (but the actual scans will take place on the IP address that this domain resolves to).
  The IP address that the domain resolves to will be scanned daily and, if pass, they receive the HackerProof trustmark for the domain.
- You can optionally add more IP addresses to this device.

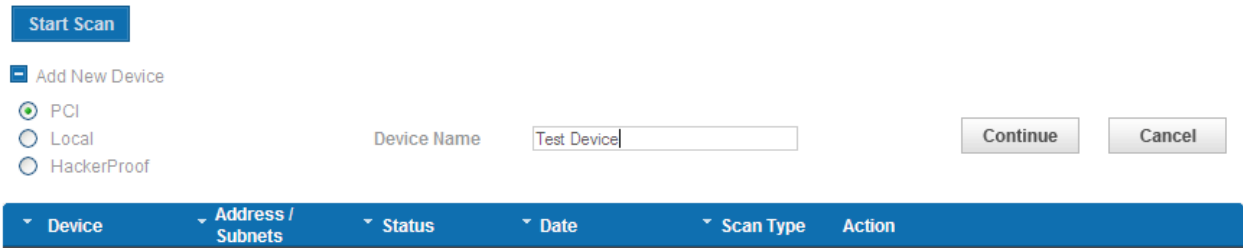
  The additional IP address(es) that were added by user can be scanned for PCI compliance. To gain PCI compliance for this device, all IP addresses must pass the PCI compliance scan.
- A device only associated with an IP cannot be daily scanned and gain HackerProof status.
- Domain ownership must be validated by Comodo before scanning is allowed to commence.

2.3.4. How to Create a New Device

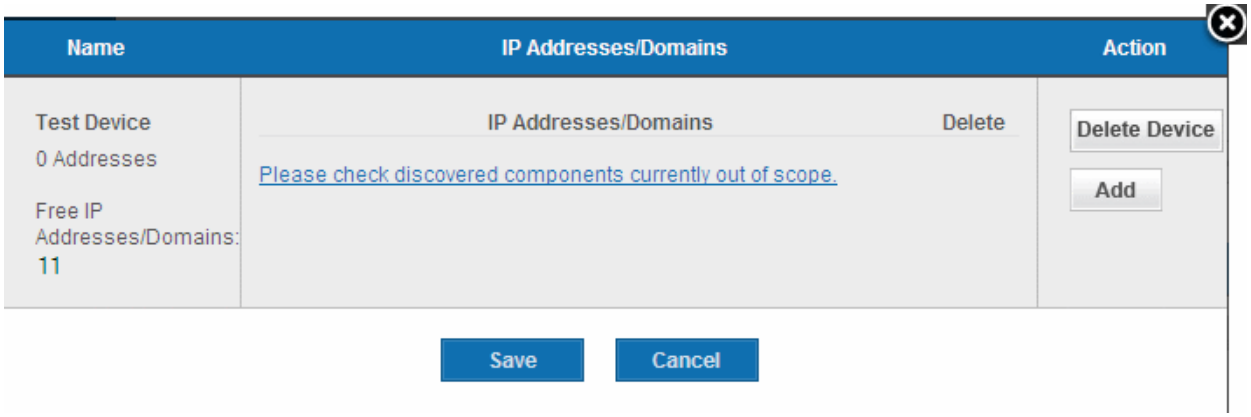
1. Switch to 'Device List' area of the interface.
2. Click on '+' button beside 'Add New Device' in the 'Device List' area (as shown below).



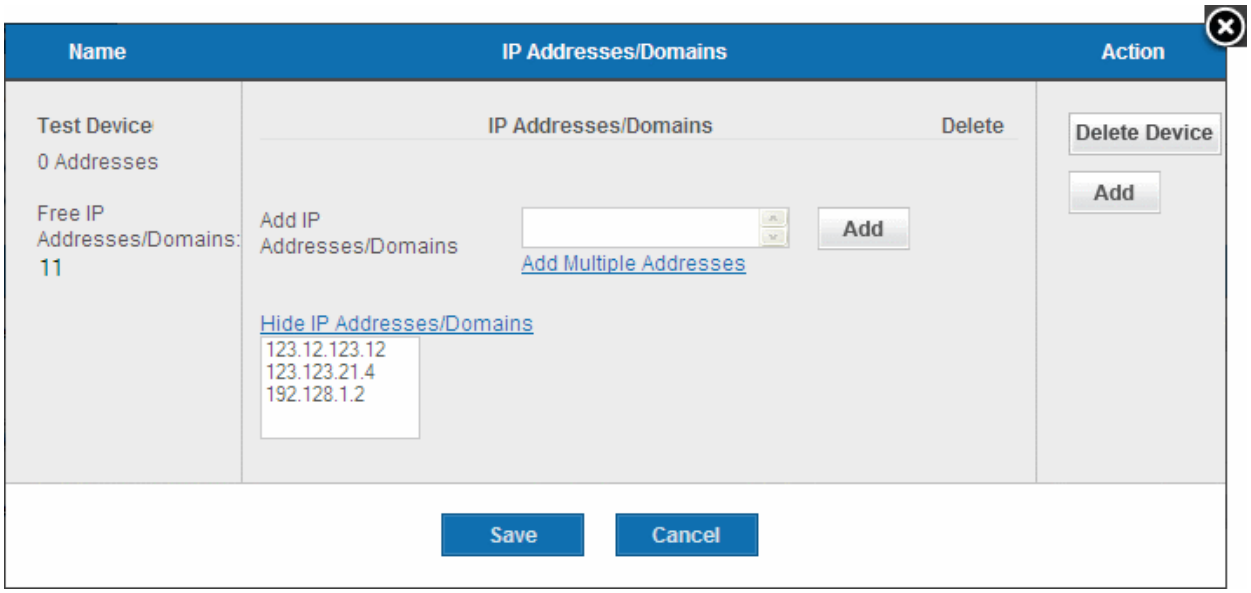
3. Select the PCI device radio button to enable PCI scanning on the device
4. Enter a friendly name for the device in the 'Device Name' text box and click 'Continue'.



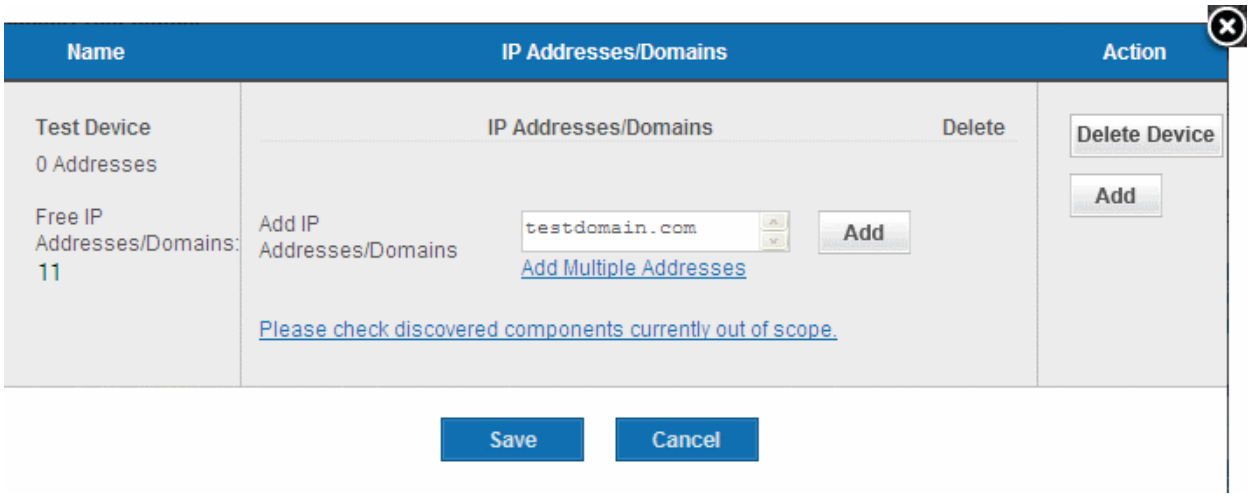
5. Click 'Add' in the next screen.



6. Enter the Domain name(s) or IP addresses to be associated with the device in the 'Add IPs or Domains' text box. You can add as many IP addresses as allowed by your PCI license. If you want to add more than one IP or domain, click on the link Add Multiple Addresses and enter the IPs/domains separated by commas.



Note: You can check for the IP addresses and the domains, which have been previously entered and deleted, or the IP Addresses that were detected through reverse lookups on the domains or common hostnames for the domains included previously, by clicking the link 'Please check discovered currently out of scope'. This helps you to identify the out of the scope components to be scanned and add to the created device.

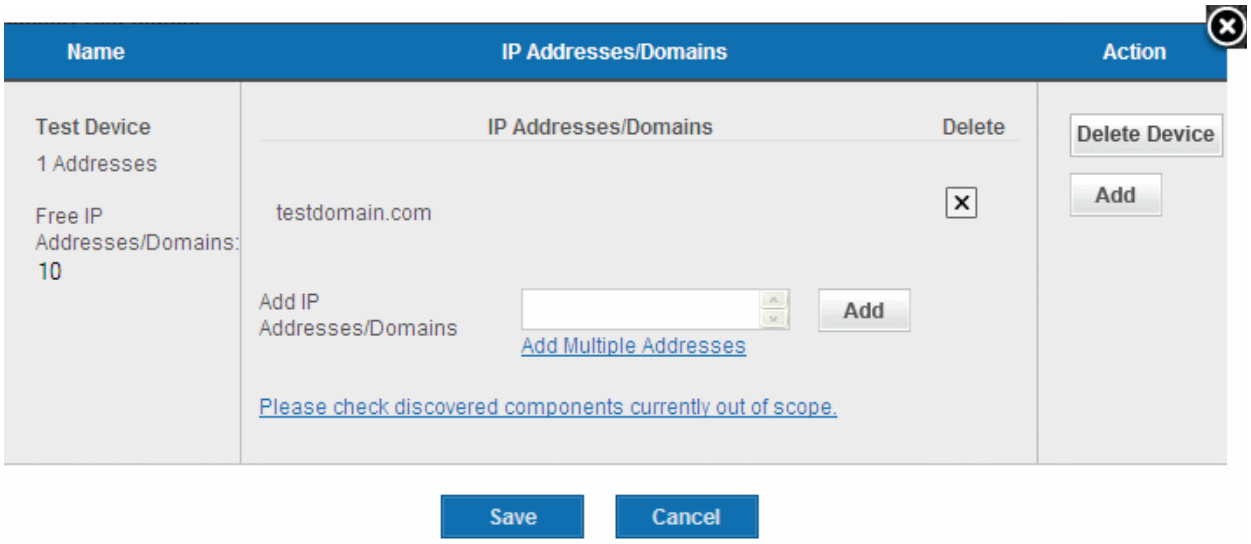


Note: You must enter external IP addresses in these fields. HackerGuardian will not run PCI scan on private IP addresses that refer to machines internal to your network.

Private IPs ranges are defined by RFC 1918 as:

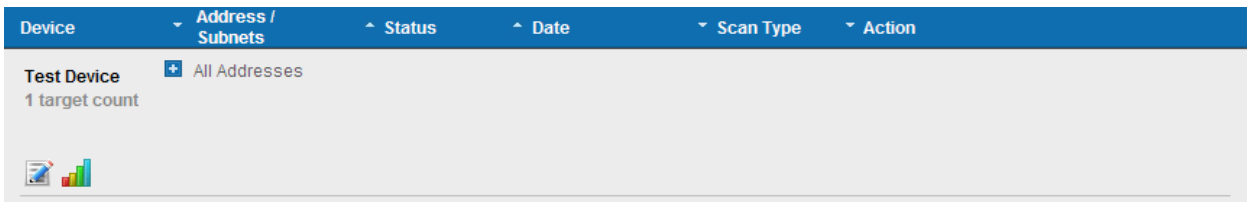
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192/168/16 prefix)

7. Click the 'Add' button beside the text box.



8. The IP(s)/Domain(s) will be added to the device. If you want to add more IPs or Domains, repeat from Step 6.
9. After adding required IPs and Domains to the Device, Click 'Save'.

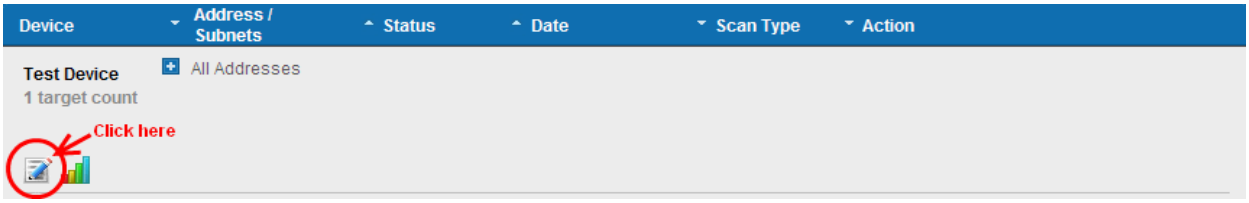
The device will be added to your HackerGuardian Account. The device will be validated for PCI compliance on your first on-demand scan and the status will be updated accordingly.



2.3.5. Devices Management

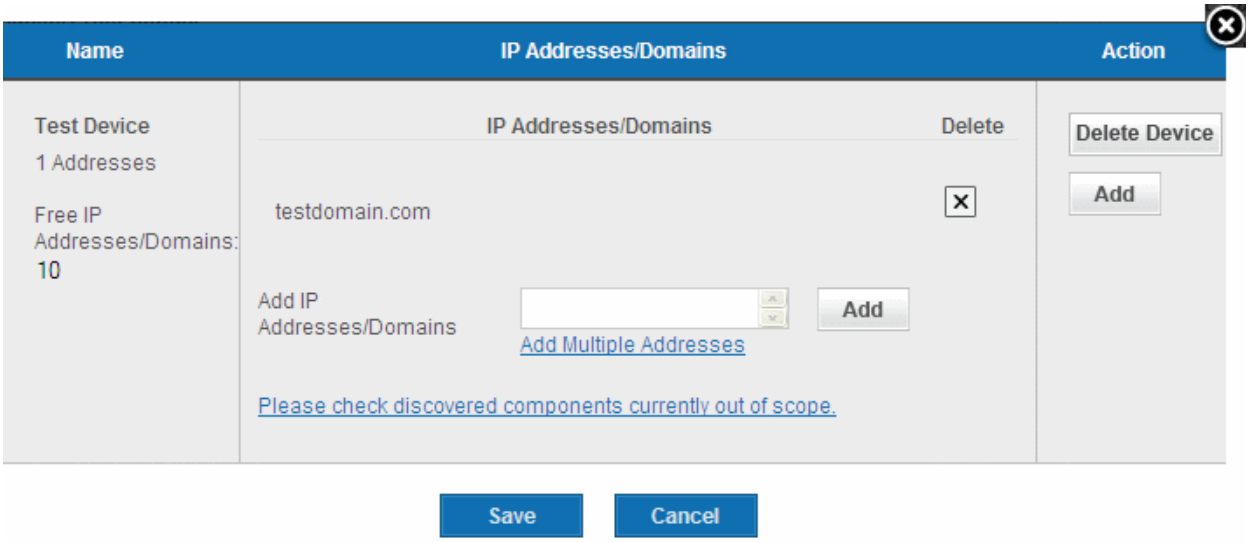
The 'Device List' area of the HackerGuardian interface displays all devices that have been created in this account. From here the administrator can edit device details, delete a device, move a domain to another device or remove a domain from a device.

To access the interface for device management, click the edit button beneath the device as shown below.



2.3.5.1. Adding Additional IPs/Domains

1. Open Edit Interface as explained above.



2. Enter the Domain name(s) or IP addresses in the 'Add IPs or Domains' text box and click Add button beside the textbox.
3. Click Save.

2.3.5.2. Removing a IP/Domain from a Device

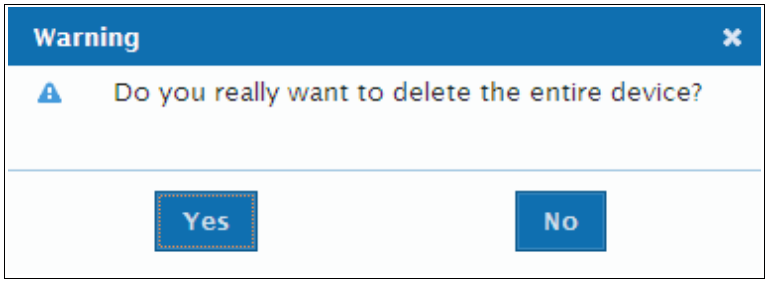
1. Open Edit Interface as explained above.
2. Click the 'X' button beside the IP/Domain name and click 'Save'.

2.3.5.3. Moving IP/Domain to Another Device

- Remove the IP/Domain from the device in which it is existing and add it to the destination device.

2.3.5.4. Removing a Device

1. Open Edit Interface as explained above.
2. Click the 'Delete Device' button and click 'Yes' in the confirmation dialog.



2.3.6. Start Scanning

Once the device is added, you can scan the target device.

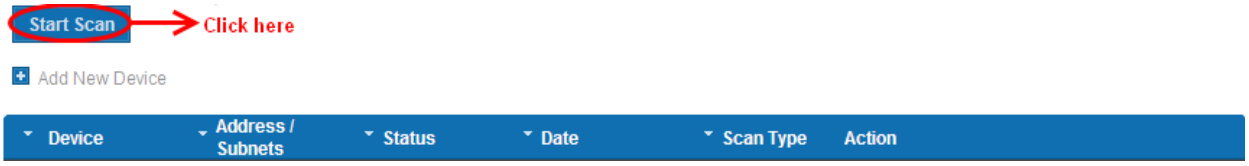
Note: The IP addresses that HackerGuardian scans originate from are:

- 99.66.200.32/28 (which translates as 199.66.200.32 through 199.66.200.48) and
- 91.209.196.32/28 (which translates as 91.209.196.32 through 91.209.196.48).

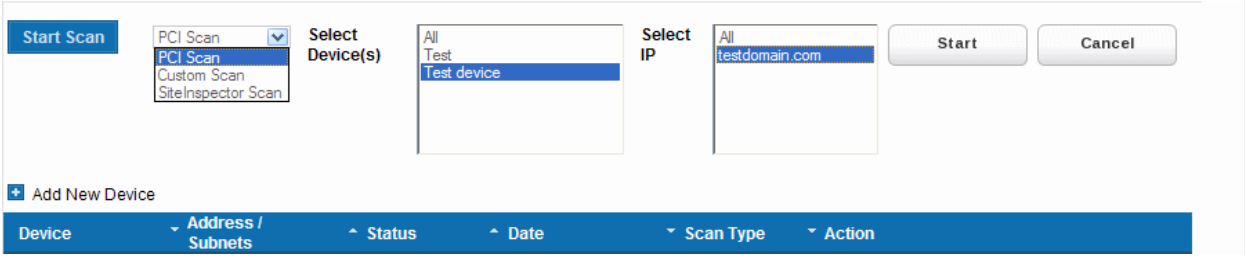
You may have to modify your firewall to allow scans from this range.

To start scanning a selected device

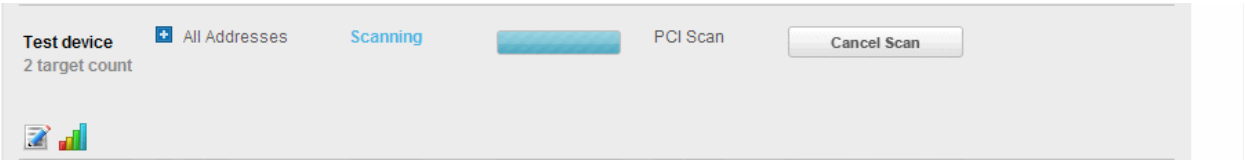
1. Click 'Start Scan' button in the upper pane of the Overview area as shown below.



The scan configuration options will be displayed.



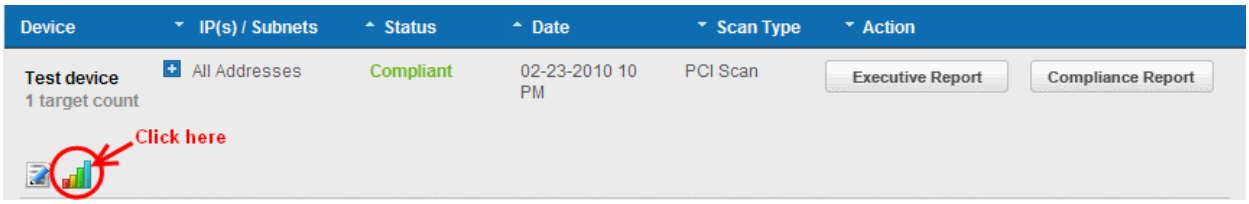
2. Select 'PCI Scan' from the scan type drop-down menu.
3. Select the device to be scanned in the next box. If you want to run the scan for all the devices at once, select 'All'.
4. Select the IPs/Domains in the next box. If you want to run the scan for all the IPs/Domains in the selected device at once, select 'All'.
5. Click 'Start'



Tip: If you want to run the scan simultaneously on multiple devices, you can start scanning on the next device by following the same procedure when the scan in running in one device. Also, you can terminate the scan at any moment by clicking 'Cancel Scan' button.

2.3.7. Viewing a dashboard summary of scan results

On completion of scan, a dashboard summary of the results will be displayed in the upper pane of the 'Overview' area. If you want to switch to the scan results of other devices, click the bar-graph button beneath the device name as shown below.



2.3.8. Viewing Executive Report, Charts and Vulnerability Reports

- To view the Executive scan Report, click the Executive Report button beside the device name.
- To view the Charts page that contains at-a-glance summary of the scan results on the device and graphical representations of proportions of identified vulnerabilities according to their categories , click the charts page button  in the row of the Device.
- To view the Vulnerability Report, click the Vulnerability Report button beside the IP/domain name from the list of IPs/domain names displayed by clicking the '+' button beside the Device name.

The Administrator can also download a Report Pack containing the pdf files of the reports for submitting to the acquiring bank from the Reports area, after a successful scan. Refer to **HackerGuardian Reports** for more details.

2.4. Internal Scanning

The Internal Scanning feature allows customers to run HackerGuardian vulnerability scans on computers located on a local area network (LAN). These computers are typically 'inside' the company's private network and are protected by a perimeter firewall or other network security device.

In order to run an internal scan, the administrator must first install and configure the HackerGuardian internal scanning Agent on the local network.

Once installed and configured, this Agent will establish a secure connection to a HackerGuardian Access server which will in turn establish a secure communication channel (connection) to a HackerGuardian scanning server. The scanning server will then be able to connect to and run scans on the local computers located at the IP addresses that have been specified as Local Devices in HackerGuardian. The Agent software is available as an iso image (to create a Live CD), as files (to create a Live USB stick) or as files to run from a VM ware player. The scans can be run directly from the 'Overview' area of HackerGuardian interface after installation and configuration of the agent. (see '**How to install the Agent**' , '**Configuring the Agent**' and '**Using the Agent - Main Menu**' for more details on set up and configuration of the agent. See '**Start Device Scanning**' to learn how to run an internal scan once the agent has been installed.)

There are two main prerequisites to running an internal scan:

- The creation of a 'Local Device' as a target for the scans in the 'Device List' area of the HackerGuardian interface. Local Devices are defined by one or more IP addresses.
- The internal scanning Agent has been installed on your local network to communicate with the HackerGuardian scanning servers via VPN connection.

Once these two steps are complete, users can start an internal scan on the device by clicking the 'Start Scan' button in the 'Overview' area.

For creating local devices and to run scans on the local devices, switch to 'Device List' area of HackerGuardian. **Click here** for more details on the interface.

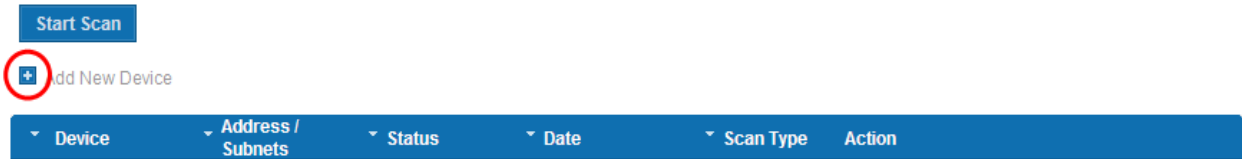
Note: The Internal Scanning feature allows you to create and edit local target devices and to manually run scans on selected devices. Unlike other, 'external', devices, 'LAN Devices' are defined using IP addresses only.

Click on the links below for detailed explanations on steps involved in the Internal Scanning.

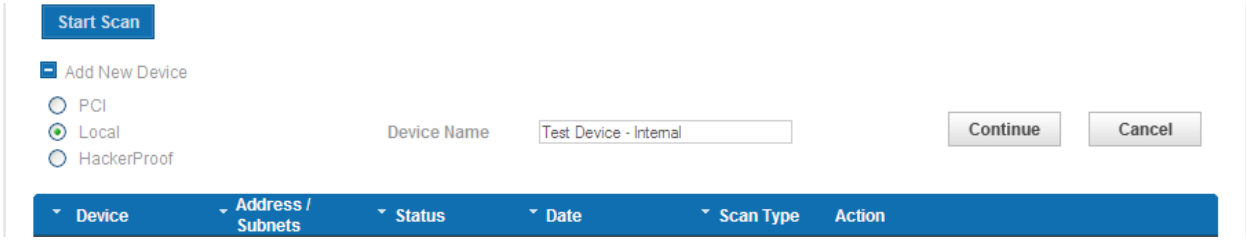
- Create new device to enable Custom (Internal) scanning;
- Manage existing devices;
- Install the Internal Scanning Agent;
- Configuring the Internal Scanning Agent;
- Start Scanning an Internal Device;
- View a dashboard summary of scan results from a specific device;
- View Executive Summary and Vulnerability Reports after running an on-demand scan.

2.4.1. How to Add a New Device

1. Switch to 'Device List' area of the interface.
2. Click on '+' button beside 'Add New Device' in the upper pane (as shown below).



3. Select the 'Local' radio button to enable internal scanning on the device



4. Enter a friendly name for the device in the 'Device Name' text box and click 'Continue'.

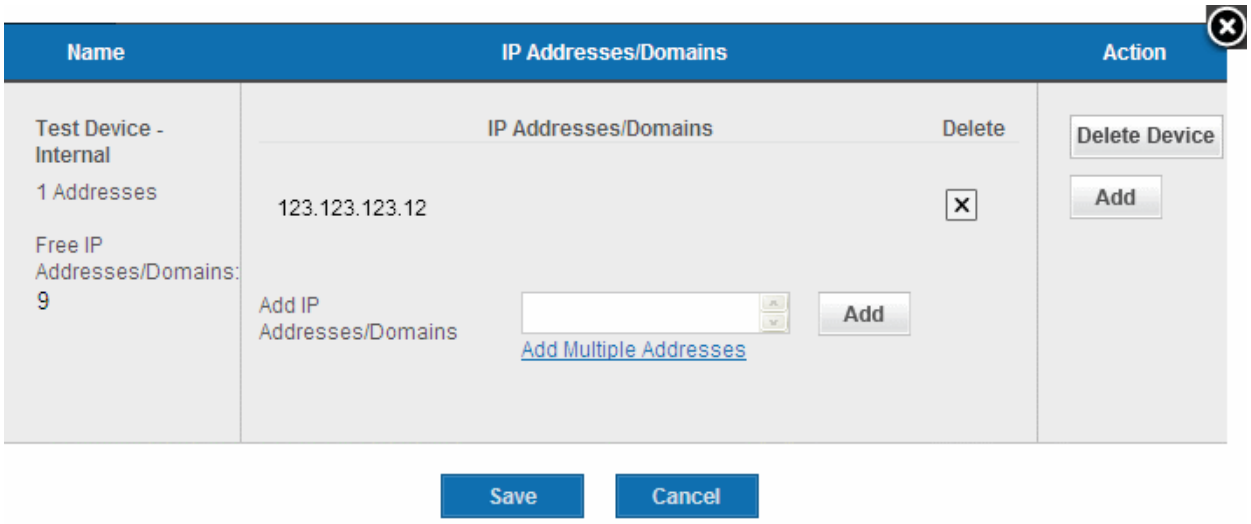
Important Note: The Device Name specified in this field must exactly match the device name that you set for the Device while installing and configuring the internal scanning agent in the local network. (see '**Configuring the Agent**' and '**Using the Agent - Main Menu**' for more details on set up and configuration of the agent.)

5. Click 'Add' in the next screen.

6. Enter the IP addresses to be associated with the device in the 'Add IPs or Domains' text box. The IP addresses you

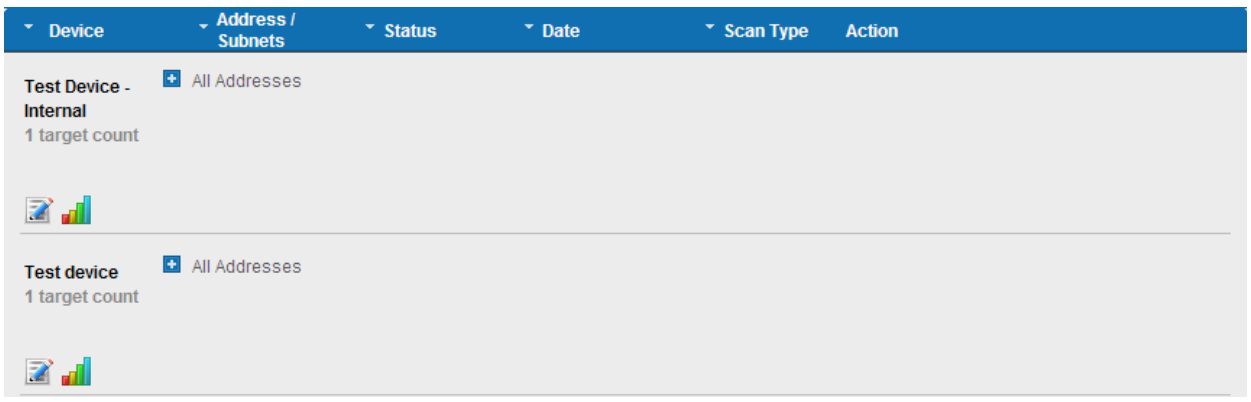
specify here will be scanned whenever you run a scan on the 'Device Name'. You can add as many IP addresses as allowed by your license. If you want to add more than one IP, click on the link Add Multiple Addresses and enter the IPs separated by commas. IP ranges can also be specified with each address in that range counting as one of your licensed total IP's.

7. Click the 'Add' button beside the text box.



8. The IP(s)/Domain(s) will be added to the device. If you want to add more IPs or Domains, repeat from Step 6.
9. After adding required IPs and Domains to the Device, Click 'Save'.

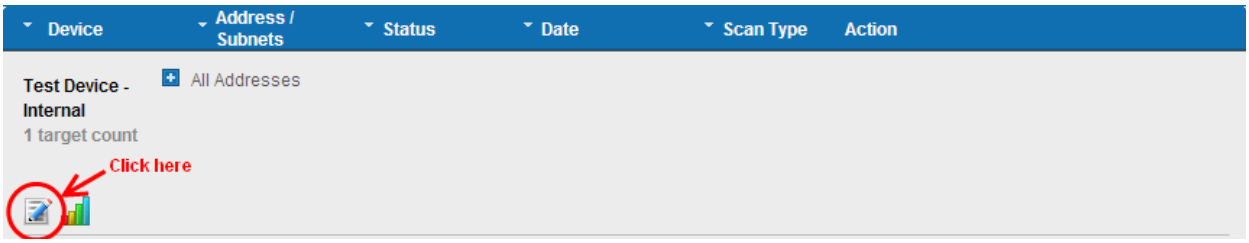
The device will be added to your HackerGuardian Account. The device will be validated for PCI compliance on your first on-demand scan and the status will be updated accordingly.



2.4.2. Internal Devices Management

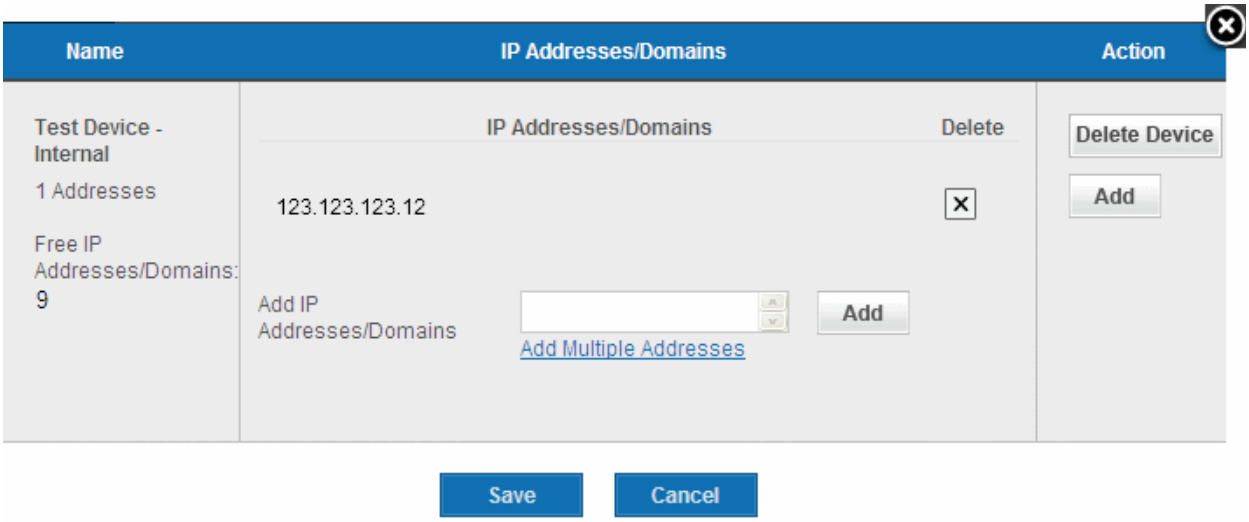
The 'Device List' area of the HackerGuardian interface provides the administrator with the possibility to the full complex of device management. From here administrator can edit a device's details, delete a device, move a domain to another device or remove a domain from a device.

To access the interface for device management, click the edit button beneath the device as shown below.



2.4.2.1. Adding Additional IPs

1. Open Edit Interface as explained above.



2. Enter the new IP addresses in the 'Add IPs or Domains' text box and click Add button beside the textbox.
3. Click Save.

2.4.2.2. Removing an IP from a Device

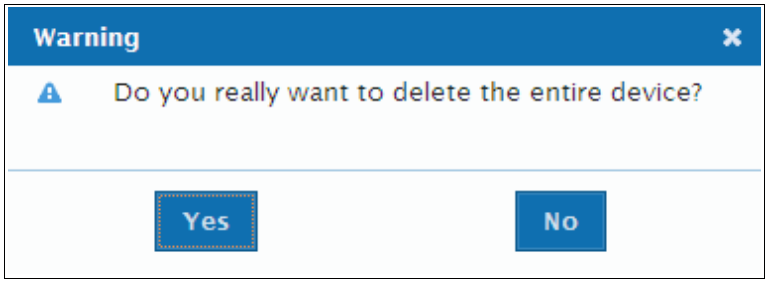
1. Open Edit Interface as explained above.
2. Click the 'X' button beside the IP address and click 'Save'.

2.4.2.3. Moving an IP to Another Device

- Remove the IP from the device in which it is existing and add it to the destination device.

2.4.2.4. Removing a Device

1. Open Edit Interface as explained above.
2. Click the 'Delete Device' button and click 'Yes' in the confirmation dialog.



2.4.3. How to Install the Agent

The Agent software is available in three formats:

- ISO image - To create a Live, bootable CD for configuring the agent on a physical machine.
- Zip file - To create a Live, bootable USB stick for configuring the agent on a physical machine.
- VMware Player - Version of the agent designed to run under VMware Player.

Installing and configuring the agent on a physical machine requires you to create a Live CD or Live USB. Download the VMware version if you wish to run under VMware player.

2.4.3.1. How to Create a Live CD

- Download the iso image file comodo_1.0.iso from http://download.comodo.com/hg/comodo_1.0.iso
- Burn a CD with the iso file.

The Live CD is successfully created and you can install and configure the agent on any local target device in your network and added to LAN Device Management area of HackerGuardian. All you need to do is to boot the device through the Live CD.

2.4.3.2. How to Create a Live USB

- Download the zip file comodo_1.0.zip from http://download.comodo.com/hg/comodo_1.0.zip
- Plug in a USB memory drive (minimum 64MB, >128MB is preferred), pre-formatted with either FAT16 or FAT32 file system.

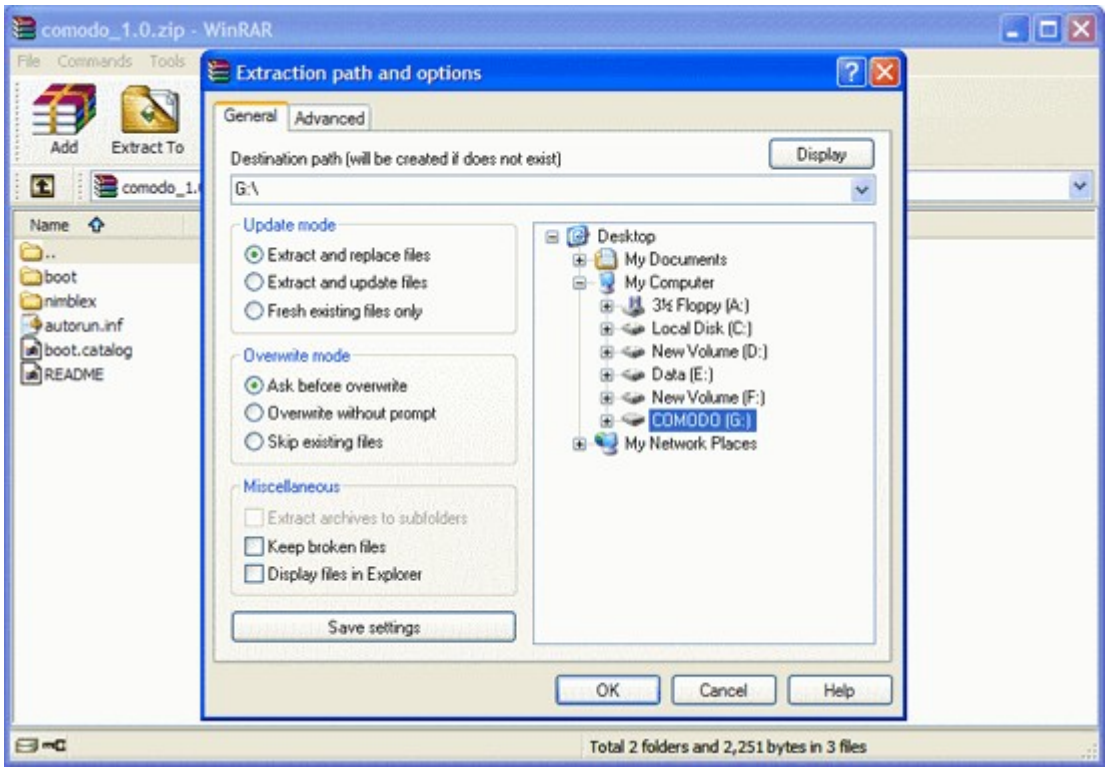
Note: USB drive must be formatted and contain only one partition with no hidden partitions.

For UNIX/Linux systems -

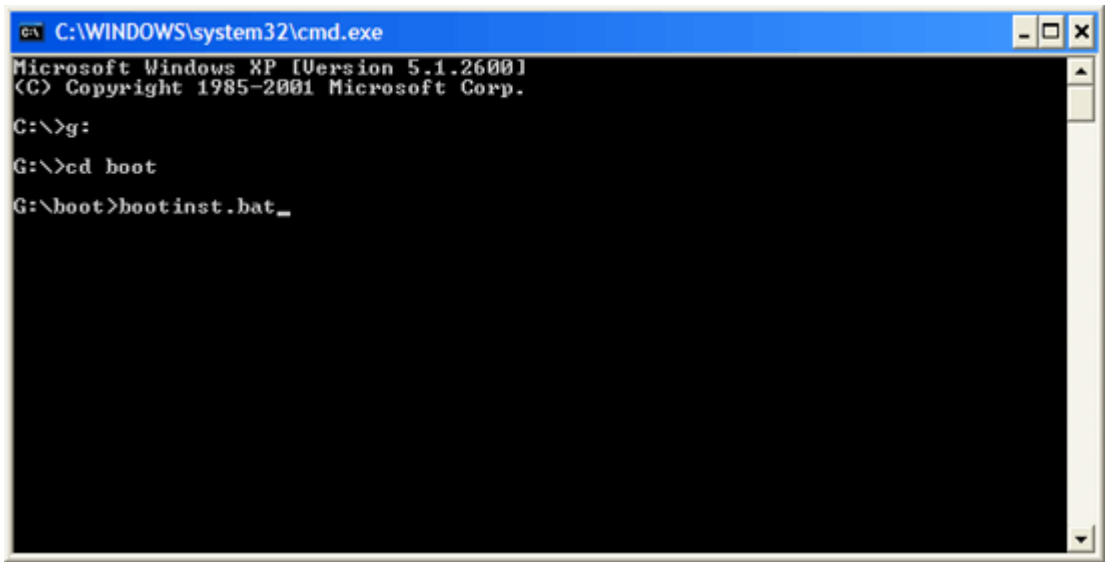
- Unzip comodo.zip on the USB drive (it must be mounted somewhere like /mnt/usb, ex: mount /dev/sdb1 /mnt/usb)
- Type *cd /mnt/usb/boot && chmod* -R +x .
- Run *sh ./bootinst.sh and follow instructions*
- Type *umount /mnt/usb*

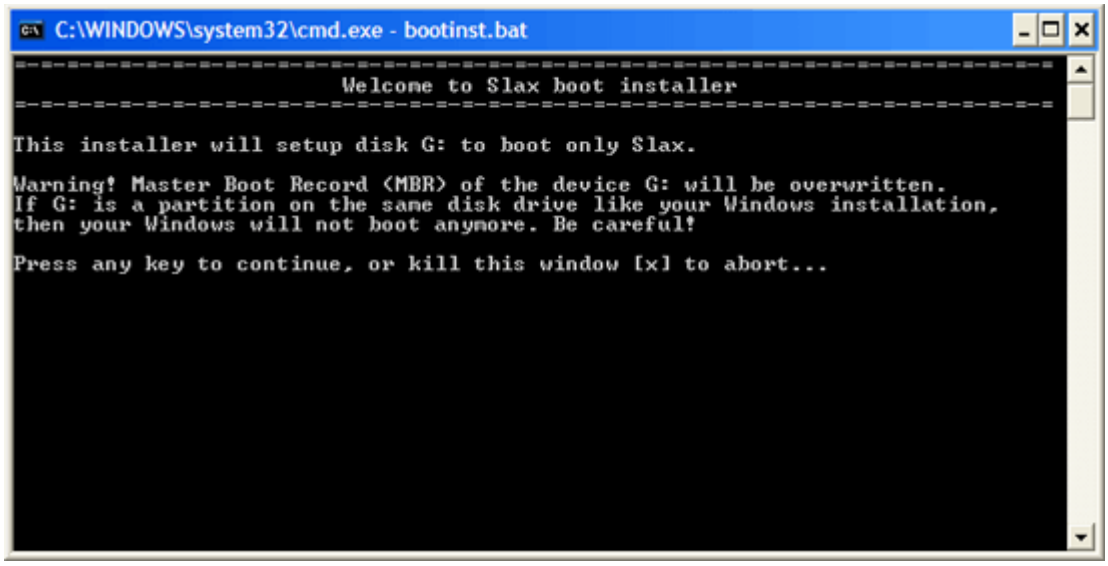
For Windows XP/2000/Vista systems -

- Unzip comodo.zip on target USB drive (it must appear as drive letter, ex: G:)

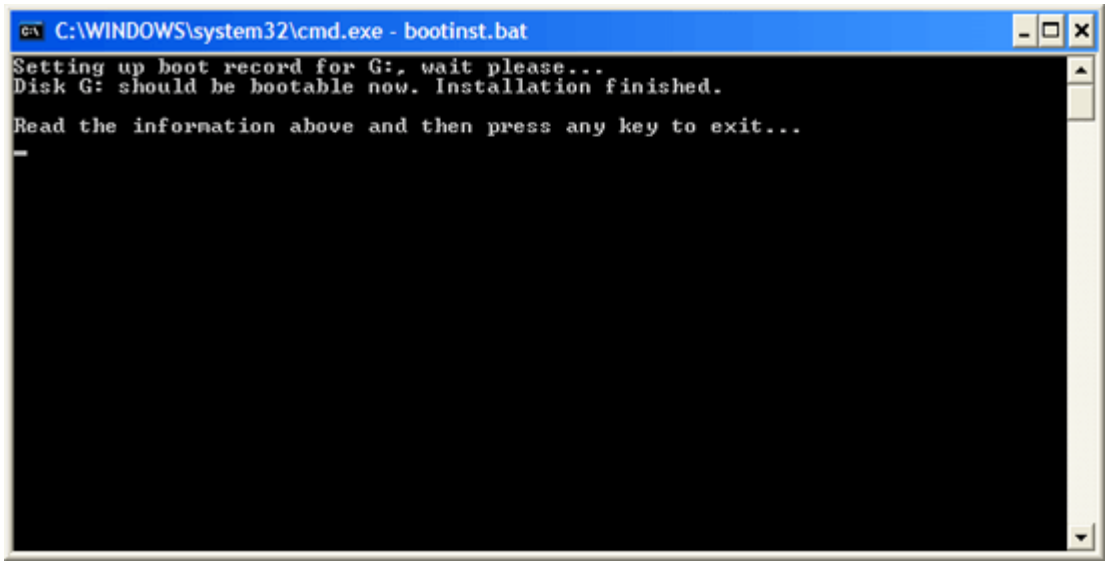


- Run *cmd.exe* and change drive letter to USB disk (ex: G:)
- Type *cd boot* in the command prompt
- Run *bootinst.bat* and follow instructions





- Read the Warning carefully. Press any key except X to continue. To cancel creating the Live USB press X.

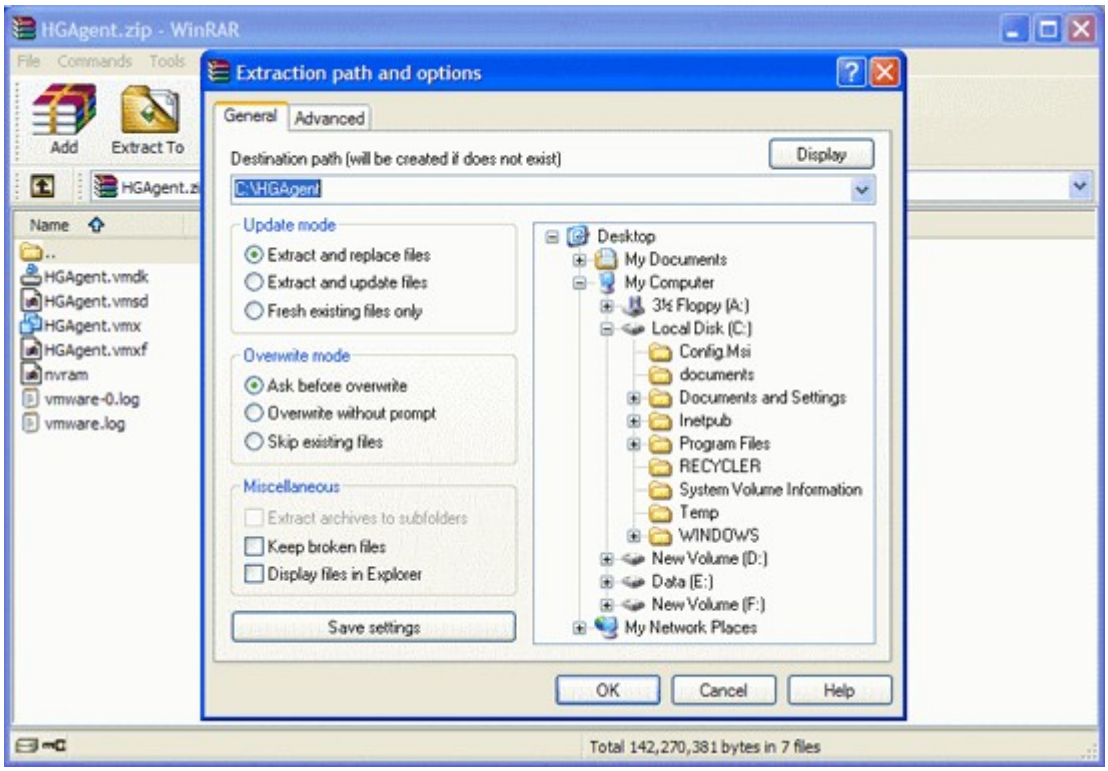


- Press any key to exit.

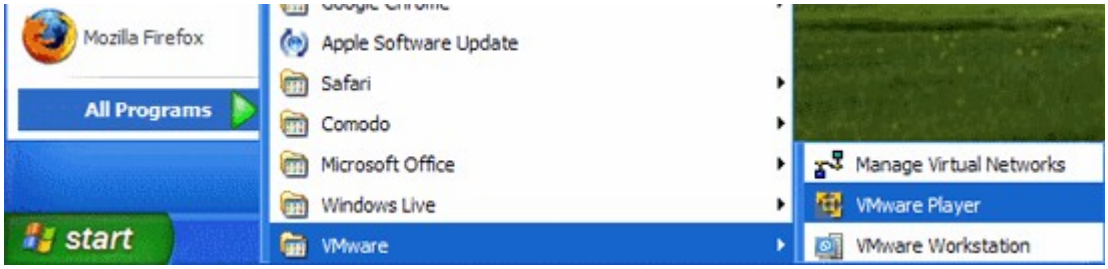
The Live USB is successfully created and you can install and configure the agent on any local target device in your network and added to LAN Device Management area of HackerGuardian. All you need to do is to boot the device through the Live USB.

2.4.3.3. How to Use the Agent on a VM Machine

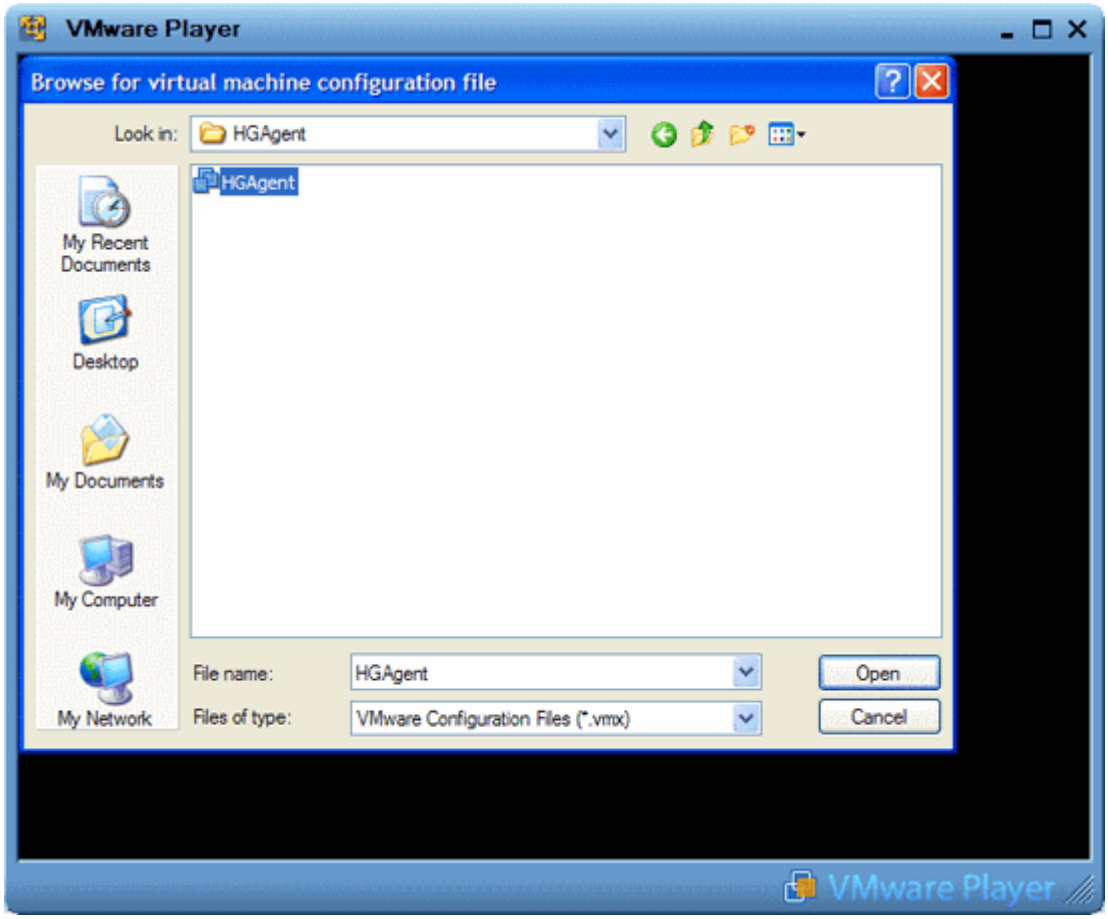
- Download the zip file HGAgent.zip from http://download.comodo.com/hg/HGAgent.zip.
- Extract the file HGAgent.zip to a folder of your choice. (e.g. C:\HGAgent)

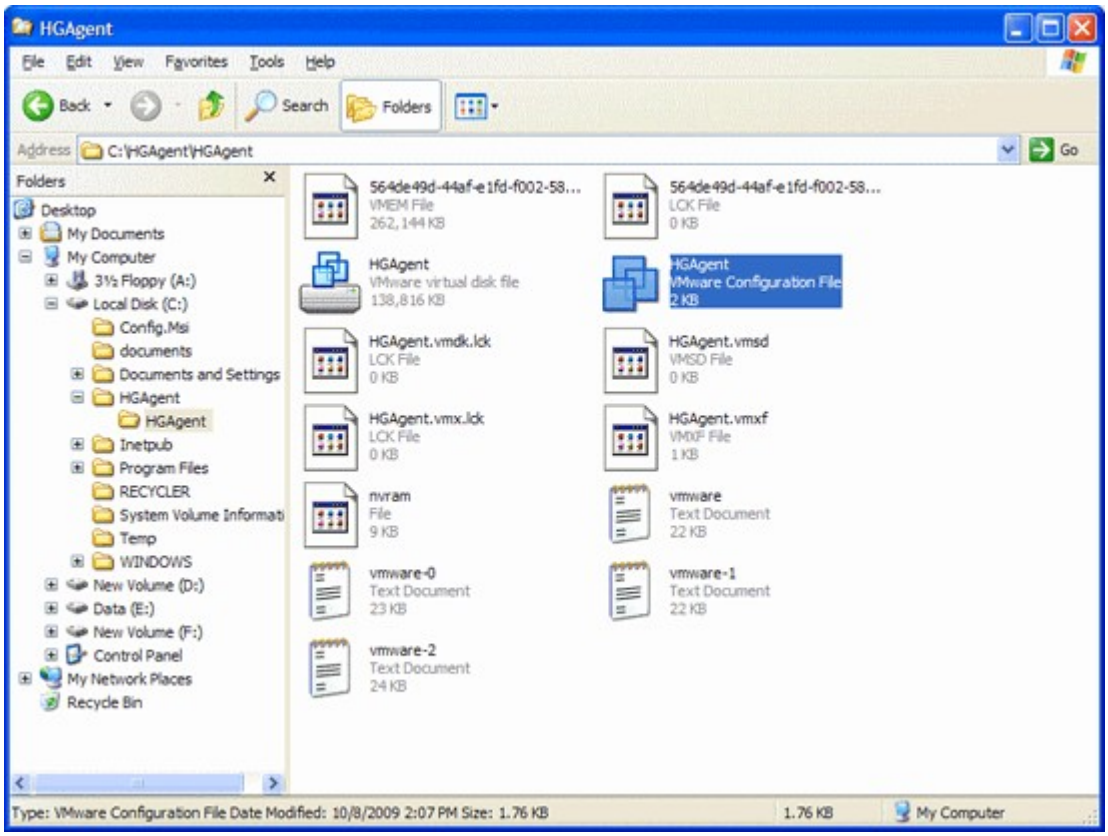


- Start VMware Player by clicking Start > All Programs > VMware > VMware Player



- Alternatively, open the folder where you have extracted the HG Agent through Windows Explorer and double click on the file 'HGAgent.vmx'.





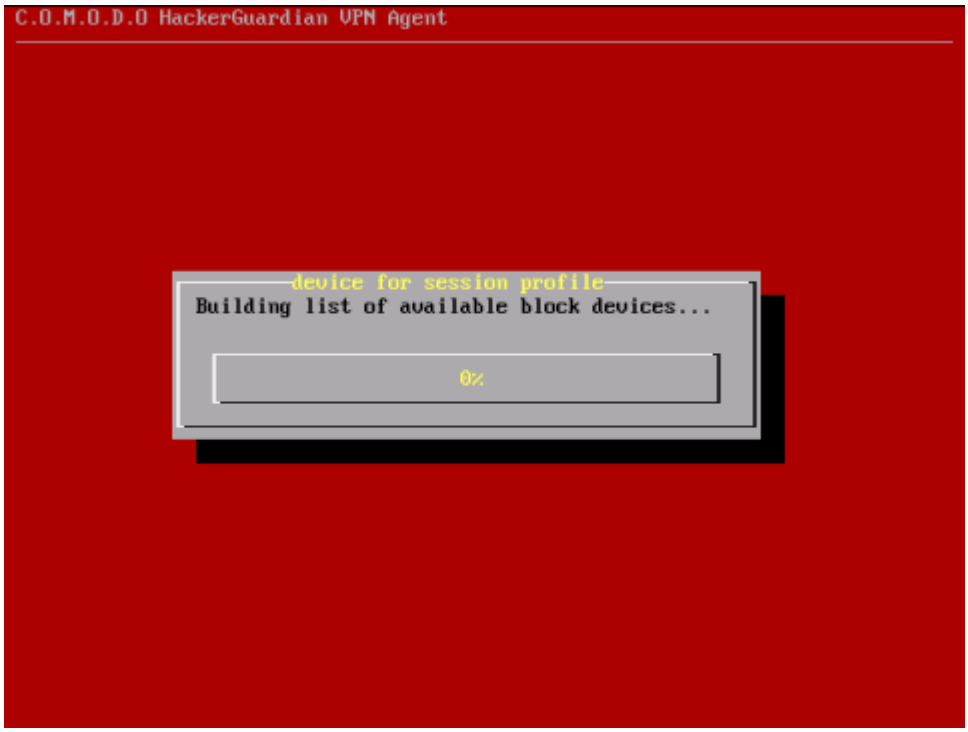
The Agent starts on the VMware Player and allows you to configure it. See **Configuring the Agent** for more details.

2.4.4. Configuring the Agent

To start the configuration, boot the device through the Live CD or the Live USB.

Step 1

The agent starts building a list of block devices for storing the configuration files. The agent detects hard disks, USB memory drives and/or other available block devices containing with live file system (like FAT 12, FAT16, FAT 32, VFAT, ext2/ext3, XFS, reisrfs etc.) and proposes a list of valid devices for you to choose from. Select a device to store the configuration files.

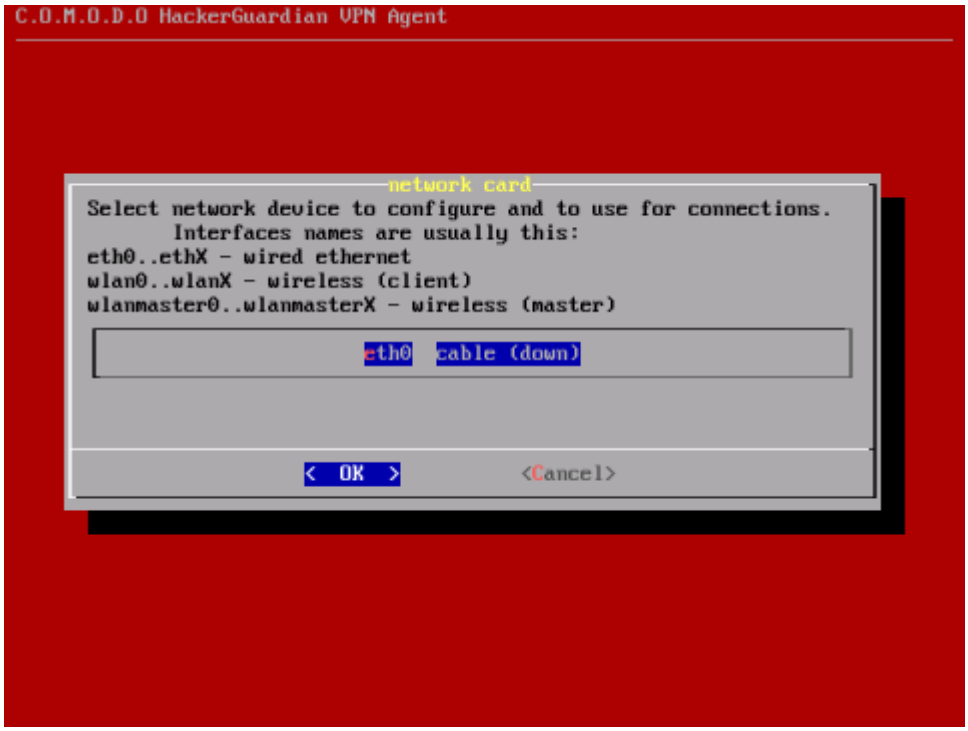


Step 2

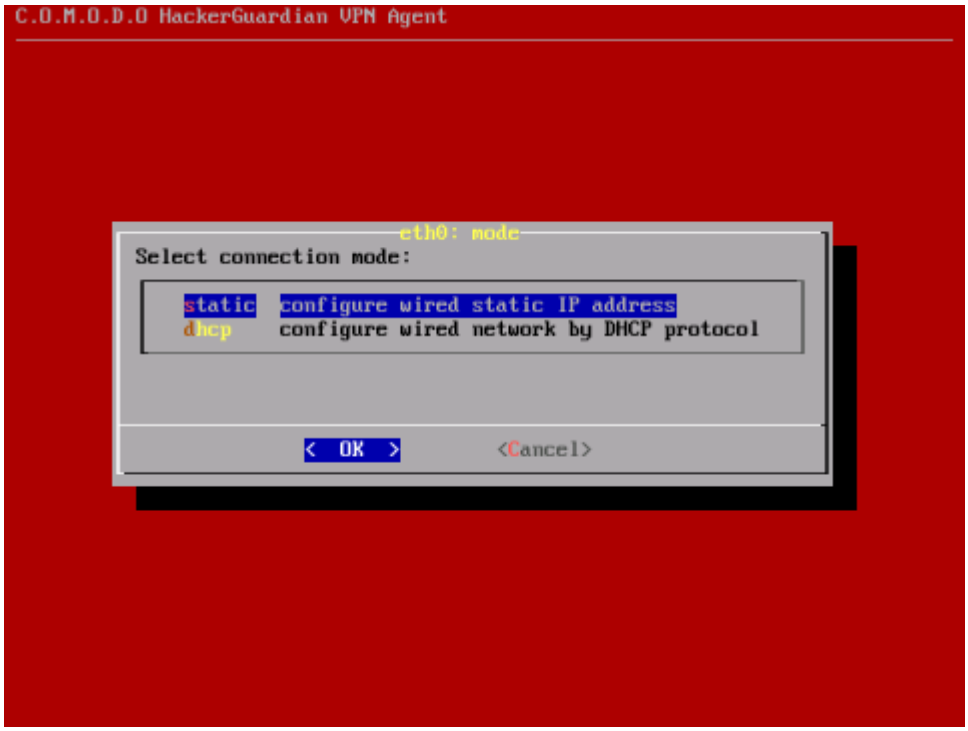
The agent asks for a short description of the saved configuration. You can give a short name/description for the configuration (Max 40 characters)

Step 3

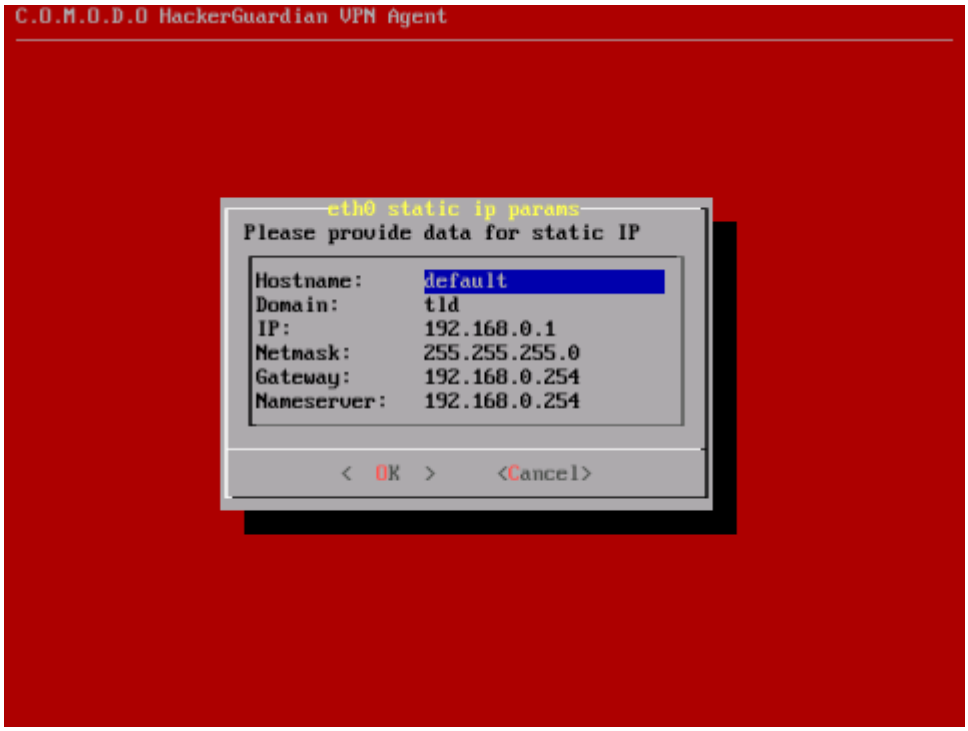
The network configuration dialog appears to specify the network configuration settings. The available network adapters are detected and displayed as a list. Only one network adapter can be used at a time. Select the network adapter through which you want the scan to be performed and select OK.



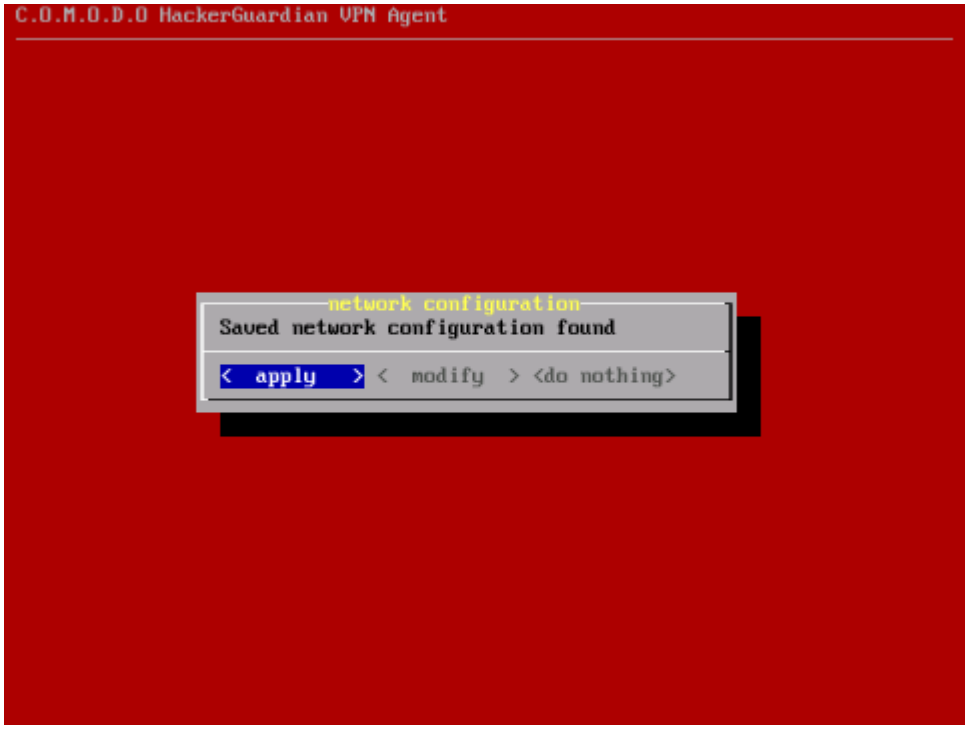
The connection mode configuration dialog appears. The available choices are Static IP address and DHCP. Select the mode in which the device is connected.



In the next dialog, set the parameters for the selected connection (The agent detects the default parameters of the device and displays them. Only change the values you wish to change and select OK. Use up and down arrow keys and the tab key for navigation).



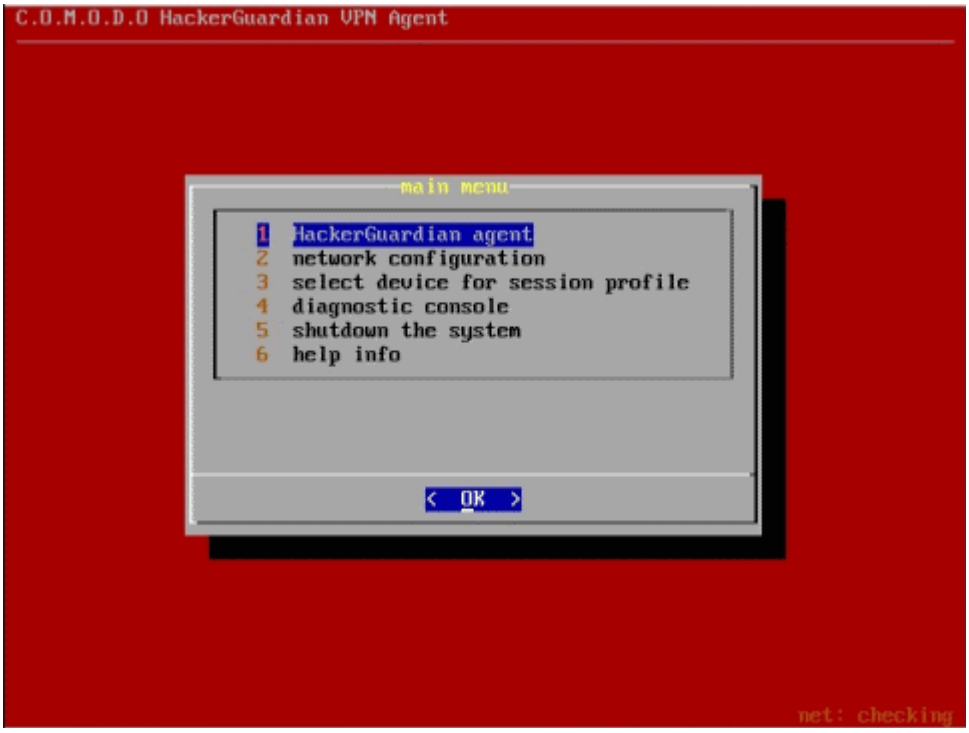
If you are satisfied with the above configurations, select 'Apply' in the next dialog.



The configuration will be saved. If you want to edit the settings before saving, select Modify. The Network configuration will be restarted. If you do not want to save the settings, select Do nothing. The configuration will not be saved and the network configuration will be restarted.

The main menu will be displayed on completion of the configuration. You can modify the configuration at any time through the options in the main menu.

2.4.5. Using the Agent - Main Menu

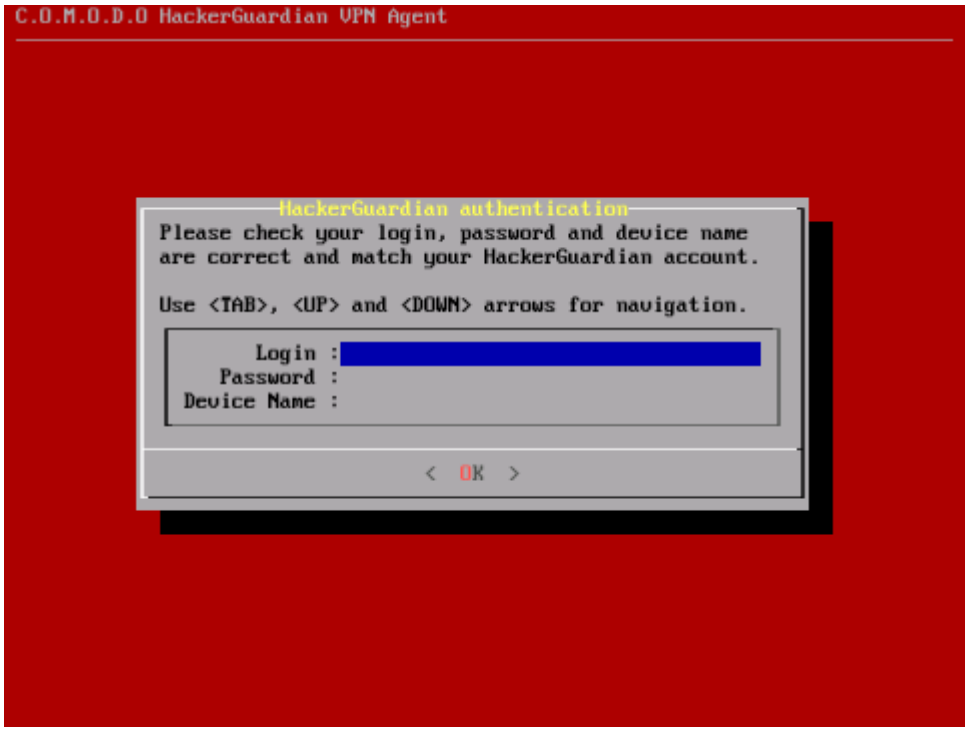


The Main Menu of the HackerGuardian VPN agent contains the following options

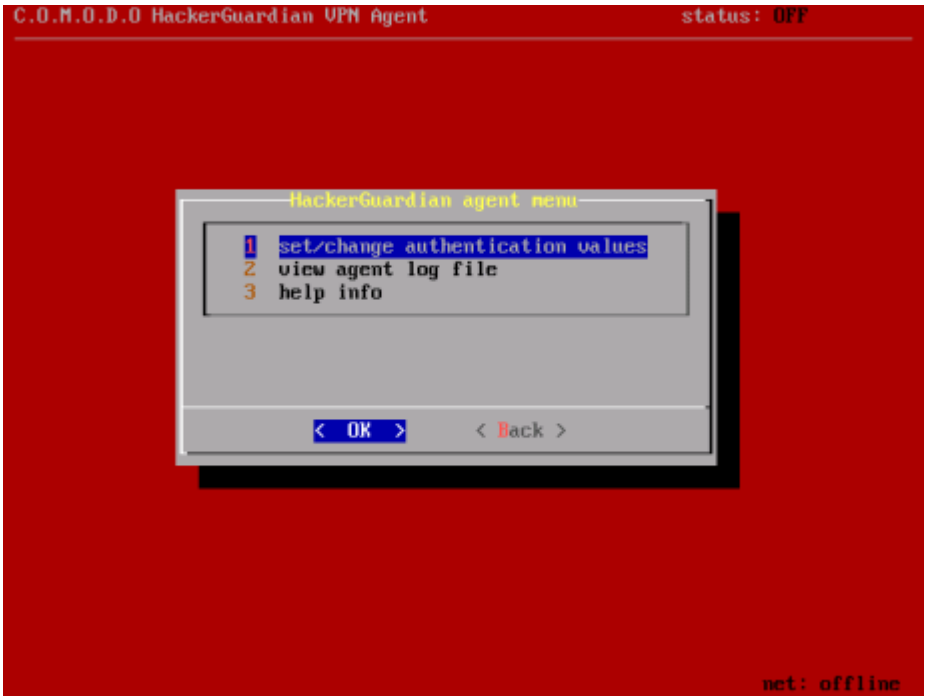
- HackerGuardian Agent
- Network Configuration
- Select a device for session profile
- Diagnostic console
- Shutdown System
- Help info

2.4.5.1. HackerGuardian Agent

The HackerGuardian sub-menu contains the options for configuring various HackerGuardian VPN authentication settings. Selecting the HackerGuardian agent first opens a Login dialog.



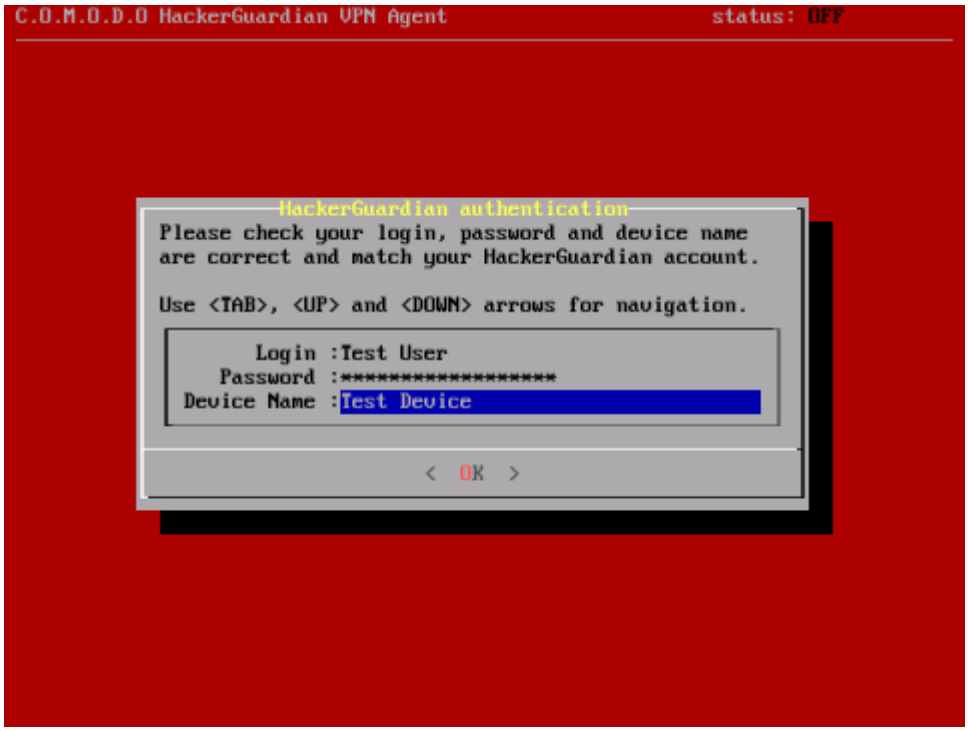
- Type your Login name, Password and the device name as you registered in the HackerGuardian website.



The options available are:

- Set/Change Authentication Values
- View Agent Log File
- Help info

Set/Change authentication values - The VPN connection values of Login Name, Password and Device name can be changed by selecting this option. This is useful when you have configured the agent on one device and wish to quickly running the scan on another pre-registered device.



Important Note: The Device Name displayed in the agent must *exactly* match the name that you set for the target Device in the 'LAN Devices' area of your HackerGuardian account. Incorrect authentication settings will lead to failure of authentication and no scan will take place.

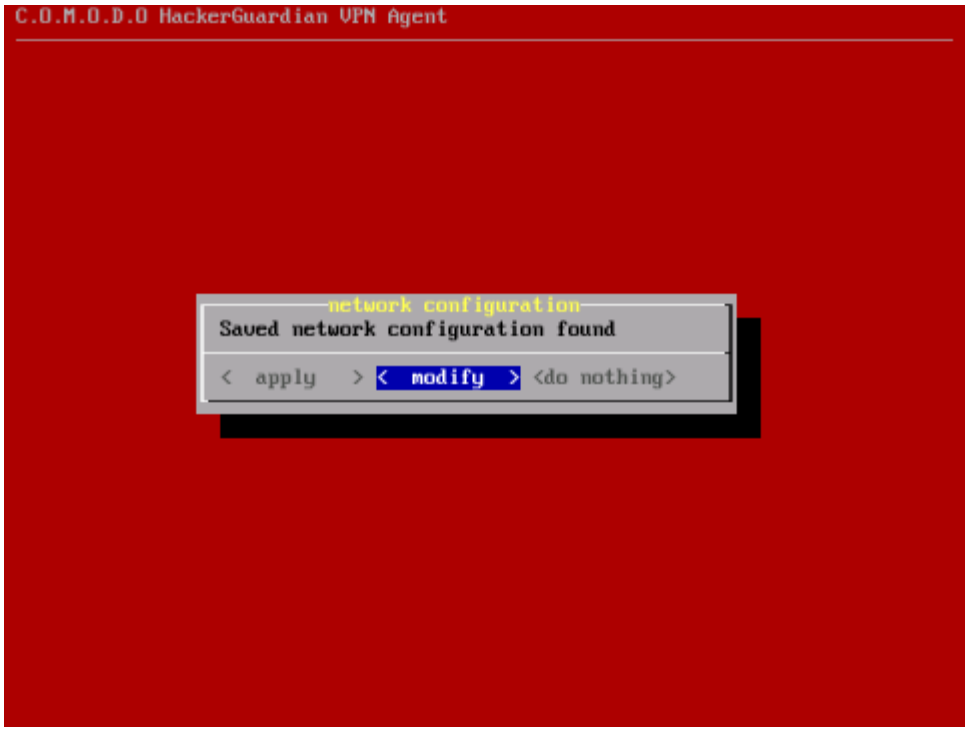
View Agent Log File - This option allows you to view the HackerGuardian agent execution progress trace, warnings or errors and diagnose connection problems.

Help info - Opens the built-in help page that give explanations on each item in the HackerGuardian Agent Menu.

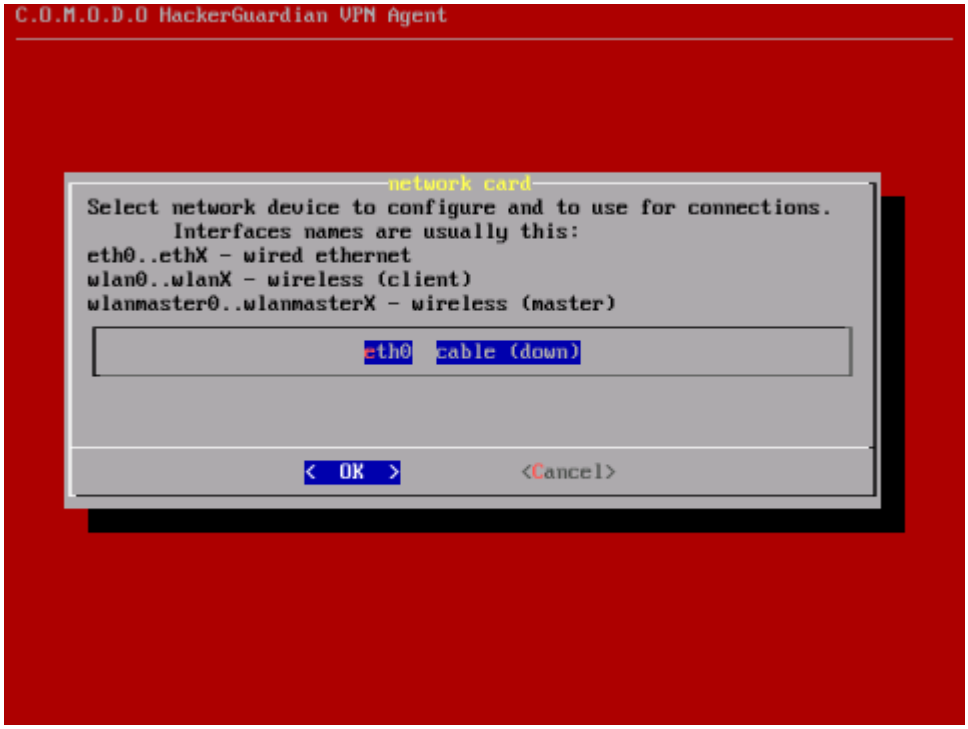
2.4.5.2. Network Configuration

The network configuration menu allows you to reconfigure the network settings you made during the configuration of the agent.

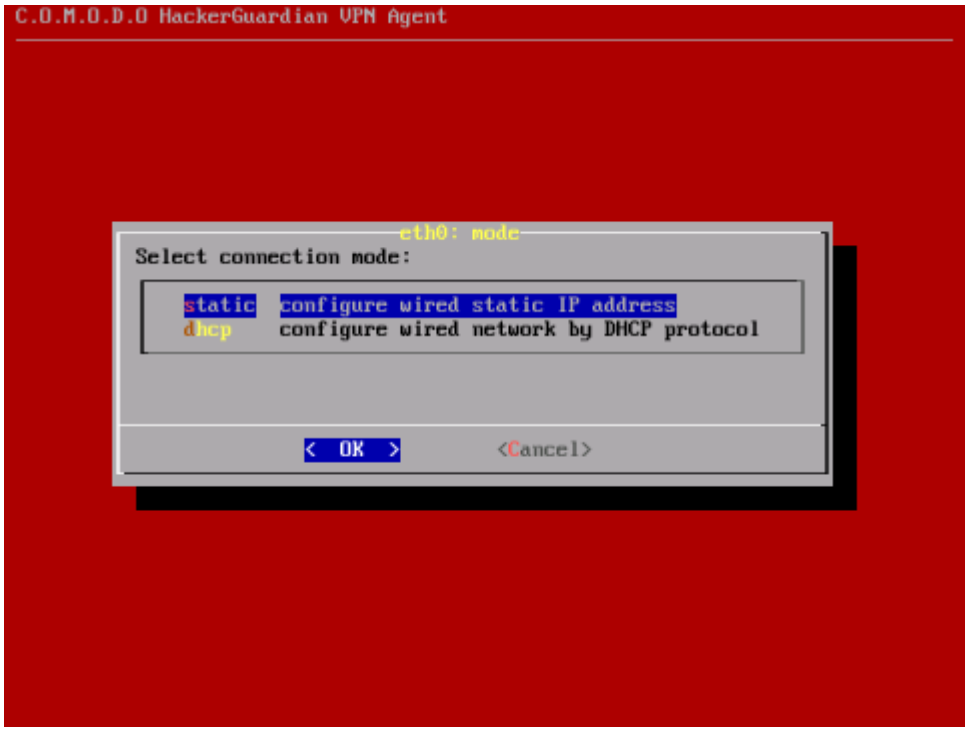
To change the existing network configuration, select 'Modify' in the network configuration dialog.



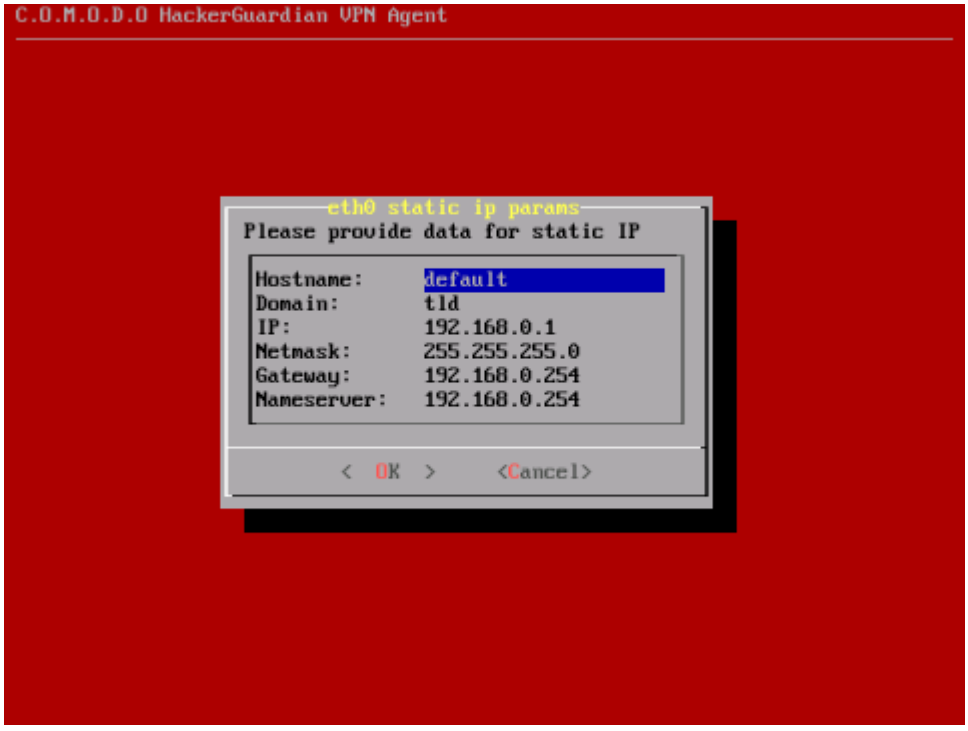
The network configuration wizard will be restarted. The available network adapters are detected and displayed as a list.



- Select the network adapter through which you want the scan to be performed and select the connection mode.



- The available connection mode choices are Static IP address and DHCP. Select the mode in which the device is connected to the network. In the next dialog, set the parameters for the connection. (The agent detects the default parameters of the device and displays them. Only change the values you wish to change and select OK. Use up and down arrow keys and the tab key for navigation).



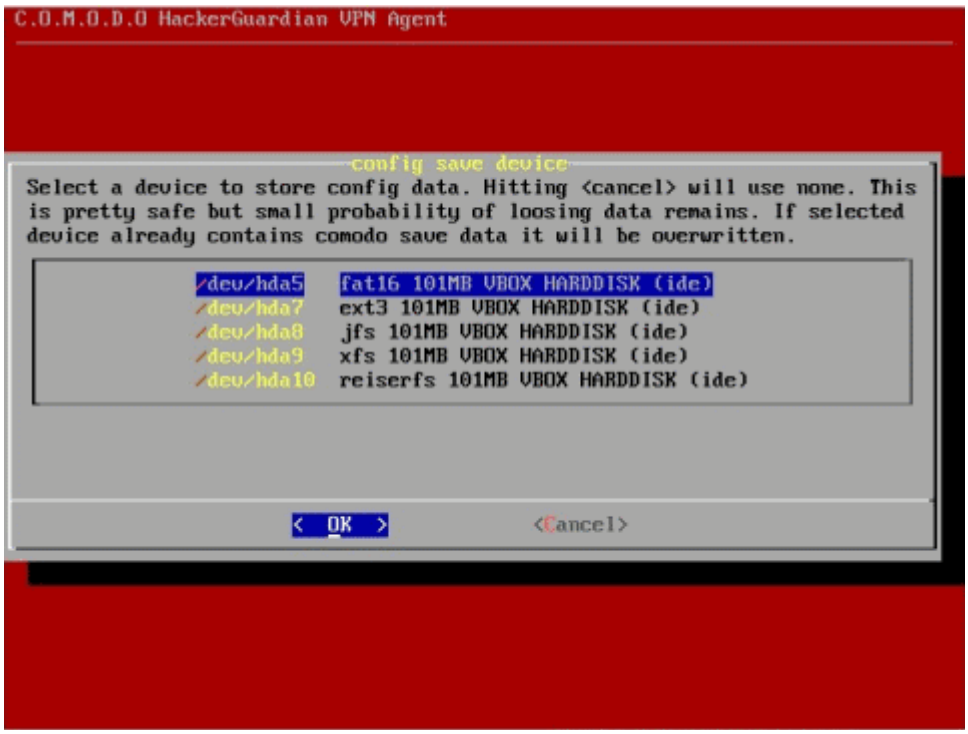
- If you are satisfied with the above configurations, select Apply in the next dialog. The previously stored parameters are overwritten with the new values. If you want to edit the settings before saving, select Modify. The Network configuration will be restarted. If you do not want to save the settings, select Do nothing. The previously stored configurations will be retained and the new configurations will not be saved.

After successfully configuring the network adapter, the network state will appear green in the lower right corner of the screen. The network state will be displayed in black if any connection problems arise indicating that the network connection setting are

to be reconfigured.

2.4.5.3. Select a Device for Session Profile

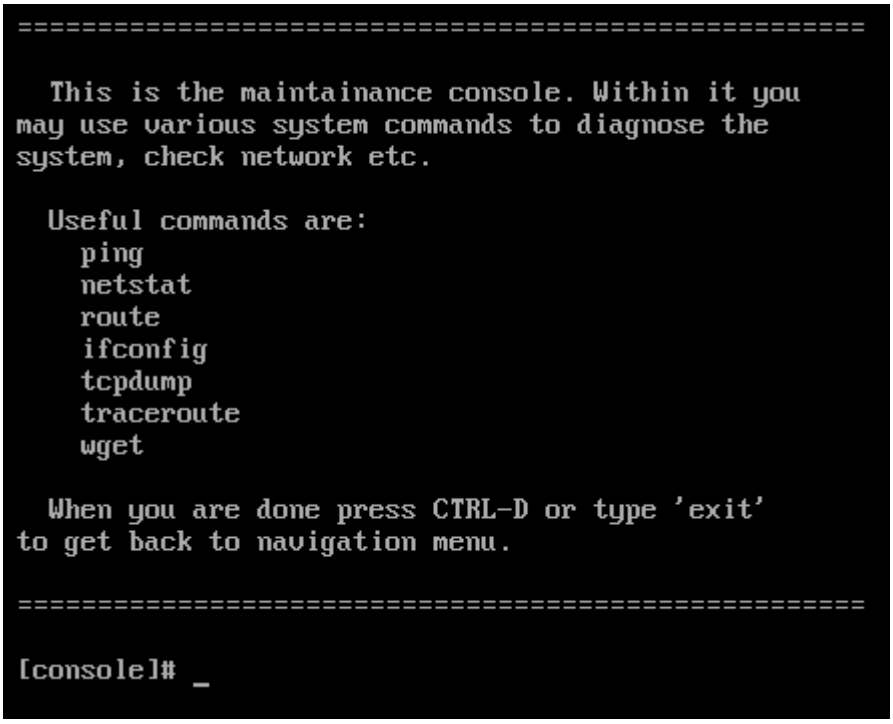
The storage device chosen previously for storing the configuration settings and the session profiles can be changed/configured by choosing this menu. Selecting this menu again starts building a list of available block devices for storing the configuration.



- Select and configure a storage device to use as a permanent storage for Live CD runtime configuration files. This is useful when you plan to boot and run the Live CD more than once with the same network settings and other configurations and do not want to reconfigure every time. The agent detects hard disks, USB memory drives and/or other available block devices containing with live file system (like FAT 12, FAT16, FAT 32, VFAT, ext2/ext3, XFS, reisrfs etc.) and proposes a list of valid devices for you to choose from. The selected device will then be used to store the configuration files by creating a special directory. The stored configuration will be automatically detected and reused every time the scanning is run. You can cancel the device selection if you do not want to store the configuration files.

2.4.5.4. Diagnostic console

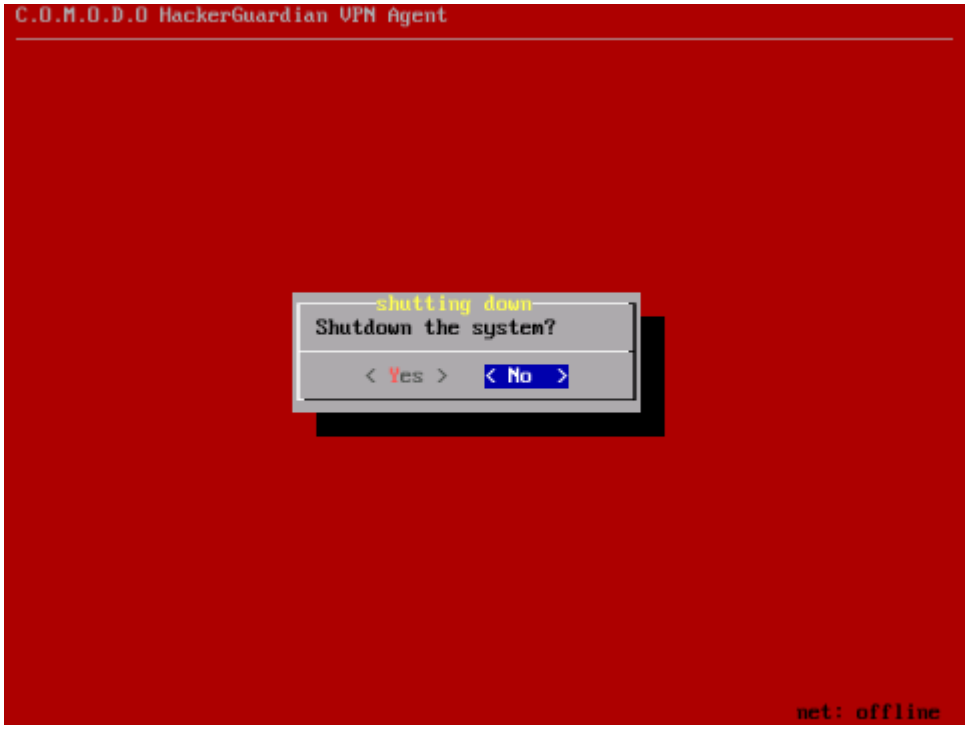
The Diagnostic Console is intended for advanced users.



The menu contains various tools to diagnose the problems if the agent is not running properly. The console can be opened any time as required and it will not interfere the agent's normal operation.

2.4.5.5. Shutdown System

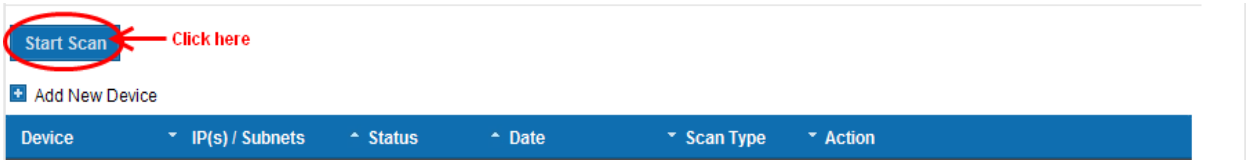
Selecting this option will shut down the system.



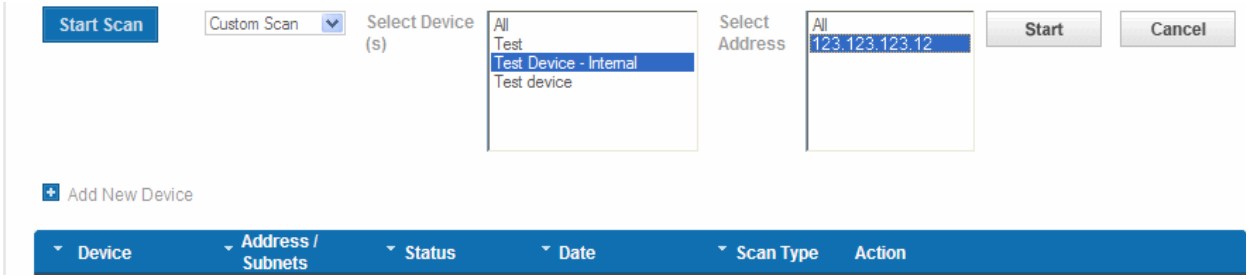
Note: The runtime settings are automatically saved in the configured storage device, so no extra action is needed for this.

2.4.6. Start Device Scanning

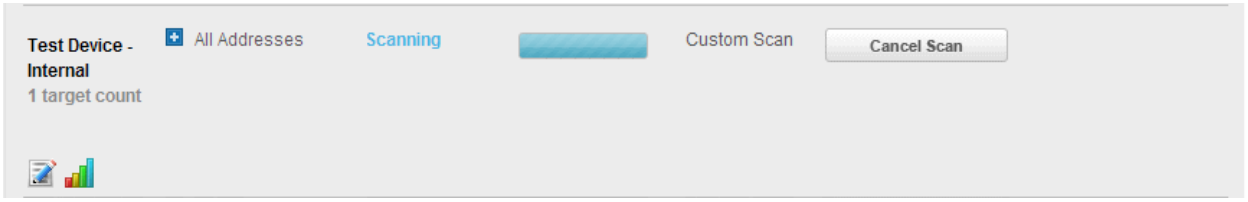
1. Login into HackerGuardian online interface and click 'Start Scan' button in the 'Overview' area as shown below.



The scan configuration options will be displayed.



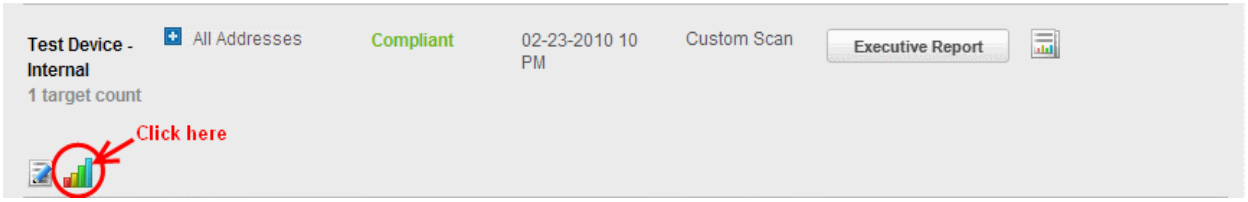
2. Select 'Custom Scan' from the scan type drop-down menu.
3. Select the device to be scanned in the next box. If you want to run the scan for all the devices at once, select 'All'
4. Select the IPs in the next box. If you want to run the scan for all the IPs in the selected device at once, select 'All'.
5. Click 'Start'



Tip: If you want to run the scan simultaneously on multiple devices, you can start scanning on the next device by following the same procedure when the scan in running in one device. Also, you can terminate the scan at any moment by clicking 'Cancel Scan' button.

2.4.7. Viewing a Dashboard Summary of Scan Results

On completion of scan, a dashboard summary of the results will be displayed in the 'Overview' area. If you want to switch to the scan results of other devices, click the bar-graph button beneath the device name as shown below.



2.4.8. Viewing Executive Report, Charts and Vulnerability Reports

- To view the Executive scan Report, click the Executive Report button beside the device name.
- To view the Charts page that contains at-a-glance summary of the scan results on the device and graphical representations of proportions of identified vulnerabilities according to their categories , click the charts page button

 in the row of the Device.

- To view the Vulnerability Report, click the Vulnerability Report button beside the IP/domain name from the list of IPs/domain names displayed by clicking the '+' button beside the Device name.

The Administrator can also download a Report Pack containing the pdf files of the reports for submitting to the acquiring bank from the Reports area, after a successful scan. Refer to HackerGuardian Reports for more details.

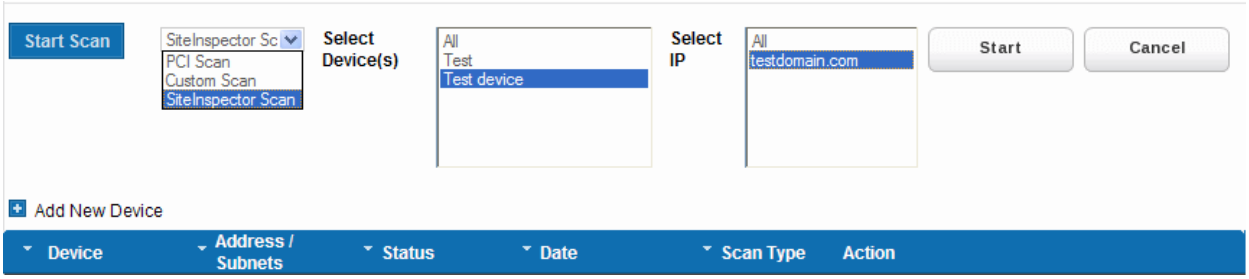
2.5. SiteInspector Scan

SiteInspector Scans identify any malicious content running on your webpages and reports them to the website owner. The scan can be run on-demand on any HackerGuardian/HackerProof network device.

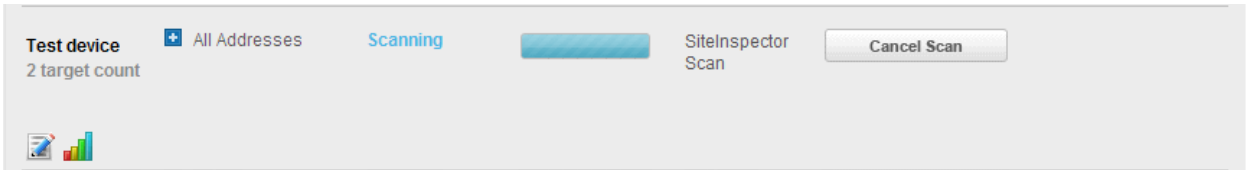
Note: In order to run a SiteInspector scan, it is necessary for the administrator to have at least one HackerGuardian/HackerProof Device created in advance.

To start a SiteInspector Scan

1. Login to your HackerGuardian Account and click 'Start Scan' from the 'Overview' area.



2. Select 'SiteInspector Scan' from the scan type drop-down menu.
3. Select the device to be scanned in the next box. If you want to run the scan for all the devices at once, select 'All'.
4. Select the IPs/Domains in the next box. If you want to run the scan for all the IPs/Domains in the selected device at once, select 'All'.
5. Click 'Start'



Tip: If you want to run the scan simultaneously on multiple devices, you can start scanning on the next device by following the same procedure when the scan in running in one device. Also, you can terminate the scan at any moment by clicking 'Cancel Scan' button.

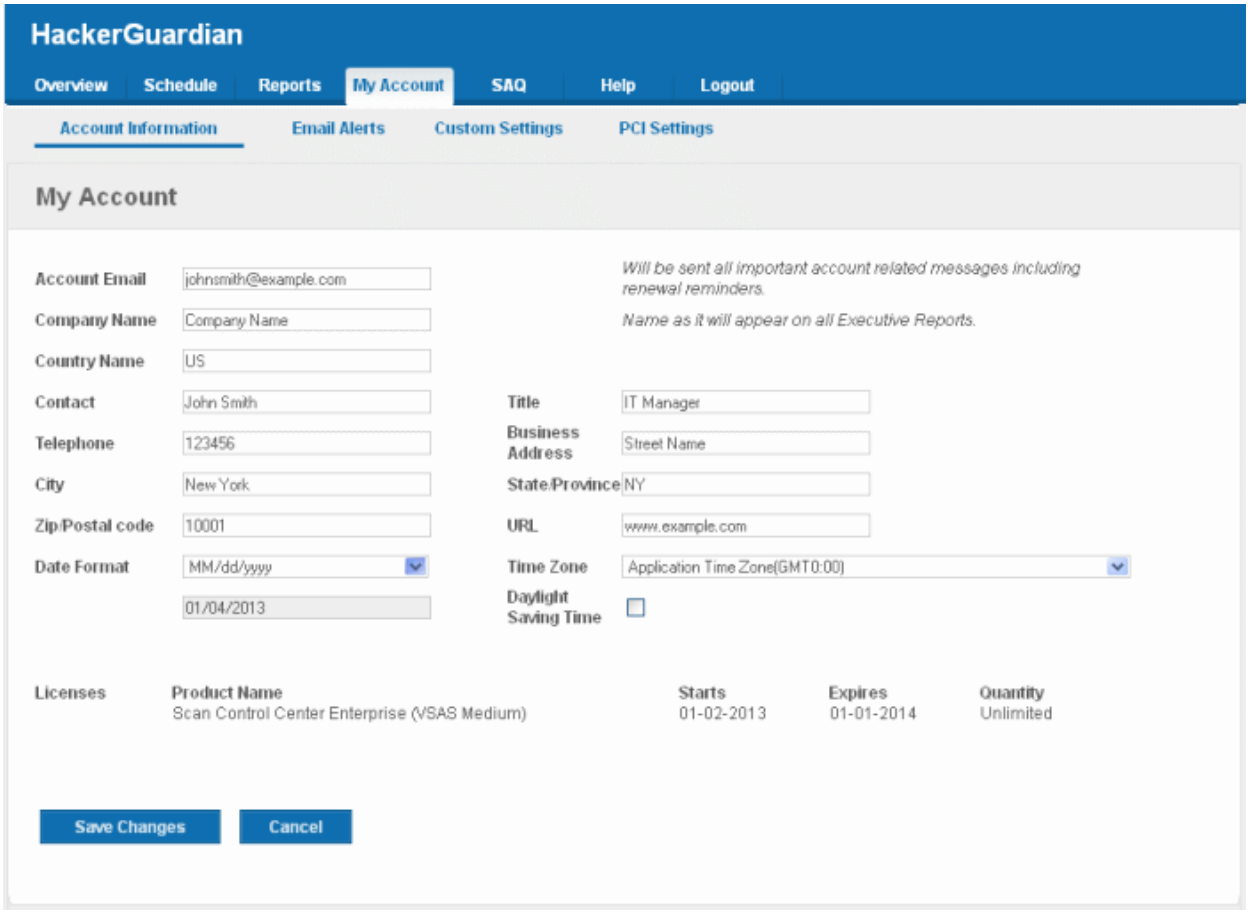
On completion of scan, SiteInspector generates a scan report, which can be accessed through the 'SiteInspector Reports' area.

2.6. Account Preferences and Scan Settings

The 'My Accounts' area of the HackerGuardian interface displays your account details, license information, and your email alert settings, and also allows you to change them if required. It also enables you to configure the

general scanning options, the HackerGuardian plug-ins to be deployed during scanning and PCI scan options like configuring start url and hidden urls of your website.

You can access this area by clicking the 'My Account' tab in the Navigation bar.



This area contains four tabs.

My Account - Enables the Administrator to view/modify the account related information, view License information and configure email alert options.

Email Alerts - Enables the Administrator to configure email alert options.

Custom Settings - Enables the Administrator to configure general scanning options and to select vulnerability plug-ins to be deployed during the scans.

PCI Settings - Enables the Administrator to configure the start url, from where HackerGuardian has to start scanning all the webpages/microsites of the website. The Administrator can also specify the hidden urls in the website to be scanned.

2.6.1. My Account Area

To access the My Accounts area

1. Switch to 'My Accounts' area of the HackerGuardian interface.
2. Click the 'My Accounts' link in the 'My Accounts' area

This interface allows you to:

- View/Modify your Account information provided while creating your account;
- View your License information.

2.6.1.1. View/Modify Your Account Information

Account Email - Displays the email address of the subscriber of the HackerGuardian service. All the account related messages and reminders for renewals will be sent to this email address.

Company Name - Displays the name of the Organization/Company attached to the account.

Country Name - Displays the name of the Country of the Organization/Company.

Contact - Displays the name of the Administrator/Contact person of the Organization/Company, responsible for subscription of HackerGuardian service.

Title - Displays the position/job title of the Administrator/Contact person.

Telephone - Displays the telephone number of the Administrator/Contact person.

Business Address - Displays the address of the Organization/Company.

City - Displays the city of the Organization/Company.

State/Province - Displays the State/Province of the Organization/Company.

Zip/Postal code - Displays the Zip/Postal code.

URL - Displays the url of Organization/Company's website.

Date Format - Allows you to change / select the date format.

Time Zone - Allows you to change / select the time zone.

Daylight Saving Time - When this option is selected, the time stamp in reports will be based on DST of the country from where you are using the application.

The administrator can enter/change the above details by deleting the old information and entering the new information.

2.6.1.2. View License Information

Licenses - Displays a list of HackerGuardian/HackerProof licenses purchased so far. The following table provides the description of columns in this area.

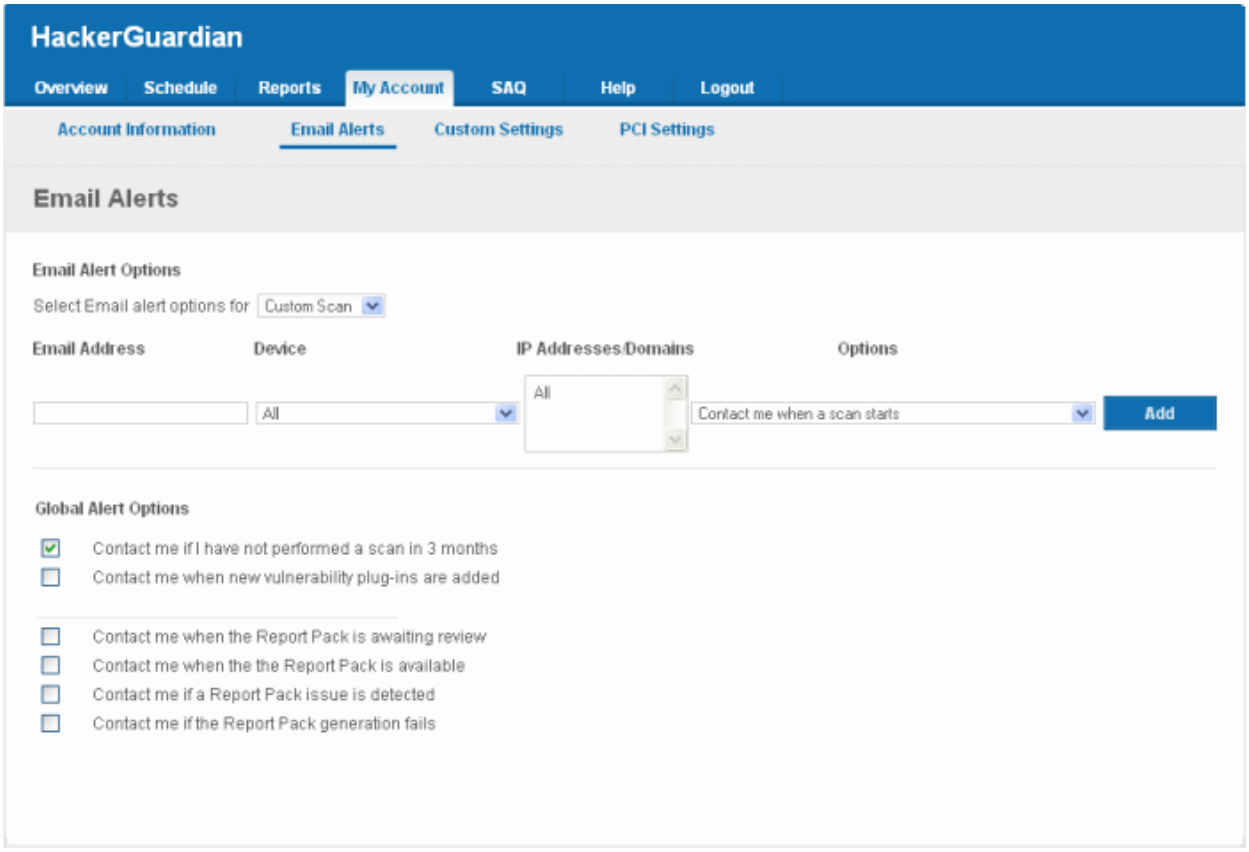
Column	Description
Product Name	The name of the HackerGuardian service subscribed
Starts	The commencement date of the service
Expires	The expiry date of the license
Quantity	The total number of IPs/Domains for which the service is subscribed

2.6.2. Configure Email Alert and Global Alert Options

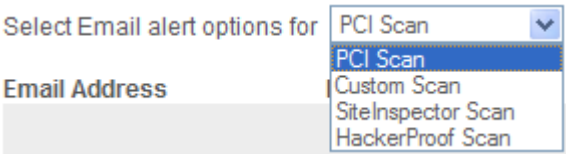
HackerGuardian sends automated email notifications to administrators upon events like the commencement of a manual or scheduled scan, the results of a scan and the failure of a scan. You can set your preferences for receiving the emails as you wish.

To configure email alert options

1. Switch to 'My Accounts' area of the HackerGuardian interface.
2. Click the 'My Accounts' link in the 'My Accounts' area



3. Select the scan type for which you wish to receive the email notification from the drop-down box beside 'Select Email alert options for'.



4. Select the preferences as given in the table below:

Option	Description
Email Address	Enter the email address to which you wish to receive the scan alert message in the text box below 'Email Address'. This address can be different from the Account Email and can belong to the administrator for the specific device/domain.
Device	Select the Device for which you wish to receive the scan alert message from the drop-down box below 'Device'. If you wish to have the alert message for all the devices, select 'All'.
IP Addresses	Select the IPs/Domains pertaining to the device selected, for which you wish to receive the scan alert message from the text box below 'IP Addresses'. If you wish to have the alert message for all the IPs/Domains, select 'All'.
Options	Select the event for which you wish to have email notification from the drop-down box below 'Options'.

5. Click 'Add'. The entry will be added to the list under Email Alert Options.
6. Repeat the procedure for setting email alerts for different types of scans and different devices.

- To remove an Email Alert entry, simply click the link Remove in the entry as shown below.

Global Alert Options

- **Contact me if I have not performed a scan in 3 months** - Selecting this option instructs HackerGuardian to send a remainder message for an on-demand scan to the Account Email address if the administrator has missed to perform a scan for three months.
- **Contact me when new vulnerability plug-in are added** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever a new vulnerability plug-in is added to HackerGuardian, enabling the Administrator to deploy the plug-in in future scans.
- **Contact me when the Report Pack is awaiting review** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report is under review by a PCI DSS approved staff of Comodo. The Report will be available for download upon completion of the Review and approval by the Comodo staff. Refer to **Downloading Report Pack** for more details.
- **Contact me when the Report Pack is available** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report is ready for download after review by a PCI DSS approved staff of Comodo. Refer to **Downloading Report Pack** for more details.
- **Contact me if a Report Pack issue is detected** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area, Report has been reviewed by a PCI DSS approved staff of Comodo and an issue has been detected in the generated report. Refer to **Downloading Report Pack** for more details.
- **Contact me if a Report Pack generation fails** - Selecting this option instructs HackerGuardian to send a notification email to the Account Email address whenever the administrator has attempted to download the HackerGuardian Scan Report pack by clicking the 'Generate Report Pack' in the Reports area and the Report generation has failed for some reasons. Refer to **Downloading Report Pack** for more details.

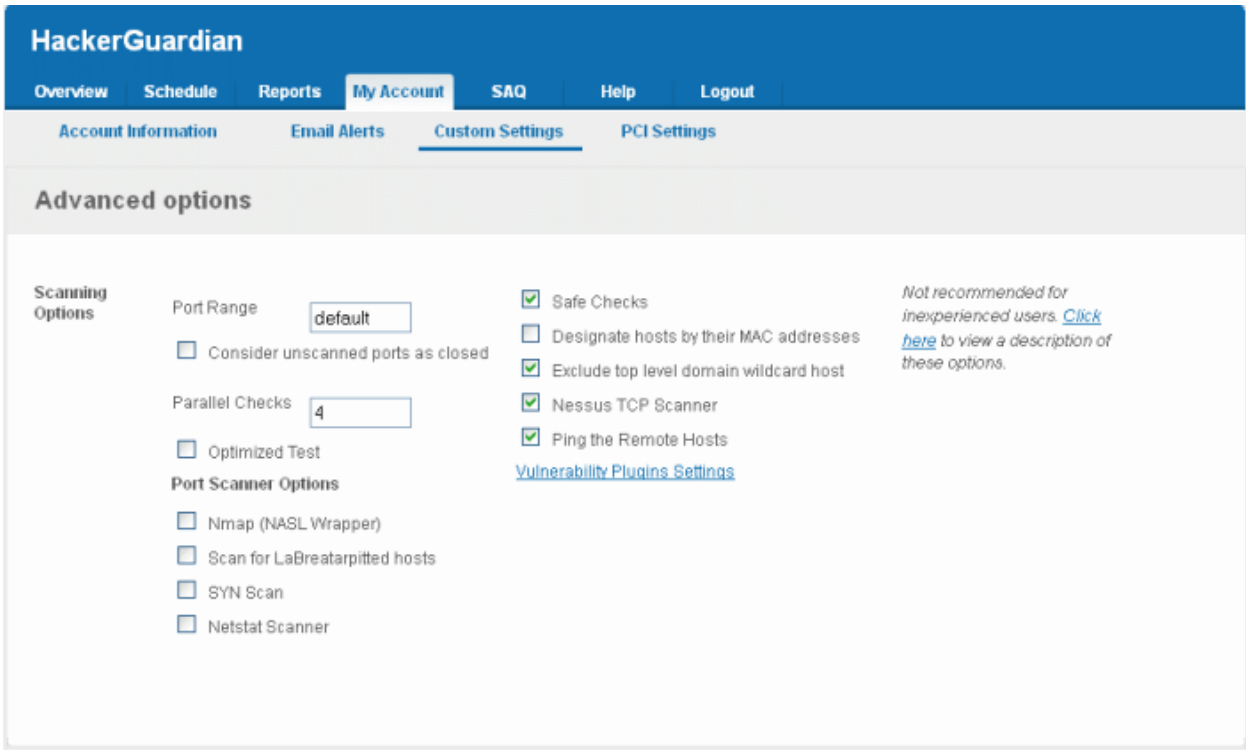
- Click 'Save Changes' for your settings to take effect.

2.6.3. Scan Configuration

The Custom Settings area enables the Administrator with advanced skills to configure the HackerGuardian scans, like specifying port range to be scanned, number of parallel checks to be done concurrently, selecting Port Scanner options, selecting plug-ins to be used for scanning etc.

To access the Advanced Options area

1. Switch to 'My Accounts' area of the HackerGuardian interface.
2. Click the 'Advanced options' link in the 'My Accounts' area



This interface allows you to:

- Configure general options pertaining to the scans;
- Choose which plug-ins are to be deployed during a scan.

2.6.3.1. Configure Scan Options

This area enables administrators to configure general options pertaining to the scans. The settings chosen in this area will apply to any scan performed on selected device in the 'Overview' and 'Scheduled Scans' areas.

Scan Option	Element Type	Description
Port Range	*Text box*	Set the range of ports to be scanned. A special value of default is allowed which scans port 1-15000. To scan all TCP ports on the target host, enter '1-65535'. Enter single ports, such as "21, 23, 25" or more complex sets, such as "21, 23, 25, 1024-2048, 6000", or enter "default" to scan default ports.
Consider unscanned ports as closed	*Check box*	Ports that are not specifically scanned will be assumed as in closed state.
Parallel Checks	*Text box*	Set the maximum number of security checks that will be performed in parallel. This may be reduced to a minimum of one to reduce network load. The maximum number of parallel checks allowed is 10% of the number of IP addresses in your account and not exceeding 25. To illustrate, If your license covers 50 IP addresses, you can run scans on five IP addresses concurrently. Lesser the number of concurrent scans, faster will be the process.
Optimized Test	*Check box*	Allows the scan to be optimized by only performing tests if information previously collected indicates a test is relevant. When disabled all tests are

		performed.

Port Scanner Options

Nmap (NASL Wrapper)	*Check box*	Runs nmap(1) to find open ports.
Scan for La Breatarpitted hosts	*Check box*	Performs a labrea tarpit scan, by sending a bogus ACK and ACK-windowprobe to a potential host. Also sends a TCP SYN to test for non-persisting lebrea machines.
SYN Scan	*Check box*	Performs a fast SYN port scan by computing the RTT (round trip time) of the packets moving back and forth between host and the target and using the value to quickly send SYN packets to the remote host.
Netstat Scanner	*Check box*	Runs netstat on the remote machine to find open ports.
Safe Checks	*Check box*	Some checks are potentially harmful to the target host being scanned. When this option is enabled scans which may harm the target host are not performed. This option should be disabled to perform a full scan.
Designate hosts by their MAC address	*Check box*	This option will identify hosts in the scan report by their Ethernet MAC address rather than their IP address. This is useful for networks in which DHCP is used.
Exclude top level domain wildcard hosts	*Check box*	Excludes the hosts whose addresses are returned by a wildcard on some top level domains or the web server.
Nessus TCP Scanner	*Check box*	Enables classical TCP port scanner. It shall be reasonably quick even against a firewalled target. Once a TCP connection is open, it grabs any available banner for the service identifications. TCP scanners are more intrusive than SYN (half open) scanners.
Ping the Remote Hosts	*Check box*	Pings the remote hosts through TCP connection and reports to the plug-ins knowledge base on whether the remote host is dead or alive. This sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYNACK.

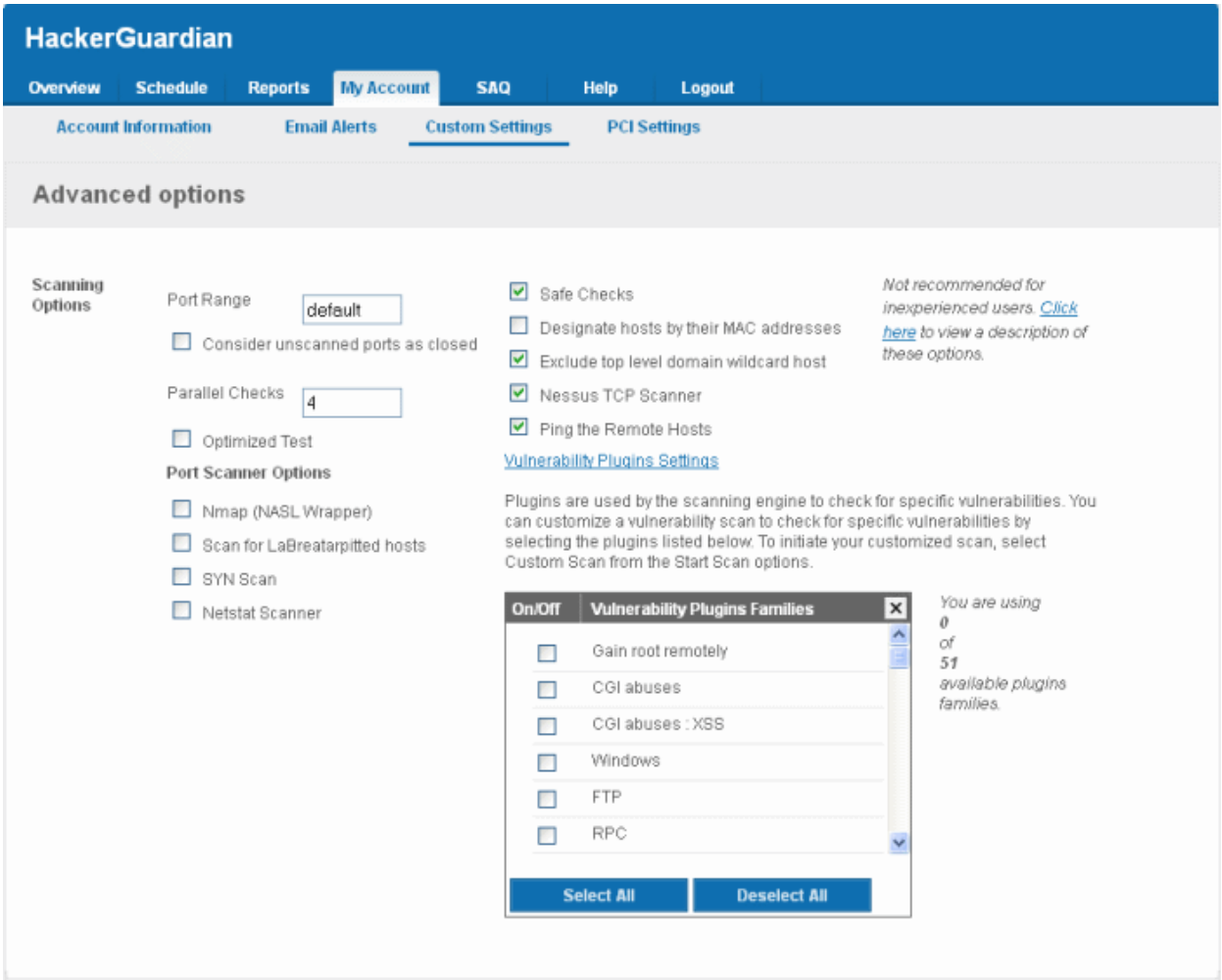
2.6.3.2. Select the Vulnerability Plug-ins to be Deployed

Each individual vulnerability test is known as a HackerGuardian 'Plug-in'. Each individual plug-in is written to test for a specific vulnerability. These can be written to actually exploit the vulnerability or just test for known vulnerable software versions.

HackerGuardian is continuously updated with the latest plug-in vulnerability tests via a direct feed available to all PCI Scanning Service subscribers - providing up to the second security against the latest vulnerabilities. At the moment there are over 30,000 with more being developed and added weekly.

This area enables the administrator to choose which plug-ins are deployed during a scan. Plug-ins can be enabled or disabled by their family type basis.

To choose the vulnerability plug-in families, click the Vulnerability Plugins Settings link from the Advanced Options interface.



- Select the plug-in families you wish to deploy.

Note: You must select Custom Scan for the chosen plug-ins to be deployed, while **starting** / **scheduling** a scan.

- Click 'Save Changes' for your settings to take effect.

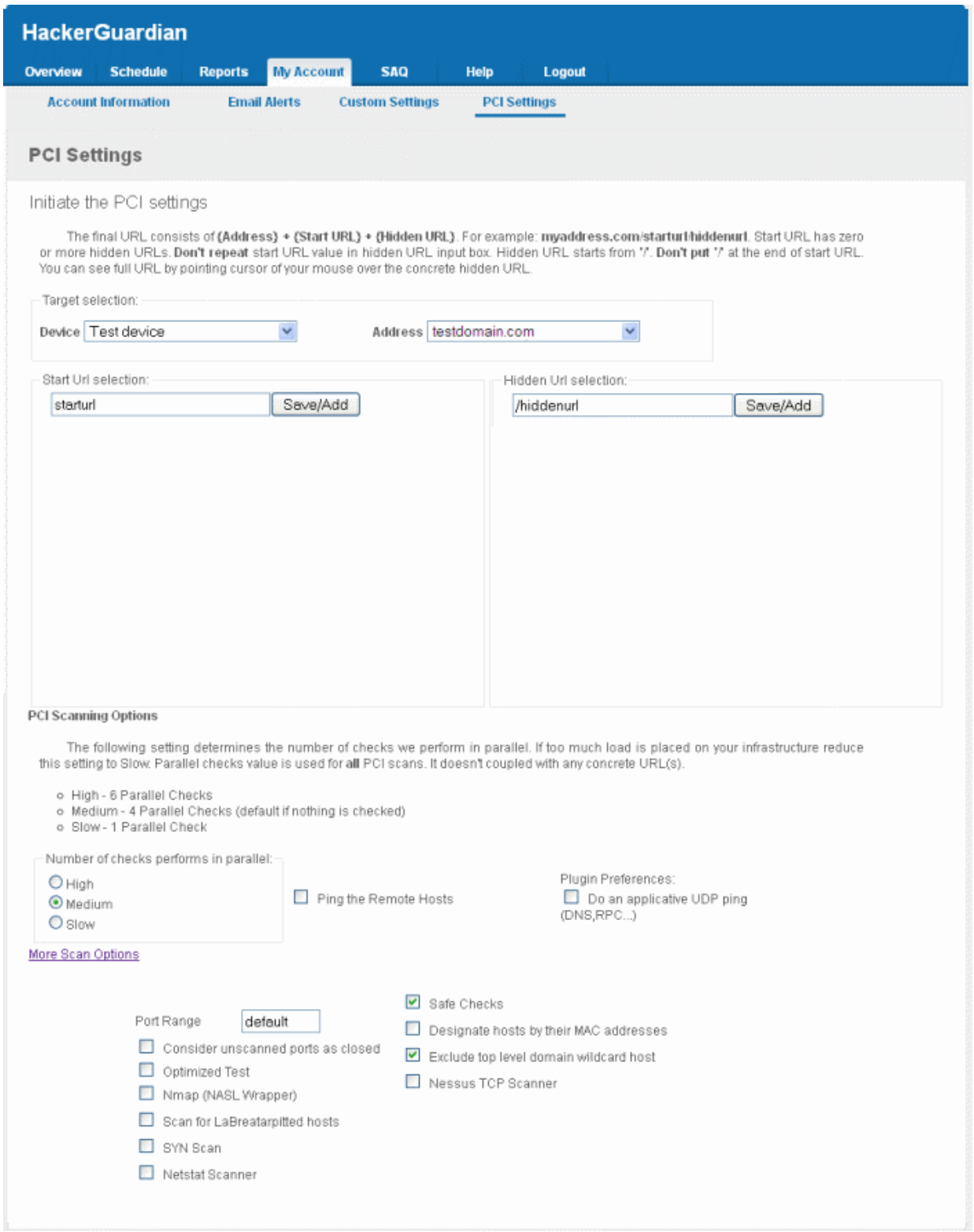
2.6.4. PCI Settings

The PCI Settings area enables the Administrator to customize the scan start page and to include hidden urls to be scanned for a Device and to specify the maximum number of concurrent scans.

- By default, the scanning is started from the main website page. If the index page of the website is different from the main site page, the Administrator has to specify the index page url as the Start url, in order to start the scanning from the index page.
- If the website(s) contained in the Device has hidden webpages, which are not linked from any other active page. Then the crawler will not be able to find them and include them for scanning. These hidden pages are to be scanned, HackerGuardian allows you to manually add them to the device for scanning.

To access the PCI Settings area

1. Switch to 'My Accounts' area of the HackerGuardian interface.
2. Click the 'PCI Settings' link in the 'My Accounts' area



This area allows the Administrator to:

- Specify the target urls, including hidden urls to be scanned;
- Specify the maximum number of allowed concurrent scans.

2.6.4.1. Specifying target URLs for scanning

1. Select the HackerGuardian Device for which the PCI Settings are to be customized from the Device drop-down.
2. Select the IP Address/Domain contained in the Device.
3. Enter the start page or index page of selected domain in the StartUrl selection textbox and click Save/Add.

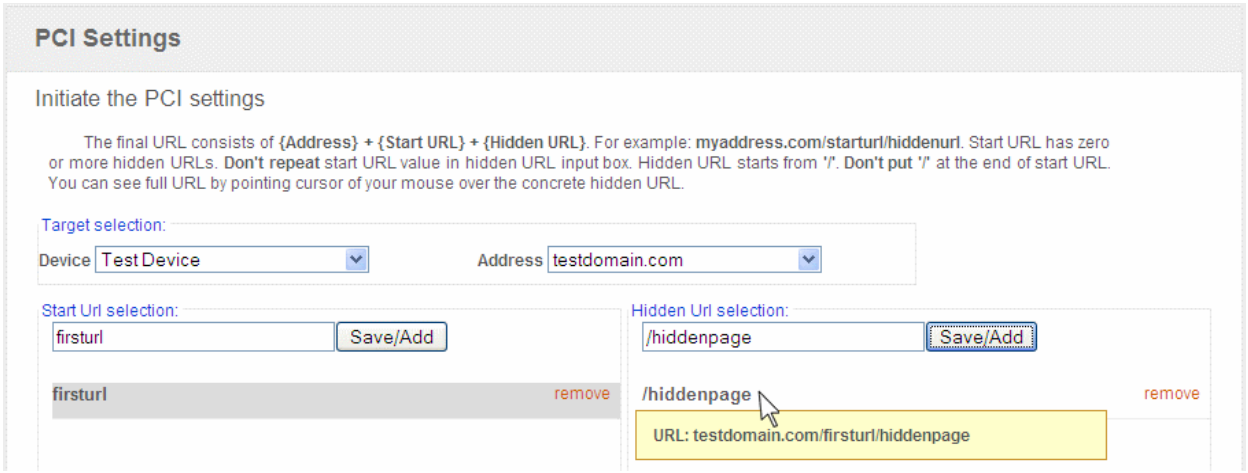
Note: The domain name need not be repeated and the startpage should not be ended with a "/" . If this field is left blank, the scanning will be started from the main website page.

For example, if the index page of the domain testdomain.com is www.testdomain.com/starturl/index.html, just enter "starturl" in the Start Url selection textbox.

4. Enter the hidden url in the Hidden Url selection text box and click Save/Add.

Note: The start page url should be mentioned for each hidden url. The hidden url should be prefixed with a "/" . The domain name and the full path need not be repeated.

For example, if the hidden page of the domain testdomain.com/starturl is www.testdomain.com/starturl/hiddenpage, just enter "/hiddenpage" in the Hidden Url selection textbox. Placing the mouse cursor over the added hidden url will display the full path.



5. Repeat the process for adding the start url and the hidden url for each hidden page in the website.

2.6.4.2. Setting Maximum Number of Allowed Concurrent Scans

Select the High, Medium or Slow radio buttons to specify the maximum number of concurrent scans. The number of allowed parallel checks are as given below:

High - Six Parallel Checks

Medium - Four Parallel Checks (default)

Slow - 0ne check at a time

Tip: Lower the number of concurrent scans, faster will be the process.

Scanning Options

Click the 'More Scan Options' link to view all the scanning options available.

This area enables administrators to configure general options pertaining to the scans. The settings chosen in this area will apply to any scan performed on selected device in the 'Overview' and 'Scheduled Scans' areas.

Scan Option	Element Type	Description
Ping the Remote Hosts	*Check box*	Pings the remote hosts through TCP connection and reports to the plug-ins knowledge base on whether the remote host is dead or alive. This sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYNACK.
Consider unscanned ports as closed	*Check box*	Ports that are not specifically scanned will be assumed as in closed state.
Do an applicative UDP ping (DNS,RPC...)	*Check box*	Performs a check if the host is up by sending a single UDP packet. The host is up if another UDP packet is returned or if an ICMP port unreachable message is returned.
Port Range	*Text box*	Set the range of ports to be scanned. A special value of default is allowed which scans port 1-15000. To scan all TCP ports on the target host, enter '1-65535'. Enter single ports, such as "21, 23, 25" or more complex sets, such as "21, 23, 25, 1024-2048, 6000", or enter "default" to scan default ports.
Optimized Test	*Check box*	Allows the scan to be optimized by only performing tests if information previously collected indicates a test is relevant. When disabled all tests are performed.
Nmap (NASL Wrapper)	*Check box*	Runs nmap(1) to find open ports.
Scan for La Breatarpitted hosts	*Check box*	Performs a labrea tarpit scan, by sending a bogus ACK and ACK-windowprobe to a potential host. Also sends a TCP SYN to test for non-persisting lebrea machines.
SYN Scan	*Check box*	Performs a fast SYN port scan by computing the RTT (round trip time) of the packets moving back and forth between host and the target and using the value to quickly send SYN packets to the remote host.
Netstat Scanner	*Check box*	Runs netstat on the remote machine to find open ports.
Safe Checks	*Check box*	Some checks are potentially harmful to the target host being scanned. When this option is enabled scans which may harm the target host are not performed. This option should be disabled to perform a full scan.
Designate hosts by their MAC address	*Check box*	This option will identify hosts in the scan report by their Ethernet MAC address rather than their IP address. This is useful for networks in which DHCP is used.
Exclude top level domain wildcard hosts	*Check box*	Excludes the hosts whose addresses are returned by a wildcard on some top level domains or the web server.

Nessus TCP Scanner	*Check box*	Enables classical TCP port scanner. It shall be reasonably quick even against a firewalled target. Once a TCP connection is open, it grabs any available banner for the service identifications. TCP scanners are more intrusive than SYN (half open) scanners.

2.7. Scheduled Scans

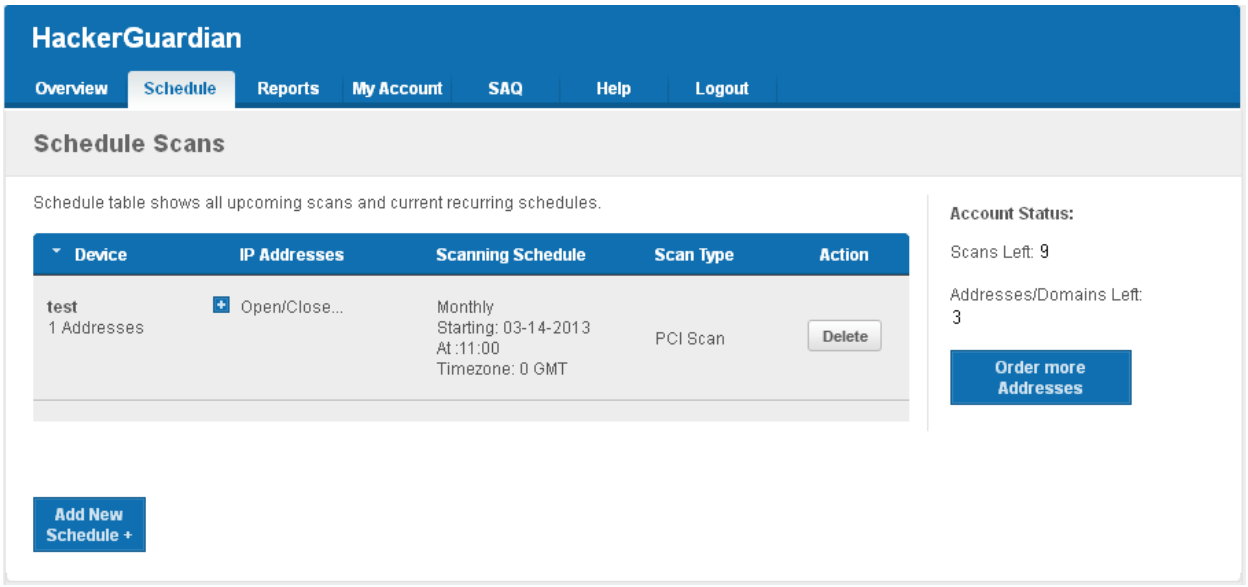
Comodo HackerGuardian features a highly customizable scheduler that lets you timetable scans to run at a time that suits your preference. HackerGuardian automatically commences the selected type of scan on the selected devices/IPs/Domains.

You can choose to run scans at a certain time on a daily, weekly, monthly or on a custom interval basis. HackerGuardian gives you the power to choose, allowing you to get on with more important matters with complete peace of mind.

HackerGuardian vulnerability scans can be scheduled to run:

- At a specific date and time;
- On a recurring basis at daily, weekly, monthly or user specified intervals.

To access the Scheduled Scan management interface, click on the 'Schedule' tab in the Navigation bar.



The 'Scheduled Scans' area displays the list of existing schedules. The following table provides description of information columns in this area.

Column	Description

Device	Displays the name of the device upon which the scan is scheduled.
IP Address	Displays all the associated domains (e.g. www.domain.com) or IP addresses that administrator specified for the device. Click the '+' button beside 'Open/Close...' to view the list of IPs and the Domains.
Scanning Schedule	Displays a summary of the scan schedule including details on recurrence period, start time etc.
Scan Type	Displays the selected scan type.
Action	Enables the Administrator to remove the schedule.

2.7.1. Adding a New Scan Schedule

1. Click 'Add New Schedule+'. The schedule options will be displayed.
2. Select the type of scan to be run as per the schedule from the 'Select scan type' drop-down box.

3. Select the device from the 'Select Device(s)' drop-down box.

4. Select the IPs/Domain pertaining to the selected device from Select IP(s) box. If you wish to scan all the IPs/Domains, select 'All'.

5. Select the start date for the scan schedule by clicking the calendar icon beside 'Set Start Date' text box.

6. Select the recurrence period.

- *Weekly* - The scan will be performed once in a week on the specified day and time.
- *Monthly* - The scan will be performed once in a month on the specified date and time.
- *Quarterly* - The scan will be performed once in three months on the specified date and time.
- *Every N days* - Scan will be performed once for every n days from the start date. For example, if you specified 2 then the scan will be performed on alternate days.

7. Select the start time from the 'Set Start Time' drop-down combo box. The scan will be started on the set time at the scheduled dates according to your time zone set in the 'My Account' area.

8. Click 'Save' to to apply your schedule.

Repeat the process for adding more schedules for running scans on other devices/IPs/Domains as per your convenience.

The scans will run on the selected device on date(s), time(s) and interval that you specified.

Notes about Scan types and Devices

- PCI Scans cannot be scheduled to run on 'Internal Devices' (devices inside your LAN devices have no external IP addresses). To scan an Internal device, you must use 'Custom Scan'
- Selecting 'PCI Scan' will launch a vulnerability scan according to PCI scanning guidelines. PCI Scan are 'predetermined' by the PCI DSS and are not user configurable. Full reports are available in the 'Reports' area.
- The composition of a 'Custom Scan' is defined by the administrator in **My Account > Custom Settings** area.

2.8. HackerGuardian Reports

At the end of each PCI/Custom scan, HackerGuardian produces a vulnerability report and an executive report for each IP/Domain scanned and an executive report and a chart depicting the scan results in pie diagrams for the network device scanned.

The compliance status for each device is set as **Compliant** or **Non-Compliant** based on the discovery of potential security flaws on the device/IP/Domain.

The security flaws or the vulnerabilities are rated based on their severity levels. The rating of each vulnerability is indicated by the color of title bar of the respective report. The following table shows the official PCI severity ratings.

Rating	CVSS Score	Vulnerability	Severity Level	Scan Result
Red	7.0 - 10	Security Hole	High	Fail PCI Scan
Orange	4.0 - 6.9	Security Warnings	Medium	Fail PCI Scan

Blue	0 - 3.9	Security Notes	Low	Pass PCI Scan

Based on the ratings, HackerGuardian categorizes the vulnerabilities as Security Holes, Security Warnings and Security Notes.

Security Holes	A vulnerability, whose severity level is more than three or 'High', is identified as a Security Hole. To pass a PCI Compliance scan, no holes are to be found during the scan. If any holes are found, the merchant or the service provider must re mediate the identified problems and re-run the scan until the compliance is achieved.
Security Warnings	A vulnerability, whose severity level, is more two or 'Medium', is indicated as a Security Warning. To pass a PCI Compliance scan, no warnings are to be found during the scan. If any warnings are found, the merchant or the service provider must re mediate the identified problems and re-run the scan until the compliance is achieved.
Security Notes	A vulnerability, whose severity level, is more one or 'Low', is indicated as a Security Note.

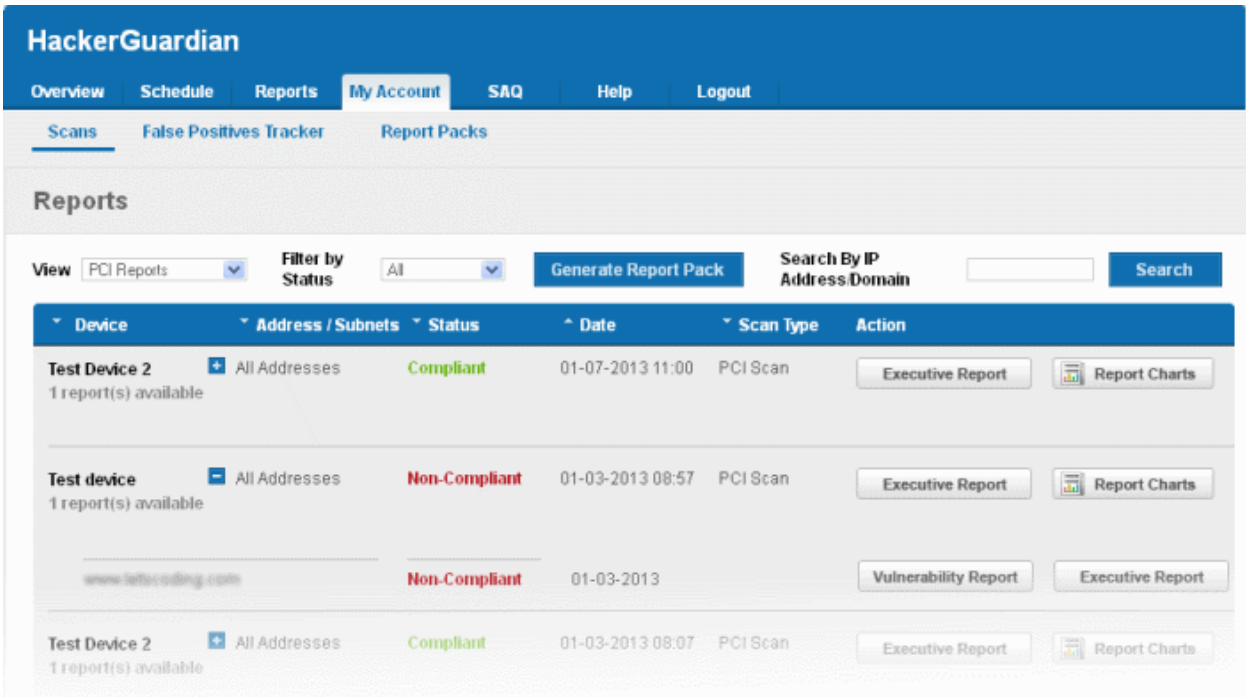
Each HackerGuardian report indicates the Security Holes, Security Warnings and Security Notes found on each device/IP/Domain and also provides solution for remediation.

The Scan Reports produced from the PCI scans can be assessed from the 'Reports' area of the HackerGuardian interface, displayed by clicking the 'Reports' tab from the Navigation bar. From this interface, you can:

- View the scan reports
- Submit False Positives
- Track the status of Submitted False Positives
- Download the entire reports as a zip file by clicking the 'Generate Report Pack' button.

2.8.1. View Scan Reports

Clicking the 'Scans' link in the Reports area opens the list of the scan reports produced by HackerGuardian at the end of each scan.



At the end of each scan HackerGuardian produces three types of reports.

- **Executive Report** - Executive Reports provide an overview of the security status of multiple hosts - allowing administrators to gain an overview of the health of their entire network. **Click here for More Details.**
- **Charts_Page** - The charts page displays the scan summary and the bar-graphs and pie diagrams indicating the proportions of vulnerabilities according to their categories. **Click here for More Details.**
- **Vulnerability Report** - Vulnerability Reports are a detailed overview of scans on a single IP/Domain. They include a prioritized list of the vulnerabilities found, expert remediation advice and thousands of cross-referenced online advisories. **Click here for More details.**

Tip : The vulnerability reports and the PCI Compliance reports can be converted into pdf format by clicking the link 'Print in PDF' from the Additional Actions area as shown below.


Additional Actions
Print in PDF
Back to All Reports

2.8.1.1. Filtering Options

The administrator can filter the reports listed, based on the scan type, status or even the reports pertaining to a specific IP or domain. The table below describes the filtering options available in this interface.

Filter	Description
View	Enables to filter the reports based on the scan type. E.g. to view only the PCI scan reports, select 'PCI Reports' from the drop-down menu.
Filter by Status	Enables to filter the reports based on success or failure of the scan results.
Search by IP/Domains	Enables to filter the reports pertaining to specific IP or Domain. The administrator can enter the IP address or the Domain name and the reports only for those will be listed.

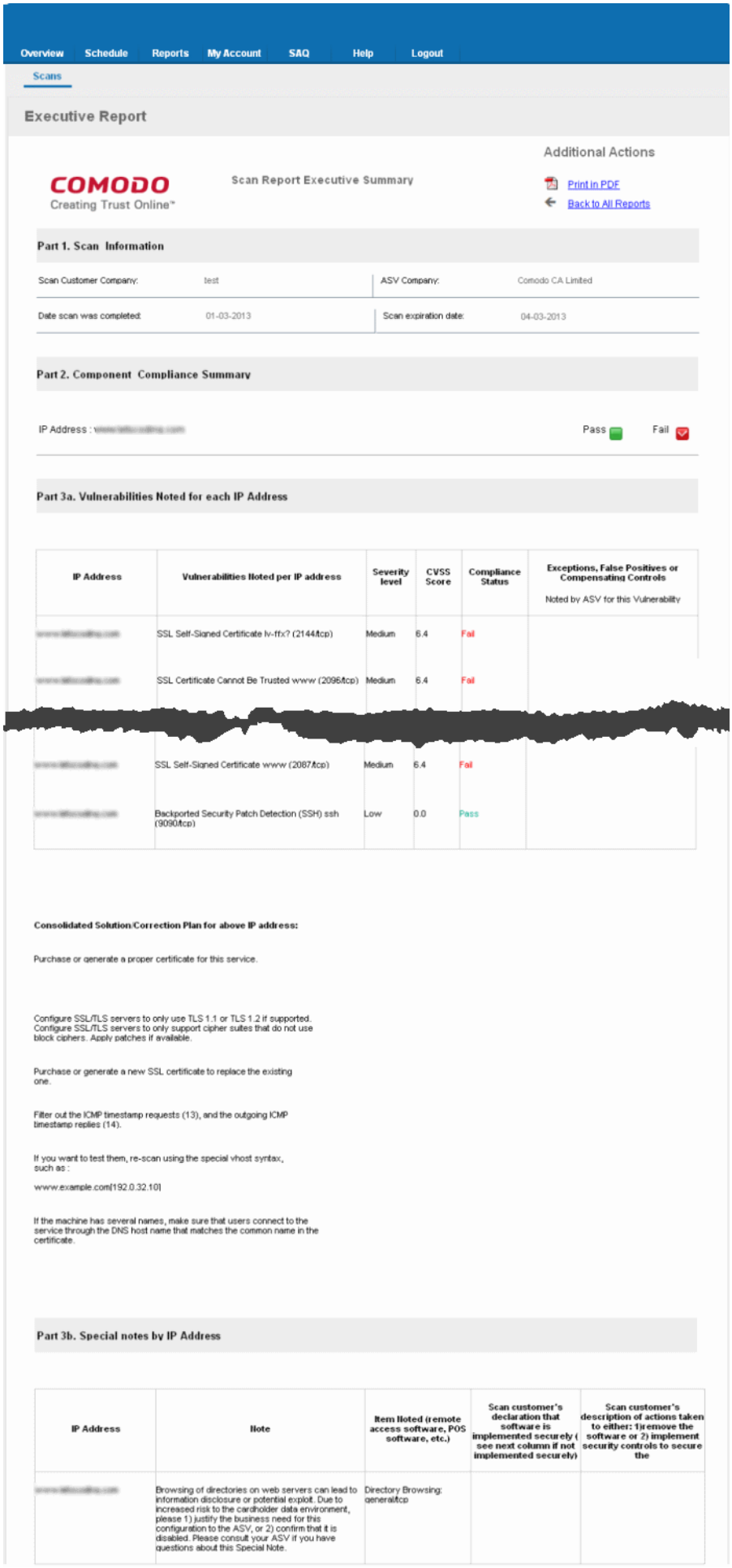
2.8.2. Executive Report

An Executive Report is a condensed view of the information available by viewing reports individually, but present it in an more easily digested manner - allowing admins to quickly pick out where insecurities lie and to assess then investigate any surges in the trends.

To view an executive summary of a device, click the Executive Report button in the row.

Tip: You can also click Executive Report button beside the device name from the 'Device List' area to view the report.

An example of an executive report is shown below.



Overview Schedule Reports My Account SAQ Help Logout

Scans

Executive Report

Additional Actions

Print in PDF

Back to All Reports

COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	test	ASV Company:	Comodo CA Limited
Date scan was completed:	01-03-2013	Scan expiration date:	04-03-2013

Part 2. Component Compliance Summary

IP Address : [redacted] Pass Fail

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
[redacted]	SSL Self-Signed Certificate lv-ffx? (2144/tcp)	Medium	6.4	Fail	
[redacted]	SSL Certificate Cannot Be Trusted www (2096/tcp)	Medium	6.4	Fail	
[redacted]	SSL Self-Signed Certificate www (2087/tcp)	Medium	6.4	Fail	
[redacted]	Backported Security Patch Detection (SSH) ssh (9090/tcp)	Low	0.0	Pass	

Consolidated Solution/Correction Plan for above IP address:

Purchase or generate a proper certificate for this service.

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Purchase or generate a new SSL certificate to replace the existing one.

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.

Part 3b. Special notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1)i emove the software or 2) implement security controls to secure the
[redacted]	Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	Directory Browsing: general/tcp		

The Executive report contains the following information:

1. Scan Information	-	Provides information on the Company name of the subscriber, scanning vendor (Comodo CA Ltd.,), date of scan and the scan expiry date.
2. Component Compliance Summary	-	Provides an at-a-glance indication of PCI Compliance status of your systems.
3a. Vulnerabilities noted for for each IP address	-	Provides details on types of vulnerabilities identified for each IP address, with their severity level, CVSS base score and compliance status. If no vulnerabilities with a CVSS base score greater than 4.0 (named 'security holes' in HackerGuardian') are detected then the scanned IP addresses, hosts and Internet connected devices have passed the test and the report can be submitted to your acquiring bank. If the report indicates 'Fail' on any of the IP address, then the merchant or service provider must re mediate the identified problems and re-run the scan until compliancy is achieved.
3b. Special Notes by IP Address	-	Provides any special details or notes of the vulnerabilities found and any special declarations given by the subscriber.

If the Component Compliance Summary section of your HackerGuardian Executive Report indicates a failure in the Compliancy Status, then vulnerabilities with a CVSS base score greater than 4.0 were discovered on your externally facing IP addresses. The accompanying **Vulnerability Report** contains a detailed synopsis of every vulnerability prioritized by threat severity. Each discovered vulnerability is accompanied with solutions, expert advice and cross referenced links to help you fix the problem. You should fix all vulnerabilities identified as a 'Security Hole'.

Furthermore, each report contains a condensed, PCI specific, '**Mitigation Plan**' - a concise, bulleted list of actions that you need to take to achieve compliance.

After completing the actions specified in the Mitigation Plan you should run another scan until the report returns a '**Compliant**' status.

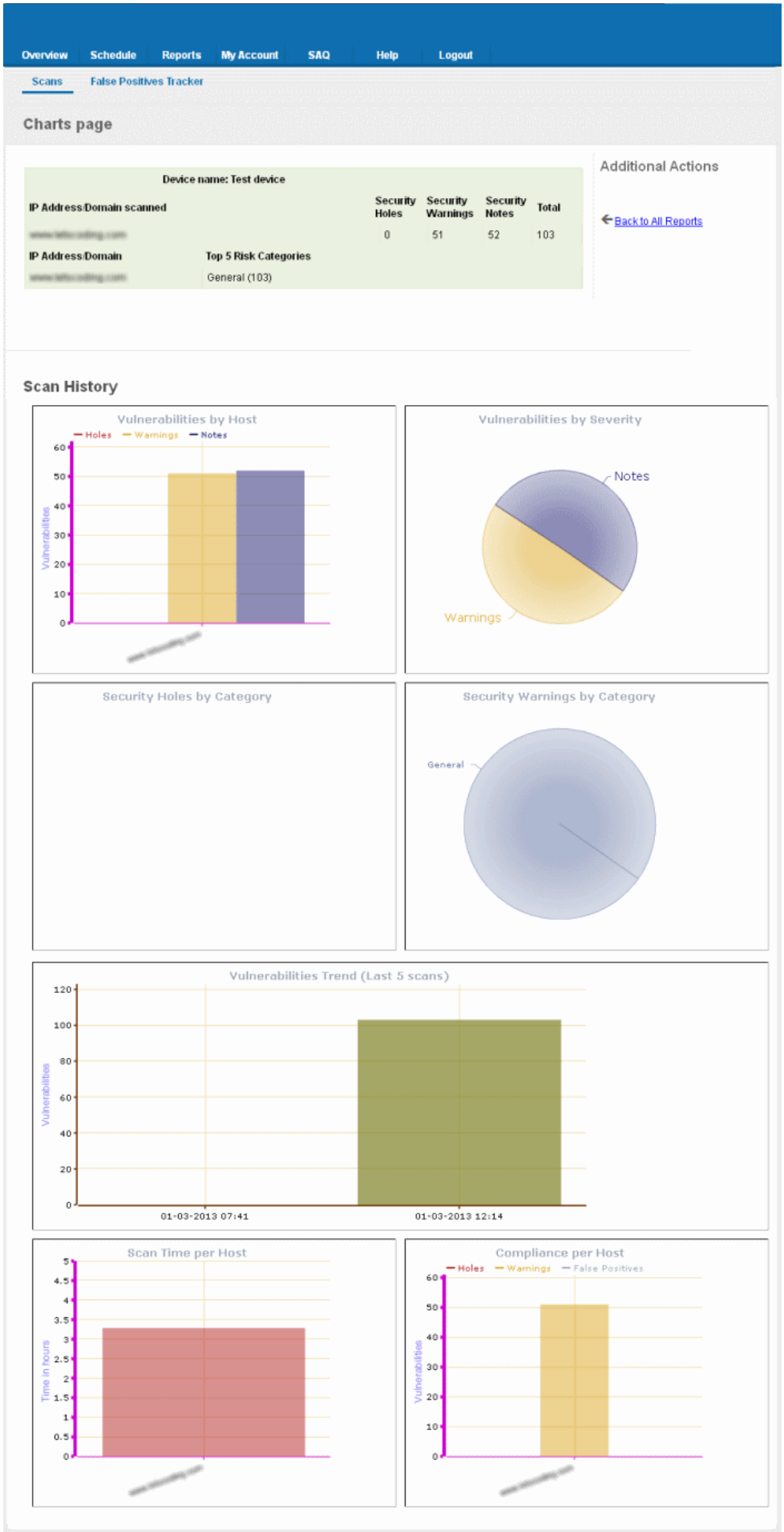
2.8.3. Charts Page

The Charts Page contains at-a-glance summary of the scan results on the device at the top and graphical representations of proportions of identified vulnerabilities according to their categories.

To view the Chart Page of a Device, click the charts page button  in the row of the Device.

Tip: You can also click the charts page button beside the Device name from the 'Device List' area to view the page.

An example of the Charts Page is given below.


Overview
Schedule
Reports
My Account
SAQ
Help
Logout
Scans
False Positives Tracker
Charts page
Device name: Test device
IP Address/Domain scanned
Security Holes
Security Warnings
Security Notes
Total
0
51
52
103
IP Address/Domain
Top 5 Risk Categories
General (103)
Additional Actions
Back to All Reports
Scan History
Vulnerabilities by Host
Holes
Warnings
Notes
Vulnerabilities
Vulnerabilities by Severity
Notes
Warnings
Security Holes by Category
Security Warnings by Category
General
Vulnerabilities Trend (Last 5 scans)
01-03-2013 07:41
01-03-2013 12:14
Scan Time per Host
Time in hours
Compliance per Host
False Positives

2.8.3.1. Summary

The summary table provides the list of IP addresses/Domains pertaining to the device scanned and the number of Security Holes, Security Warnings and Security Notes identified in each IP/Domain.

Device name: Test device

IP Address/Domain scanned		Security Holes	Security Warnings	Security Notes	Total
www.letscoding.com		0	51	52	103
IP Address/Domain	**Top 5 Risk Categories**				
www.letscoding.com	General (103)				

Also the table contains a list of flaws (with no. of flaws in parenthesis) which fall under top five risk categories, for each IP/domain scanned.

2.8.3.2. Scan History

The scan history section contains bar-graphs and pie diagrams indicating the proportions of vulnerabilities according to their categories.

Vulnerabilities by Host - A graphical representation of the information regarding the security holes found, security warnings, and security notes per host. Each category is represented by a different color. Pointing the mouse cursor over a bar in the graph displays the count of the respective item found. The graph enables administrators to gain both an overview of the overall of health their network and to monitor the security of individual hosts within that network.

Vulnerabilities by Severity - A pie-diagram representation of proportions of security holes, security warnings, and security notes found for the entire device. Pointing the mouse cursor over a sector in the diagram displays the percentage proportion of the respective item found.

Security Holes by Category - A pie-diagram representation of proportions of security holes of different categories like Trojan Horses, file R/W exploits, Remote Procedure Call (RPC) exploits etc., found for the entire device. Pointing the mouse cursor over a sector in the diagram displays the number and percentage proportion of the respective item found.

Security Warnings by Category - A pie-diagram representation of proportions of security warnings of different categories like Firewall exploits etc., found for the entire device. Pointing the mouse cursor over a sector in the diagram displays the number and percentage proportion of the respective item found.

Vulnerabilities Trend - A graphical representation of the comparison of the vulnerabilities found in the IPs/Domains of the device during the last five scans. This gives the trend of the reduction in the number of vulnerabilities in successive scans because of the remediation actions taken at the end of each scan. Each IP/Domain in a device is indicated with a different color. Pointing the mouse cursor over a bar in the graph displays the number of the vulnerabilities found in the respective IP/Domain in the respective scan. This graph also indicates the administrator on the frequency of the scans and enables to check whether scans are being conducted according to their pre-defined scan schedule.

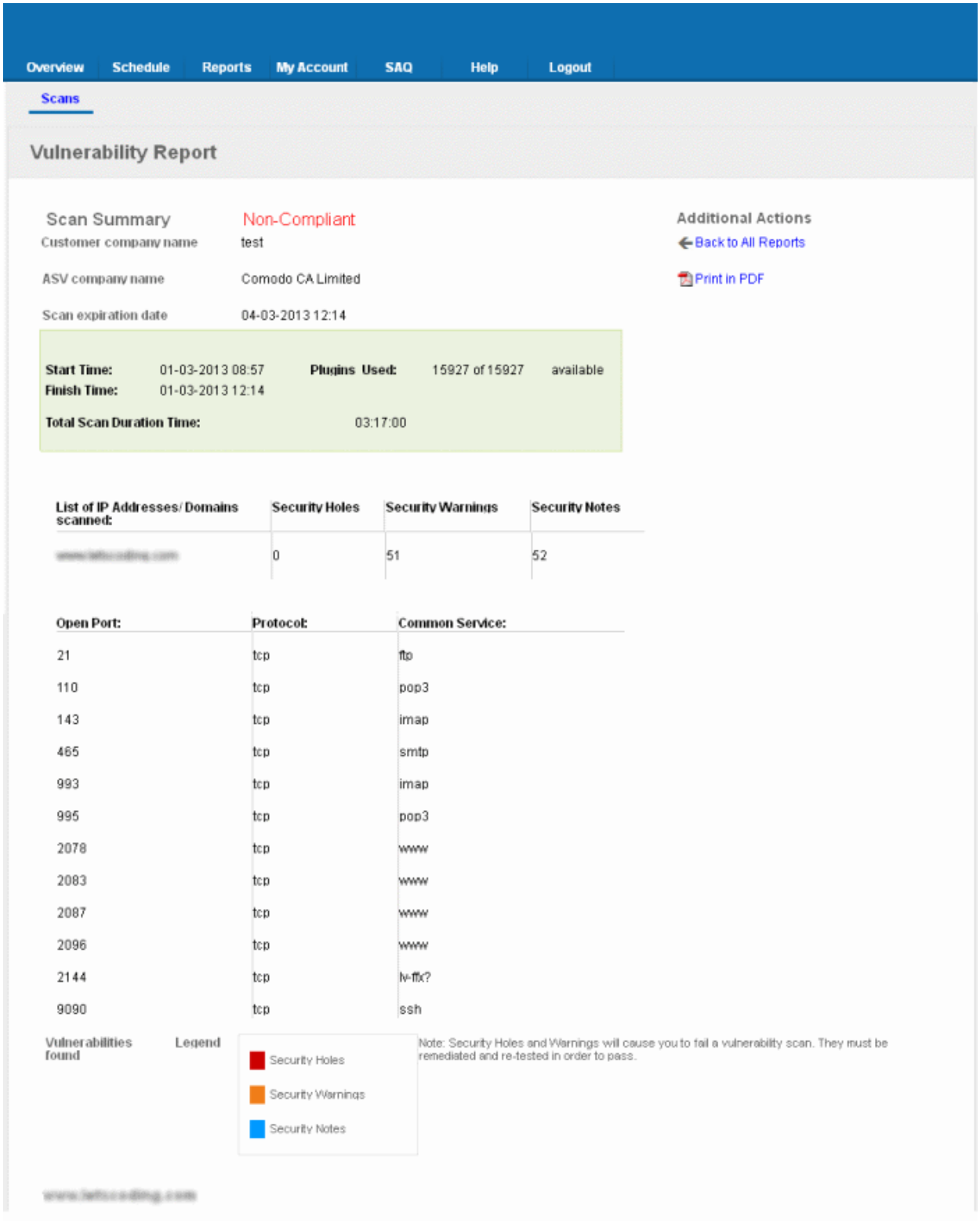
Scan Time per Host - A graphical representation of the time taken for scanning each IP/Domain in the device. Pointing the mouse cursor over a bar in the graph displays the time taken fr the IP/Domain in hours.

2.8.4. Vulnerability Report

A Vulnerability Report provides a detailed overview of scan results on a single IP/Domain. It includes a prioritized list of the vulnerabilities found, expert remediation advice and thousands of cross-referenced online advisories.

To view a Vulnerability Report of a IP/Domain, click the '+' beside the respective device and then click the 'Vulnerability Report' button in the row of the respective IP/Domain.

Tip: You can also click Vulnerability Report button beside the IP/Domain name from the 'Device List' area to view the report.



The Vulnerability Report consists of a summary of the scan details and the prioritized list of the vulnerabilities found.

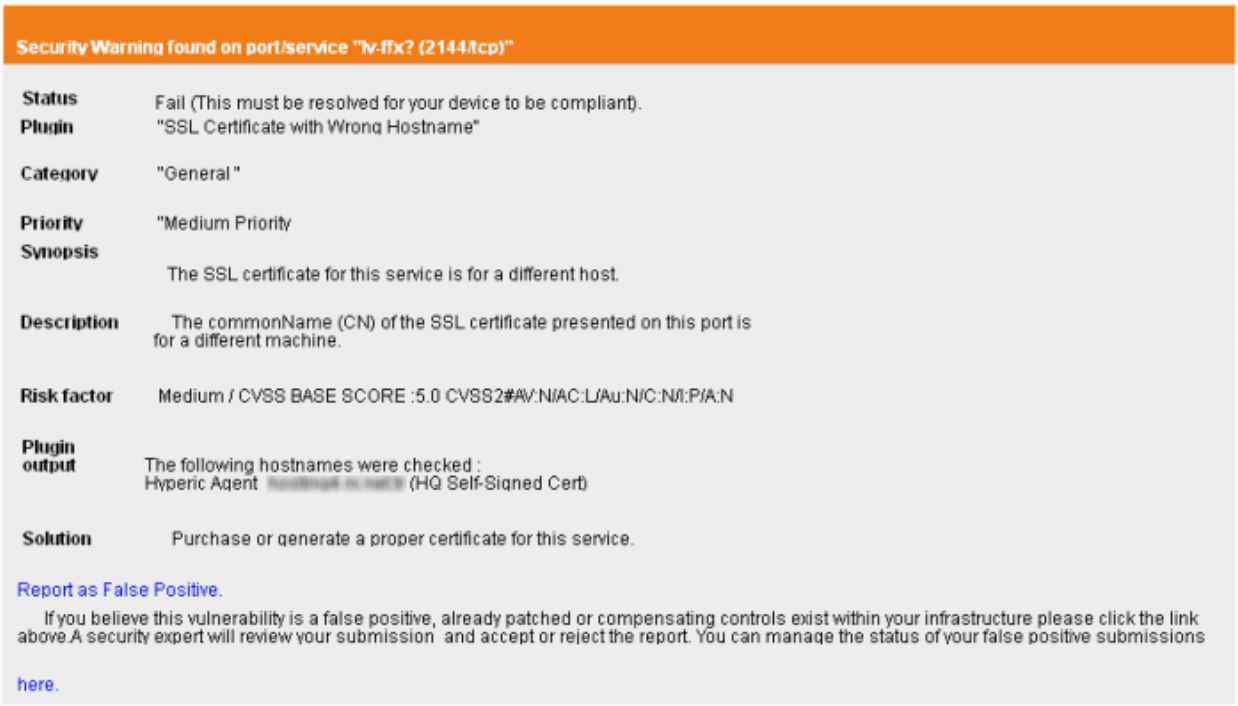
2.8.4.1. Scan Summary

The scan summary contains the following details:

- **Company Name** - The Company name of the subscriber.
- **ASV company name** - Name of the approved scanning vendor (Comodo CA Ltd.,)
- **Scan expiration date** - The expiry date of the scan for which the report was generated.

- **Start Time** - The date and time at which the scan was started.
- **Finish Time** - The date and time at which the scan was completed.
- **Total Scan Duration Time** - The total time taken for the scan.
- **Plugins Used** - The number of vulnerability plug-ins deployed during the scan.
- A table providing the number of Security Holes, Security Warnings and Security Notes identified the IP/Domain.
- A list of open ports detected on the IP/Domain and their respective communication protocols and dedicated services.

Following the scan summary, the identified vulnerabilities are listed with their descriptions, priority, the plug-in that identified the flaw, risk factor, expert advices for remediation etc. An example is shown below.



The title bar indicates the type of the vulnerability and the port/service in which it is identified.

Status - Indicates the status of the device whether it has passed or failed.

Plugin The vulnerability plug-in that has detected the vulnerability.

Category - The category of the flaw that is responsible for the vulnerability.

Priority - Indicates the priority at which the vulnerability has to be re mediated.

Synopsis - The Synopsis in the report provides a short description of the vulnerability. For example: if the protocol is encrypted, if debugging is enabled etc.

Description - A detailed description of the vulnerability and its effects. This section also contains links for additional reading about the vulnerability.

Risk Factor - Shows the severity of the vulnerability according to the CVSS score. The NVD provides severity rankings of "Low", "Medium", and "High" in addition to the numeric CVSS scores but these qualitative rankings are simply mapped from the numeric CVSS scores:

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Additional Information - Provides CVE index of standardized names for vulnerabilities and other information security exposures, BID numbers and other references to the vulnerability.

CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

Examples of universal vulnerabilities include:

- phf (remote command execution as user "nobody")
- rpc.ttdbserverd (remote command execution as root)
- world-write able password file (modification of system-critical data)
- default password (remote command execution or other access)
- denial of service problems that allow an attacker to cause a Blue Screen of Death
- smurf (denial of service by flooding a network)

Examples of exposures include:

- running services such as finger (useful for information gathering, though it works as advertised)
- inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
- running services that are common attack points (e.g., HTTP, FTP, or SMTP)
- use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)

Each CVE name includes the following:

- CVE identifier number (i.e., "CVE-1999-0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

Solution - Provides expert advices on the action to be taken by giving a set of rules to be configured for the specific port/service vulnerability. This gives the best suited remediation measure for the vulnerability found.

2.8.4.2. Mitigation Plan

HackerGuardian will conduct an in-depth audit of your network to detect vulnerabilities on your network and web-server. If your servers fail the test, you will find lots of helpful advisories in the scan report that will help you patch the security holes.

Mitigation Plan

You must undertake the following remedial actions or provide us with the relevant information if you think the vulnerabilities are already patched or if compensating controls exist:

- Disable the 'Maintain synchronization information' option from the Remote Info category of the advanced view of the Site Definition dialog box. In addition, remove the offending files if already created by the system.
- Modify the relevant CGIs so that they filter metacharacters, convert &lt and &gt to escape sequences
- Modify the relevant CGIs so that they filter metacharacters, convert &lt and &gt to escape sequences
- Upgrade to PHP version 5.2.10 or later.
- Upgrade to PHP version 5.2.11 or later.
- Add the following lines for each virtual host in your configuration file :
  RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
  RewriteRule .* - [F]
  Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.
  Plugin output :
  Nessus sent the following TRACE request :
  ---------- snip ---------- TRACE /Nessus431087684.html
  HTTP/1.1
  Connection: Close
  Host: www.mydomain.com
  Pragma: no-cache
  User-Agent: Mozilla/4.0 (compatible MSIE 6.0 Windows NT 5.0)
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
  Accept-Language: en
  Accept-Charset: iso-8859-1,*,utf-8

  ---------- snip ----------
  and received the following response from the remote server :
  ---------- snip ---------- HTTP/1.1 200 OK
  Date: Wed, 03 Mar 2010 23:37:08 GMT
  Server: Apache
  Connection: close
  Transfer-Encoding: chunked
  Content-Type: message/http

  TRACE /Nessus431087684.html HTTP/1.1
  Connection: Close
  Host: www.mydomain.com
  Pragma: no-cache
  User-Agent: Mozilla/4.0 (compatible MSIE 6.0 Windows NT 5.0)
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
  Accept-Language: en
  Accept-Charset: iso-8859-1,*,utf-8

  ---------- snip ----------
- In httpd.conf, set the 'UserDir' to 'disabled'.
- Upgrade to OpenSSH version 5.0 or later.
- Upgrade to OpenSSH version 5.0 or later.
- Upgrade to OpenSSH version 5.0 or later.
- Upgrade to OpenSSH 4.4 or later.
- Upgrade to OpenSSH 4.4 or later.
- Upgrade to OpenSSH 4.4 or later.

We recommend you undertake the following remedial actions:

- Upgrade to OpenSSH 4.2 or later.
- Upgrade to OpenSSH 4.2 or later.
- Upgrade to OpenSSH 4.2 or later.
- Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
- Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.
- Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

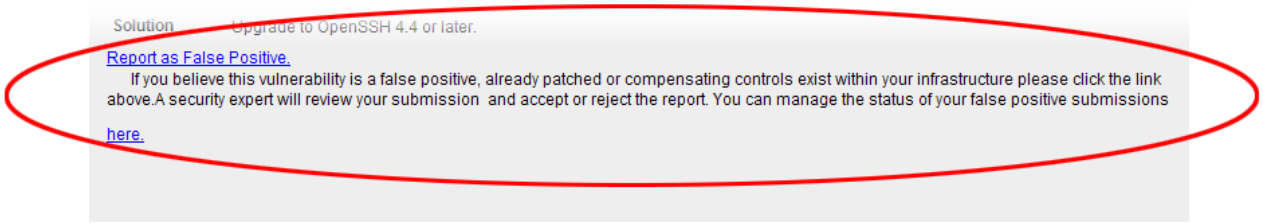
That's why EACH report contains a condensed, PCI specific, 'Mitigation Plan' - a concise, bulleted list of actions that you need to take to achieve compliance. The mitigation plan is available at the end of the list of the vulnerabilities.

Tip: You an directly view the mitigation plan by clicking the link Jump to Remediation Plan from the 'Additional Actions' area.

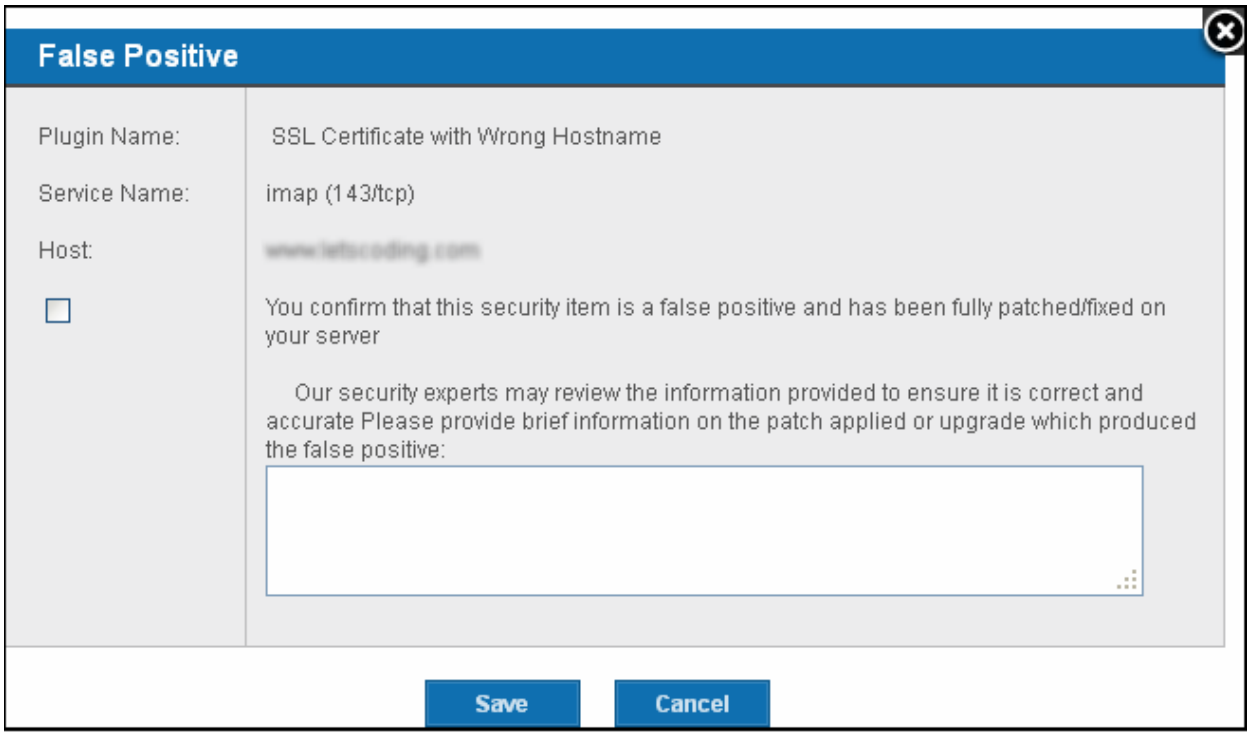
2.8.5. Reporting False Positives

A false positive exists when HackerGuardian incorrectly detects a Security Hole (vulnerability with a CVSS base score greater than 4.0) or if compensating controls exist elsewhere in the network's security infrastructure to offset or nullify the vulnerability.

Administrators have the ability to submit suspected false positives to Comodo from with the security advisory itself (see below)



If you think this is a legitimate false positive, click the 'Report as False Positive' link or here 'link' shown above. This will open the false positive reporting interface. (shown below).



- Next, check the box 'You confirm that this security item is a false positive and has been fully patched/fixed on your server'.
- **Important** - administrators must include information in the text box detailing the patch or compensating control that they have deployed. If this space is left blank then the request will be automatically rejected
- Click 'Save' to submit the report to the HackerGuardian technicians for analysis and verification. The advisory will contain the following message to indicate that your submission is under review:

Our support team will review the information provided to ensure it is satisfactory.

The administrator can check the status of the submitted false positive at any time. Click here for more details.

If Confirmed as false positive by our technicians - This security hole will no longer count against your IP address/Domain. Genuine false positives are *automatically* removed from the list of security holes from which your PCI report is derived.

Your **Host Compliancy Status** will be **automatically** updated in your **Executive Report**. - ***You do not need to run another scan.***

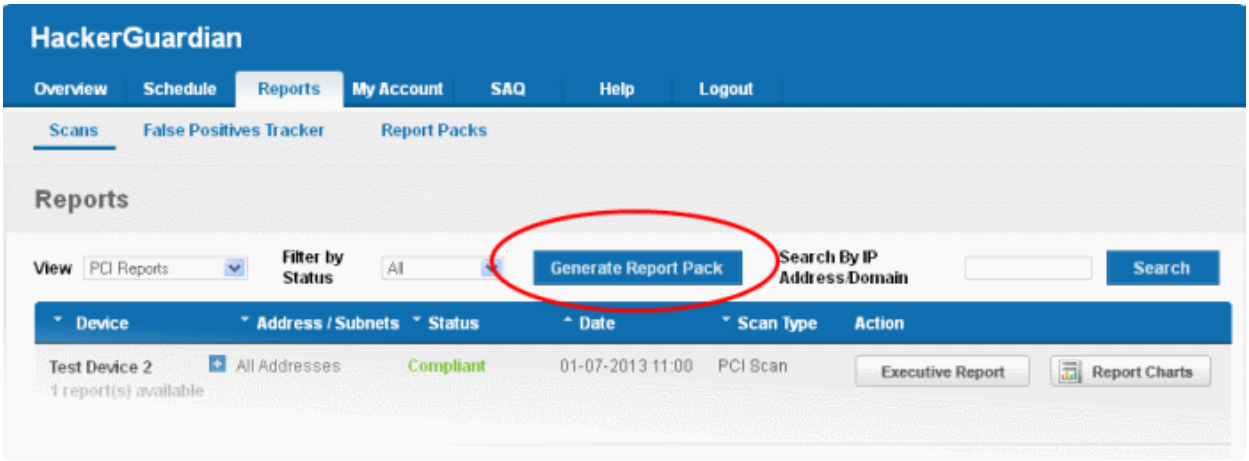
For example - If this false positive represented the only security hole on your host, then your PCI report will change from 'Not Compliant' to 'Compliant' and you can immediately download it.

2.8.6. Downloading Reports Pack

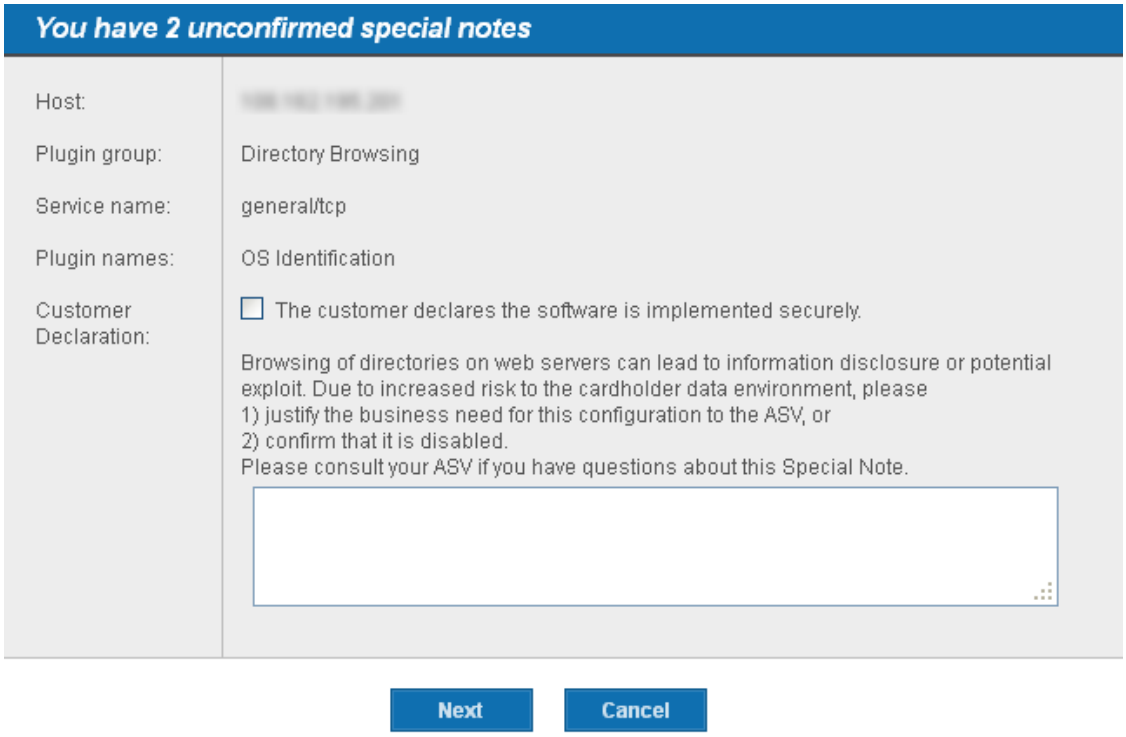
The Administrators can download all the reports in pdf format as a zip file by clicking the 'Generate Report Pack' button in the Reports > Scans interface.

The Report Pack will contain Executive Report, Vulnerability Report and the Attestation Scan Compliance report of the PCI scans executed within the past 90 days. These scan reports should be submitted to the acquiring bank or payment bank according to their instructions, to demonstrate compliance.

To download the report pack, click the 'Generate Report Pack' button from the 'Reports' area.

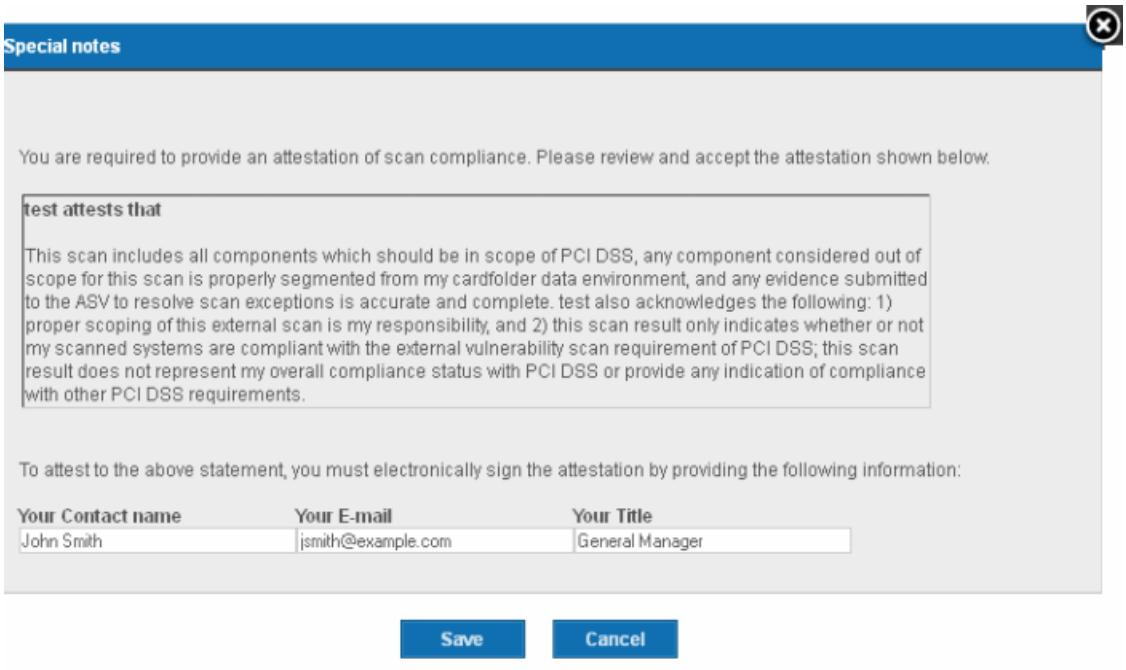


If some unresolved security notes are present in the report, the following warning will be displayed.



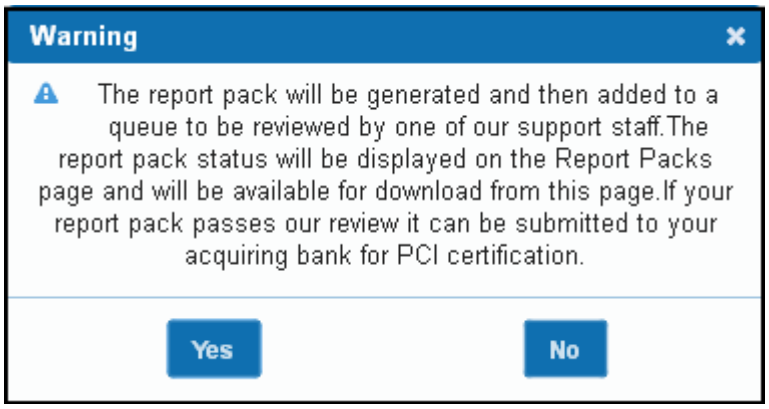
Address the issue or confirm that the security notes are taken care by selecting the check box and click 'Next'.

An attestation screen will appear.



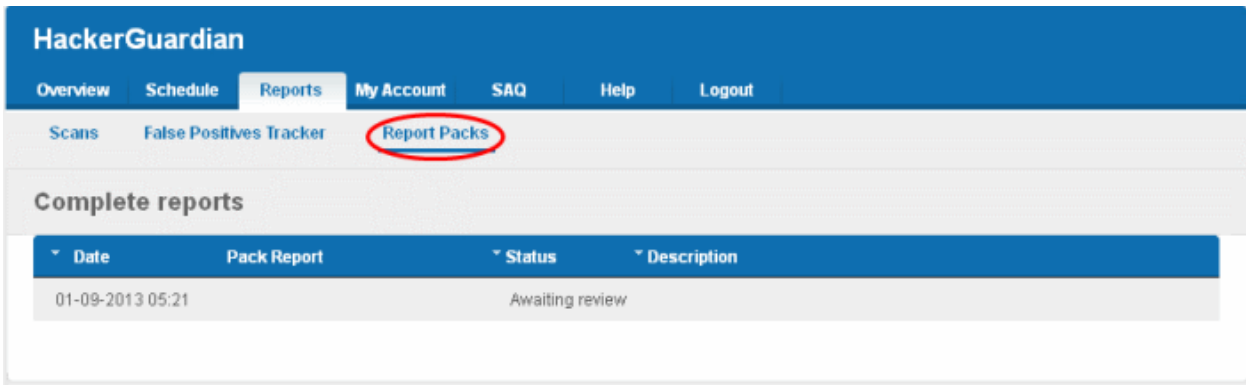
- Read the Attestation statement and fill your Contact name, email address and your role in the subscribing Organization, as a token of digitally signing the attestation form and click 'Next'.

Immediately, the report pack generation will be started. On completion, your report pack will be reviewed by our support staff and will be passed on for download. This will be indicated by a dialog.

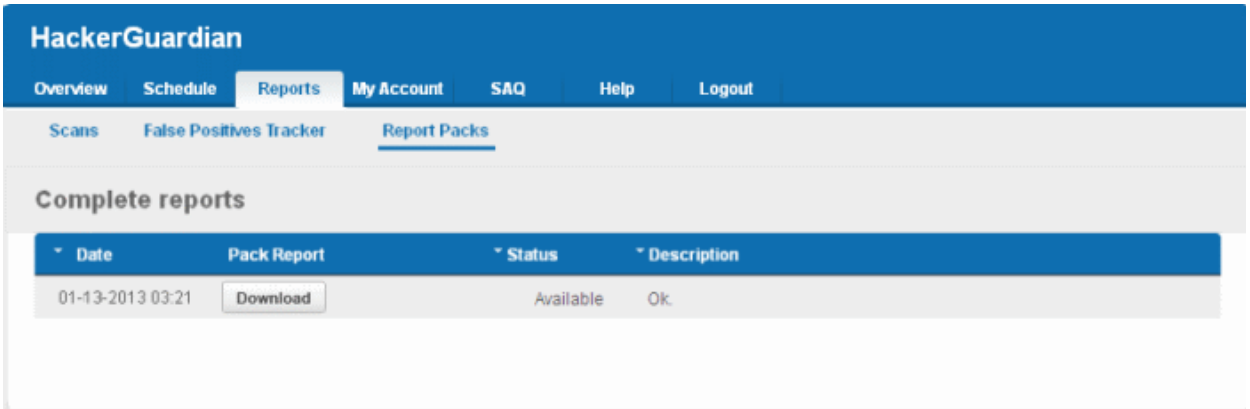


- Click 'Yes'.

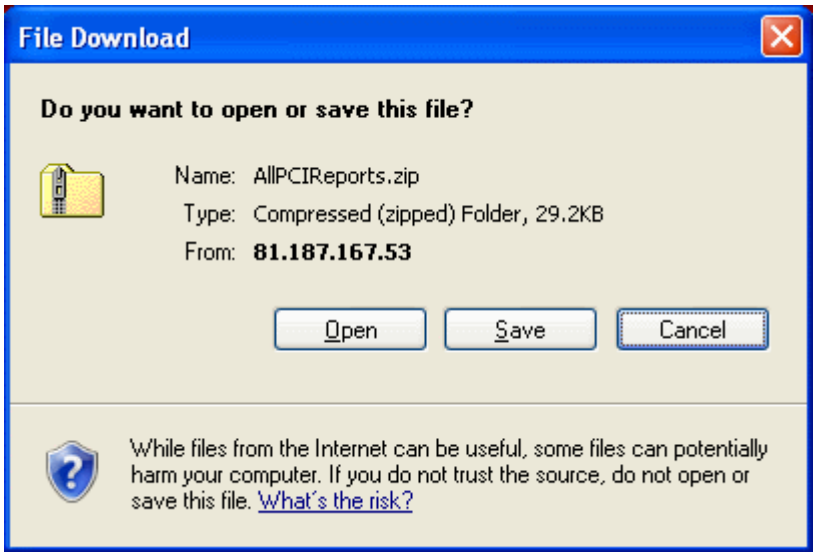
To check your report pack status, click the “Report Packs” tab in the 'Reports' area. The status of your requested report pack will be displayed.



Once the pack is generated and reviewed by our PCI DSS approved support staff, it will be available under the same tab for download.

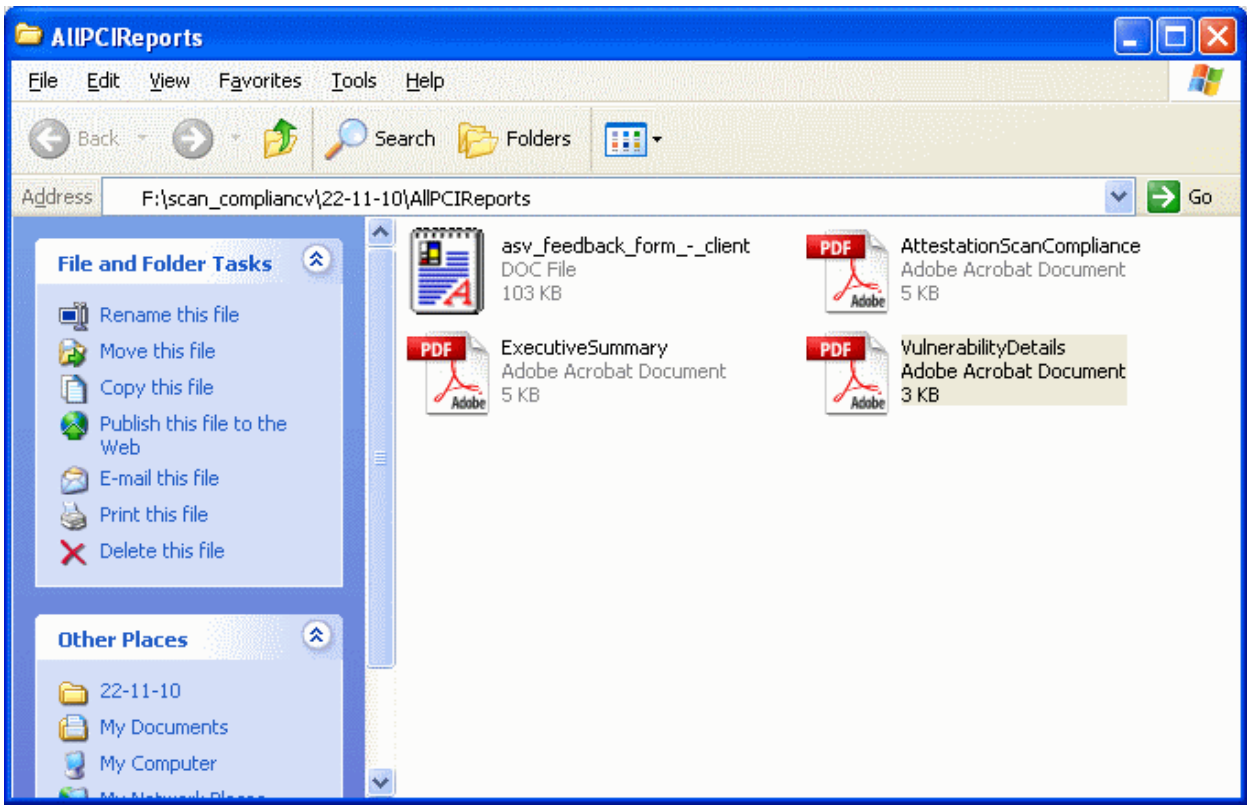


- Click the 'Download' button. The file download dialog will appear.



- Save the file in a desired location.

This report pack will contain pdf files of Attestation of Scan Compliance report, Executive Summary, and the Vulnerability Details and the of the PCI scans executed within the past 90 days.

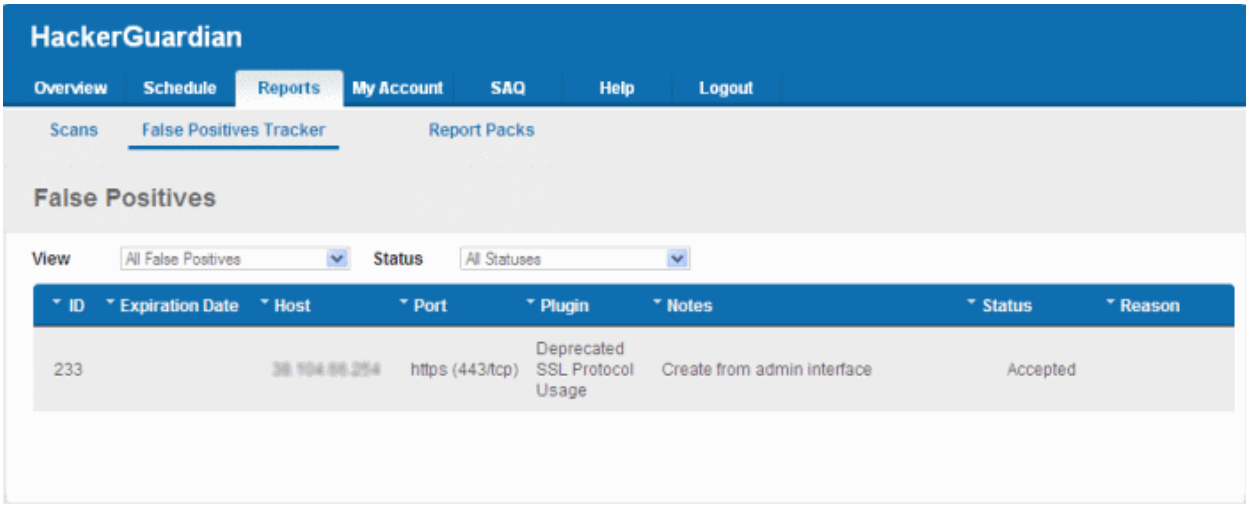


These scan reports should be submitted to the acquiring bank or payment bank according to their instructions, to demonstrate compliance.

Also, the report pack contains an ASV Feedback form to be filled up and sent to the PCI SSC at asv@pcisecuritystandards.org, as a feedback for the scanning service provided by Comodo, the Approved Scanning Vendor.

2.8.7. Tracking Status of Submitted False Positives

HackerGuardian allows the administrator to track the status of the false positives submitted from the 'Reports' area. To view the status, click the False Positives Tracker link from the 'Reports' area.



2.8.7.1. Filtering Options

The administrator can filter the listed false positives, based on the scan type.

- Click the drop-down arrow beside 'View' to select the false positives based on scan types. To view the false positives submitted for PCI scans, select 'PCI'.

The following table provides description of information columns in this area.

Column	Description
ID	The identity number of the submitted false positive.
Date	Date and time of submission
Host	The IP/Domain for which the vulnerability was detected and submitted as false positive
Notes	Notes entered by the administrator at the time of submission
Status	Indicates the review status or whether accepted or rejected by the Administrator or the Comodo support team after validation.
Reason	The reason for accepting or rejecting the false positive.

Note: Clicking on the up or down arrows beside each column heading sorts the list of devices in ascending order based on the category.

2.9. SiteInspector Reports

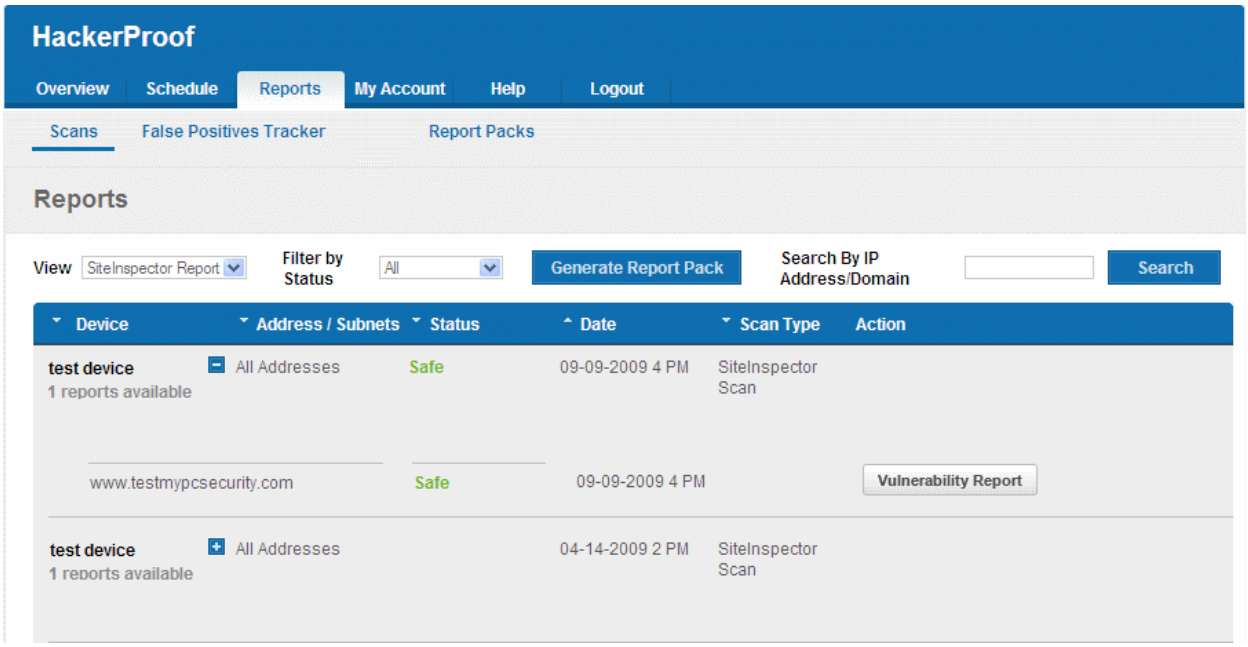
At the end of each scan, SiteInspector produces a vulnerability report for each network device/domain scanned. The status for each device is set as Safe or Malicious based on the discovery of malicious content in the webpages. The report enables the website owner/administrator to exactly find the location of the malicious content and to take the corrective measures.

The Scan Reports produced from the SiteInspector scans can be assessed from the 'Reports' area of the HackerGuardian interface, displayed by clicking the 'Reports' tab from the Navigation bar. From this interface, you can:

- View the scan reports
- Download the PCI reports as a zip file by clicking the 'Generate Report Pack' button

2.9.1. View Scan Reports

Clicking the 'Scans' link in the Reports area opens the list of the scan reports produced by HackerGuardian, HackerProof and SiteInspector at the end of each scan.



2.9.1.1. Filtering Options

The administrator can filter the reports listed, based on the scan type, status or even the reports pertaining to a specific IP or domain. The table below describes the filtering options available in this interface.

Filter	Description
View	Enables to filter the reports based on the scan type. E.g. to view only the SiteInspector scan reports, select 'SiteInspector Reports' from the drop-down menu.
Filter by Status	Enables to filter the reports based on success or failure of the scan results.
Search by IP/Domains	Enables to filter the reports pertaining to specific IP or Domain. The administrator can enter the IP address or the Domain name and the reports only for those will be listed.

2.9.2. Vulnerability Report

A Vulnerability Report provides a detailed overview of scan results on a single Domain. It includes a prioritized list of the vulnerabilities found, expert remediation advice and thousands of cross-referenced online advisories.

To view a Vulnerability Report of a Domain, select SiteInspector Report from the View drop-down, click the '+' beside the respective device and then click the 'Vulnerability Report' button in the row of the respective IP/Domain.

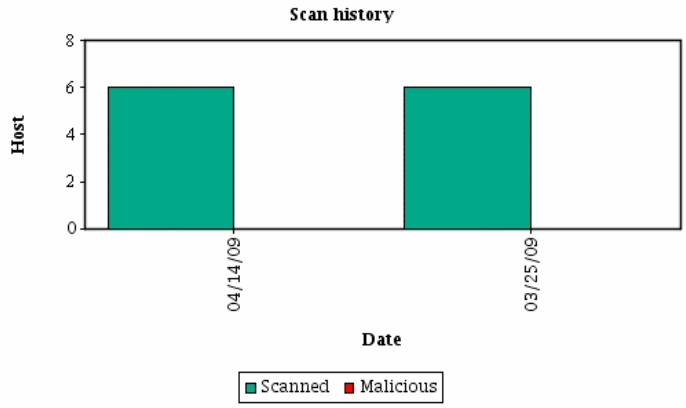
Site Inspector Report

Additional Actions

Print in PDF
Back to All Reports

Start time:	3/25/09 6:43 PM	Found **6** host(s)
End time:	3/25/09 6:44 PM	
Duration:	0 h, 0 min, 58 sec, 806 millis	

Host	Description	Comment	Status
https://testdomain.com/order/register/agreement.php?siteid=20788			SAFE
https://testdomain.com/services/complaint/complaint.php?siteid=20788			SAFE
http://testdomain.com/domains/			SAFE
http://testdomain.com/vps/infrastructure.php			SAFE
http://testdomain.com/design/			SAFE
http://testdomain.com/domains/transfers.php			SAFE



The Vulnerability Report consists of a summary of the scan details and a list of IPs/domains scanned with their status.

Tip: The vulnerability reports can be converted into pdf format by clicking the link 'Print in PDF' from the Additional Actions area as shown below.

2.9.2.1. Scan Summary

The scan summary contains the following details:

- **Start Time** - The date and time at which the scan was started.
- **End Time** - The date and time at which the scan was completed.
- **Duration** - The total time taken for the scan.

The number of IPs/Domains found in the selected network device.

Following the scan summary, the list of IPs/domains scanned and their status are displayed as a table. The following table provides description of information columns in this area.

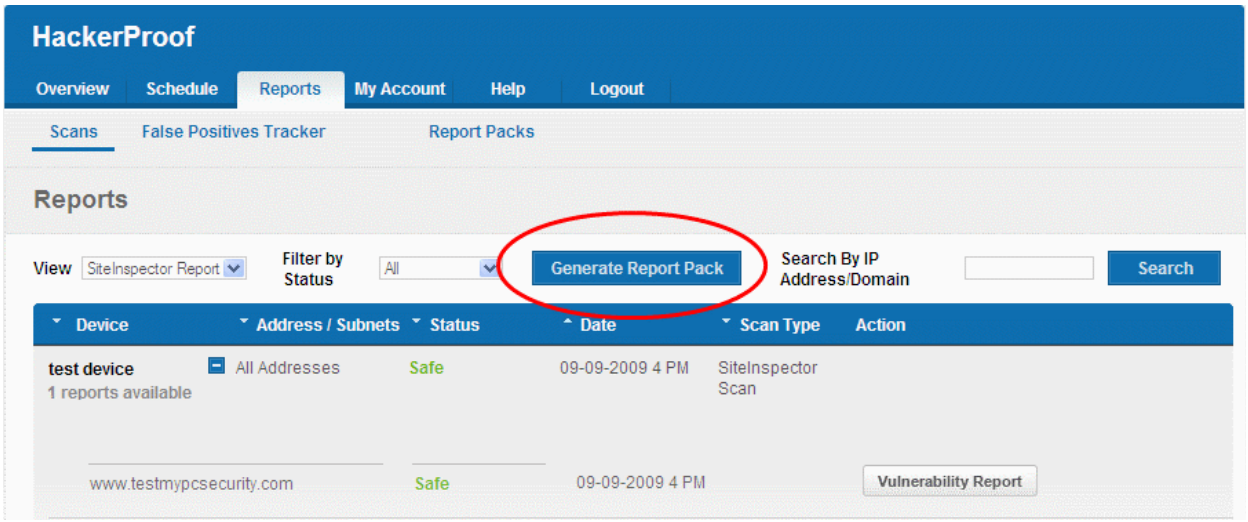
Column	Description
Host	The IP/Domain or the webpage scanned.
Description	Description on whether the target has passed or failed the scan.
Comment	Comment on the malicious found (if any).
Status	Status of the IP/Domain, it can be 'Safe' or 'Malicious'.

2.9.2.2. Scan History

A graphical representation of the comparison of the malicious content found in the domains of the device during the last five scans is displayed. This gives the trend of the reduction in the malicious content due to the corrective actions taken by the website owner/administrator.

2.9.3. Downloading Reports Pack

Administrators can download the PCI reports as a zip file by clicking the 'Generate Report Pack' button in the Reports > Scans interface.



The report packs available via the 'Generate Report Pack' button are for PCI devices and do not contain SiteInspector scan reports.

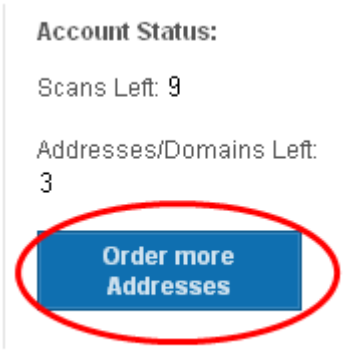
2.10. Purchasing Additional IP Packs

The HackerGuardian interface allows administrators to add additional IP addresses/Domains to their

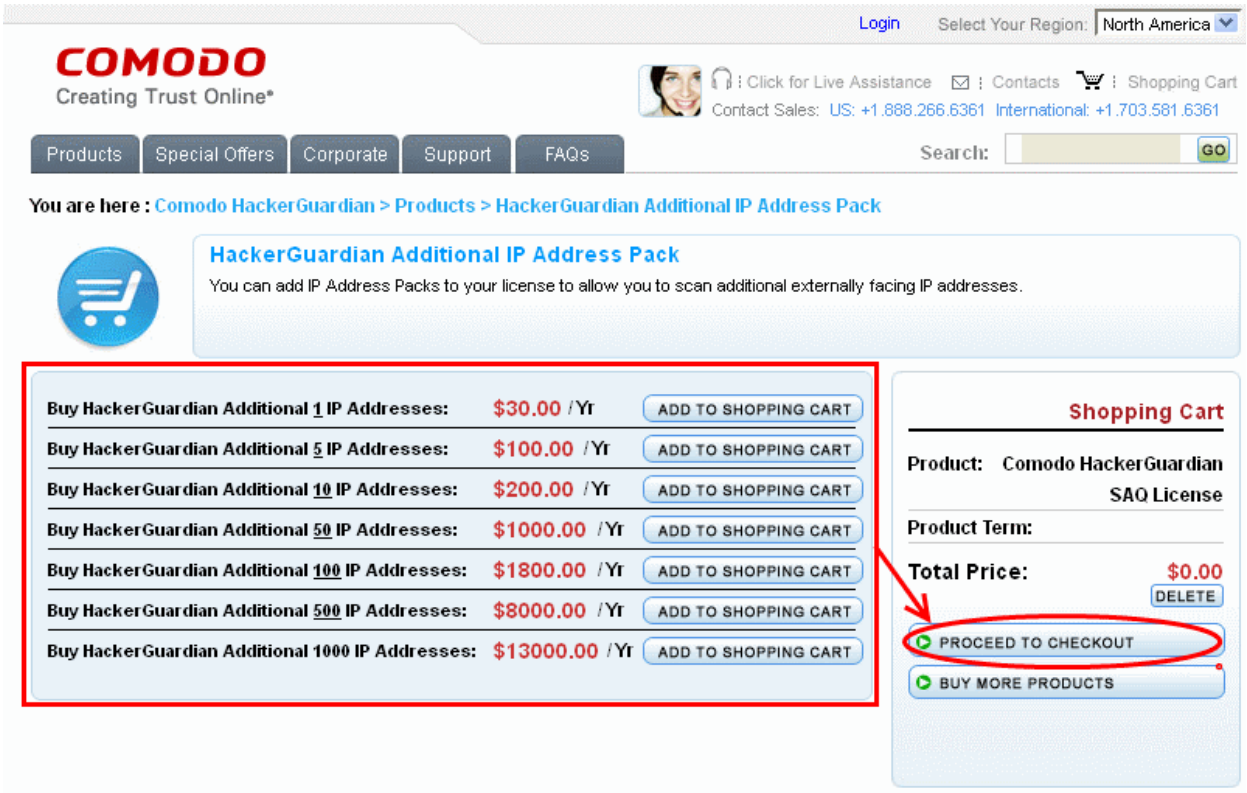
license at any time.

To buy additional IP addresses/domains

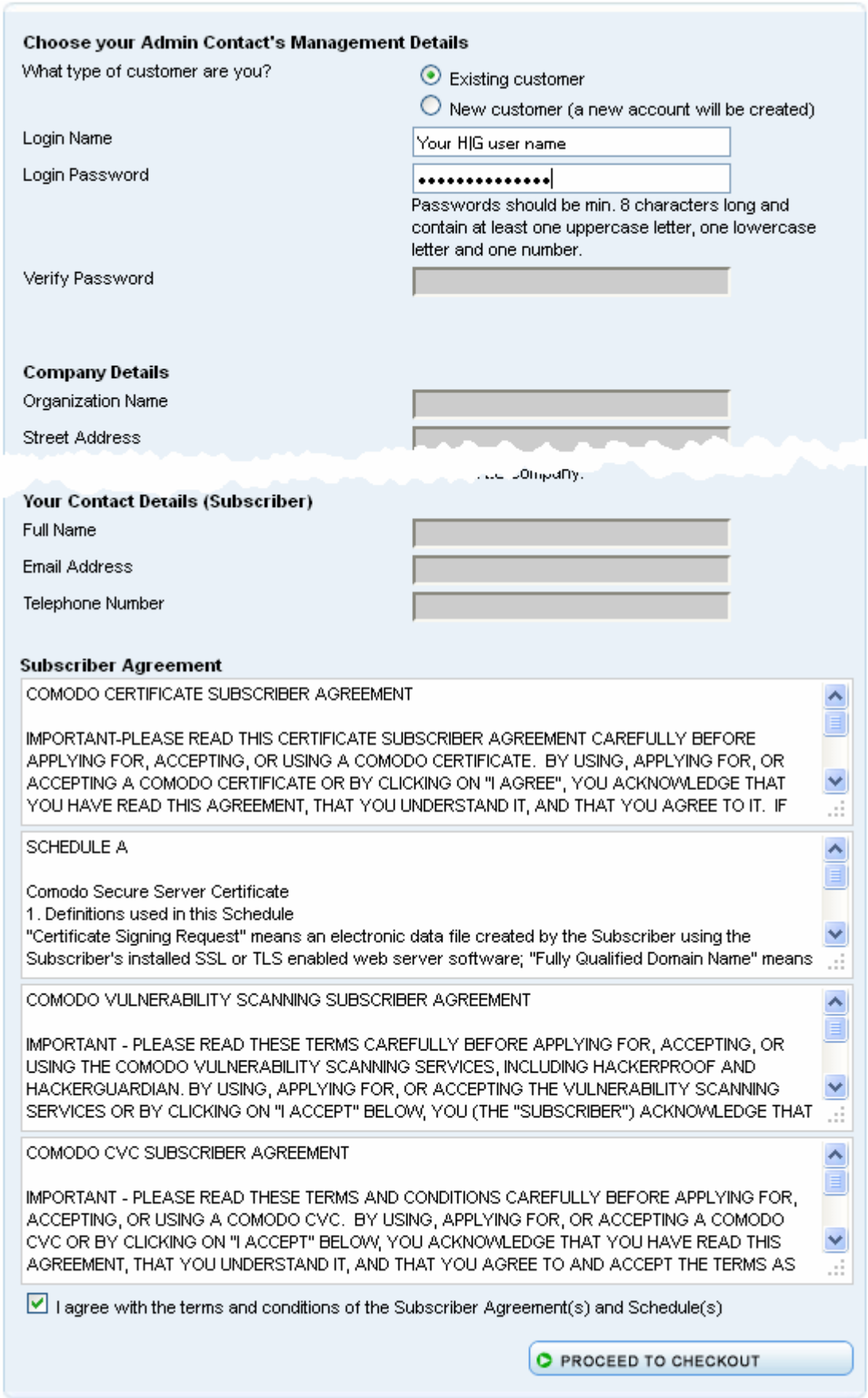
1. Click on the 'Order more Addresses' button in the Account Status area of the interface as shown below.



You will be taken to the product purchase page for HackerGuardian Additional IP Address Packs.



2. Choose the Additional IP pack that suits your requirements. You can add more than one pack of a particular type by clicking 'ADD TO SHOPPING CART'
3. When you are happy with your choices, click 'PROCEED TO CHECKOUT'.
4. On the ordering form, ensure you check the radio button 'Existing Customer' and fill out your username and password. This is important as it ensures the additional IP packs are added into your existing account.



5. Read the Subscriber Agreements fully and select the checkbox 'I agree with the terms and conditions of the Subscriber Agreement(s) and Schedule(s)'.
6. Click 'PROCEED TO CHECKOUT'.

The ability to scan the additional IP addresses will be automatically added to your license.

3.HackerGuardian FAQs

- HackerGuardian Services - General FAQ
- HackerGuardian Services - Technical FAQ
- PCI FAQ

3.1.HackerGuardian Services - General FAQ

- What's the difference between the HackerGuardian services?
- Why do I need vulnerability scanning if I have an SSL certificate?
- Are home users a serious target for hackers?
- Where can I find a glossary of terms used on this website?
- Is there a User Manual for HackerGuardian?

What's the difference between the HackerGuardian services?

HackerGuardian PCI Scan Compliancy

The PCI Scan Control Center is an on-demand, vulnerability assessment scanning solution to enable merchants and service providers to achieve PCI scan compliance.

After each scan, users receive a comprehensive vulnerability report detailing any security issues with remediation advice and advisories to help fix them.

Following a successful scan (no vulnerabilities rated higher than CVSS base score 4.0), merchants receive an official PCI compliance report that can be sent to an acquiring bank.

The Standard version enables merchants to run 10 PCI scans per quarter on up to 5 IP addresses using the full complement of over 21,000 individual vulnerability tests. The Enterprise version is a more powerful and flexible service which provides for up to 100 scans per quarter on 20 IP addresses.

HackerGuardian Free PCI Scan

The Free PCI Scan service is valid for 90 days and allows merchants to achieve PCI scan compliancy free of charge. The service contains all the functionality of the Scan Compliancy but restricts the user to 5 PCI scans per quarter on a maximum of 3 separate IP addresses. The service generates an official 'PCI Compliant' report after every successful scan.

Learn More

Why do I need vulnerability scanning if I have an SSL certificate?

SSL certificates do not secure a web server from malicious attacks or intrusions.
High assurance SSL certificates such as InstantSSL provide the first tier of customer security and reassurance, namely:

- A secure connection between the customer's browser and the web server
- Validation that the web site operators are a legitimate, legally accountable organization

However, consumer fears in the light of recent attacks on high profile merchant web sites now mean that businesses need to ensure that their websites are tested and are secure against all known vulnerabilities. Furthermore, organizations such as the Payment Card Industry (PCI) have introduced guidelines that make server vulnerability testing a mandatory requirement. The HackerGuardian Scan Compliance service provides merchants with a fast, low cost way of meeting the PCI scanning guidelines.

Are home users a serious target for hackers?

Yes!! Home users are arguably the most vulnerable people around simply because they are usually not well protected. Adopting a 'path of least resistance' model, intruders will often zero-in on home users - often exploiting their 'Always on' broadband connections and typical home use programs such as chat, Internet games and P2P files sharing applications. HackerGuardian

Free Scanning Service allows home users and network administrators alike to identify and fix any security vulnerabilities on their desktop or laptop computers.

Where can I find a glossary of terms used on this website?

There is a glossary of terms available in the help section of the HackerGuardian website at http://www.hackerguardian.com/help/glossary.html

Is there a User Manual for HackerGuardian?

There is an online manual at the following location: http://www.hackerguardian.com/help/manualmainpage.html

3.2. HackerGuardian Services - Technical FAQ

- All Services: Do I need to allow the HackerGuardian scanning IP address?
- All Services: I signed up and got the following message: 'No vulnerabilities were found and the host did not respond to any of our checks' - what does this mean?
- Free Scan: Can I change the IP address that the Free Scan tests?
- Scan Compliancy - I have a dynamic IP assigned by my ISP. Can I still use HackerGuardian?
- All Services: Does Comodo maintain any statistics about what % of clients consistently a score of 0% on the 'High Risk' threats? Or what % of all commercial servers would have this score?
- All Services: How do I upgrade from a trial account to the full version?
- All Services: After upgrading, will I have to re-enter my IP/Domain information?
- All Services: I am an existing Comodo account holder (e.g. SSL) - can I use my existing Username and Password during purchase?
- All Services: Explain the password/username system to me.
- All Services: Can I scan private (internal) IP addresses?
- Scan Compliancy: How many concurrent scans can I run?
- All Services: How many ports does each service test?
- Scan Compliancy: I get an error when trying to start a scan saying 'no plug-ins are selected'
- All Services: I have changed my password, and now cannot login to the HackerGuardian website, why?
- Scan Compliancy: Does HackerGuardian use the latest CVSS v2?

All Services: Do I need to allow the HackerGuardian scanning IP address?

In order for the HackerGuardian scan to be successful your firewall must be set to allow the IP address the scan is coming from.

The IP ranges that we scan from are:

199.66.200.32/28 (which translates as 199.66.200.32 through 199.66.200.48) and

91.209.196.32/28 (which translates as 91.209.196.32 through 91.209.196.48)

All Services: I signed up and got the following message: 'No vulnerabilities were found and the host did not respond to any of our checks' - what does this mean?

This can mean one of two things.

Either:

1) The host is currently unreachable.
It could be that the host is unreachable because of a problem with your server.

Quite often, however, it is because your firewall is denying access to the HackerGuardian scanner. In order for the HackerGuardian scan to be successful your firewall must be set to allow the IP address the scan is coming from.

The IP ranges that we scan from are:

199.66.200.32/28 (which translates as 199.66.200.32 through 199.66.200.48) and

91.209.196.32/28 (which translates as 91.209.196.32 through 91.209.196.48)

Or:

2) No services are available on the host and it is secure.

Free Scan: Can I change the IP address that the Free Scan tests?

No, the Free Scan can only scan the IP address of the machine that you sign into the HackerGuardian website from.

If you need to scan specific IPs or websites then you should consider purchasing one of following:

HackerGuardian PCI Scan Compliancy
HackerGuardian PCI Scan Compliancy Enterprise

Scan Compliancy: I have a dynamic IP assigned by my ISP. Can I still use HackerGuardian?

No. It is not possible to use the Scan Control Service unless you have a static IP.

All Services: Does Comodo maintain any statistics about what % of clients consistently a score of 0% on the 'High Risk' threats? Or what % of all commercial servers would have this score?

Comodo does not maintain any sort of global statistics about the scan results we produce.

All Services: How do I upgrade from a trial account to the full version?
Upgrade PCI Scan Control Service

Click the Upgrade to Full Service button in the HackerGuardian interface.

Or

Upgrade by buying the full version through this link: http://www.hackerguardian.com/ssl-certificate-products/ssl-certificate-index.html

Remember to select 'Existing Customer' and use your regular Comodo account username and password to during signup.

All Services: After upgrading, will I have to re-enter my IP/Domain information?

Free Scan and Free PCI Scanning Service

Both free license types are for a fixed period. At the end of this period the license expires.

Scan Control Centre:
For the PCI Scan Control Service any previously validated IP addresses will still be usable.

All Services: I am an existing Comodo account holder (e.g. SSL) - can I use my existing Username and Password during purchase?

Yes. You should use the 'Existing Customer Option' and enter your existing Comodo UN/PW during the signup process. You can then also use your Comodo account Password and Username to log into the HackerGuardian interface at www.hackerguardian.com

All Services: Explain the password/username system to me.

During signup you created a Comodo account with a Username and Password. This Username and Password has dual functionality:
1. Use it to log into your Comodo account and manage your Comodo account details. You can log in at http://www.comodo.com
2. Use it to log into the HackerGuardian web-application interface. Do this using the login box at: http://www.hackerguardian.com

Also see documentation at: http://www.hackerguardian.com/help/starting_up.html

All Services: Can I scan private (internal) IP addresses?

Yes. Internal IP addresses can be scanned if you have a HackerGuardian PCI Scan Compliancy Enterprise license. It is not possible to scan internal IPs with the standard license.

Private IPs ranges are defined by RFC 1918 as:

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192/168/16 prefix)

Scan Compliancy: How many concurrent scans can I run?

The number of concurrent scans you can run is 10% of the number of IP's covered by your license and the maximum number is 25. For example, if the number of IP addresses covered by your license is 50, you can run five concurrent scans on different IP's.

All Services: How many ports does each service test?

Different level of services will allow for different total numbers of ports to be scanned. (If you use the Scan Control service, you may define ranges of ports to be scanned within the 'Set Options' page in the 'Port Range' field.)

- The PCI Scan Control Service scan tests up to a total of 65,535 ports - the total number of ports available on your system.
- The Daily and Free services will scan the first 15,000 ports on your system. This is a targeted selection of the most commonly used (and commonly attacked) ports.*

Note that most services run on the reserved ports below 1024 and security industry experts agree that these are the most commonly targeted ports. In some circumstances it will be beneficial to test all 65,535 ports, but administrators should be aware that this will lengthen the scan time.

All Services: I have changed my password, and now cannot login to the HackerGuardian website, why?

When you change your password there is a delay between changing it, and that change being synchronized with the HackerGuardian database.

Please allow 15 minutes for the synchronization to take place after changing your password.

Scan Compliancy: Does HackerGuardian use the latest CVSS v2?

Yes. HackerGuardian uses the latest Common Vulnerability Scoring System version 2 (CVSS v2). All HackerGuardian PCI Scan customers are not impacted by the change from CVSS v1 to v2 as we have already been using v2.

3.3. PCI FAQ

- What is PCI DSS?
- What is the Self Assessment Questionnaire?
- What are the compliance validation reporting requirements for merchants?
- To whom does the PCI regulations apply?
- What is defined as 'cardholder data'?
- What if a merchant or service provider does not store cardholder data?
- Are there alternatives, or compensating controls, that can be used to meet a requirement?
- Are there alternatives to encrypting stored data?
- What are the compliance validation reporting requirements for merchants?
- Do merchants need to include their service providers in the scope of their review?

- What is a network security scan?
- How often do I have to scan?
- What reports are provided by HackerGuardian scanning service?
- What criteria causes a Pass or Fail on a PCI scan?
- What if I fail the PCI scan?
- Where can I find and complete the Self-Assessment Questionnaire?
- Where can I find a PCI Approved Scanning Vendor capable of providing quarterly PCI vulnerability scans?
- What's the deadline for compliance/ When must I begin using the new PCI standards?
- What are the penalties for non-compliance with the PCI standards?
- Make it easy for me. What do I have to do to become compliant?

What is PCI DSS?

The Payment Card Industry Data Security Standards (PCI DSS) are a set of 12 requirements developed jointly by Visa, MasterCard, JCB International, Discover and American Express to prevent consumer data theft and reduce online fraud. The PCI DSS represents a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Compliance and validation of compliance with some or all of the 12 requirements is mandatory for any organization that stores, transmits or processes credit card transactions.

- The exact number of requirements (out of the 12) that any one organization need comply with is dependent on that organization's 'Validation Type'. An organization's Validation Type is determined by precisely how that organization handles credit card data. There are 5 such 'Validation Types' and every organization will that needs to be PCI compliant will be categorized as one of these types. (see table 'Validation Types')
- Once an organization has determined its 'Validation Type' (or the organization has been assigned as a particular validation type by its acquirer) it can complete the Self Assessment Questionnaire (SAQ) and Attestation of Compliance that is appropriate for that 'Validation Type'.

What is the Self Assessment Questionnaire?

The PCI Data Security Standard Self Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Comodo has simplified this often confusing process with the HackerGuardian PCI Compliance Wizard - an intuitive web-based application guides merchants through every step of the PCI Self Assessment Questionnaire. Each question is accompanied by expert advice to help the merchant interpret and appropriately answer each question. At the end of the wizard you will find out immediately whether or not your answers qualify your organization as PCI compliant.

The wizard will provide:

- A Questionnaire Summary - Listing security control areas on which you failed compliance
- A custom 'Remediation Plan' for your company containing:
    - A comprehensive list of remedial actions that you need to take to attain full PCI compliance
    - A remediation planning tool enabling task prioritization and project management
    - Links to recommended products and services that will help you cost-effectively resolve non-compliant areas
- A 'ready-to-submit' PCI DSS Self Assessment Questionnaire

Your progress is automatically saved after each question - allowing you to log out and return at a later date to complete the questionnaire. Your free account and responses are retained, giving you an opportunity to revise and modify any of your answers. This also allows you to update, schedule and track the progress of outstanding remediation tasks.

Click the SAQ tab in the HackerGuardian navigation bar to begin the wizard.

What are the compliance validation reporting requirements for merchants?

Under the new PCI standard, the compliance validation requirements of the old VISA CISP and MasterCard SDP programs have been aligned so that merchants need only validate their compliance once to fulfill their obligation to all payment cards accepted. Merchants will provide compliance validation documentation to their Acquirer(s). Compliance validation documentation consists of the appropriate annual self assessment questionnaire (and accompanying attestation of compliance) and possibly the quarterly PCI scan compliance report.

To whom does the PCI regulations apply?

The PCI DSS standards apply to all entities that process, store or transmit cardholder data. This includes all merchants and service providers with external-facing IP addresses handle, store or transmit credit card data. Even if your website does not offer website based transactions (for example, you link to a payment gateway) there are other services that may make card data accessible. Basic functions such as e-mail and employee Internet access will result in the Internet accessibility of a company's network. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems if not properly controlled.

What is defined as 'cardholder data'?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

What if a merchant or service provider does not store cardholder data?

If a merchant or service provider does not store cardholder data, the PCI requirements still apply to the environment that transmits or processes cardholder data.

Are there alternatives, or compensating controls, that can be used to meet a requirement?

If a requirement is not, or cannot, be met exactly as stated, compensating controls can be considered as alternatives to requirements defined by the PCI DSS. Compensating controls should meet the intention and rigor of the original PCI requirement, and should be examined by the assessor as part of the regular PCI compliance audit.

Are there alternatives to encrypting stored data?

Stored cardholder data should be rendered unreadable according to requirement 3 of the PCI Security Audit Procedures document. If encryption, truncation, or another comparable approach cannot be used, encryption options should continue to be investigated as the technology is rapidly evolving. In the interim, while encryption solutions are being investigated, stored data must be strongly protected by compensating controls.

An example of compensating controls for encryption of stored data is complex network segmentation that may include the following:

- Internal firewalls that specifically protect the database
- TCP wrappers or firewall on the database to specifically limit who can connect to the database
- Separation of the corporate internal network on a different network segment from production, fire- walled away from database servers.

What are the compliance validation reporting requirements for merchants?

Under the new PCI standard, the compliance validation requirements for merchants of the VISA CISP and MasterCard SDP programs have been aligned so that merchants need only validate their compliance once to fulfill their obligation to all payment cards accepted. Merchants will provide compliance validation documentation to their Acquirer(s). Compliance validation documentation consists of the annual self assessment questionnaire and the quarterly PCI scan compliance report.

Do merchants need to include their service providers in the scope of their review?

No. Service providers are responsible for validating their own compliance with PCI regulations independent of their customers.

What is a network security scan?

A Network Security Scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by qualified scan vendors such as Comodo the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

How often do I have to scan?

Every 90 days / once per quarter. Merchants and Service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI Approved Scanning Vendor (ASV). Comodo is a PCI Approved Scanning Vendor.

What reports are provided by HackerGuardian scanning service?

HackerGuardian Scan Control service provides two reports after each scan - the Audit Report and the PCI Compliance report. The PCI Compliance report is the one you need to submit to your acquiring bank to demonstrate compliance. The Audit Report is a more technical document used to identify and re mediate any security holes.

What criteria causes a Pass or Fail on a PCI scan?

Each post-scan HackerGuardian vulnerability report states a PCI compliance status of 'Compliant' or 'Not Compliant' based on the discovery of potential security flaws on your systems.

If no vulnerabilities with a CVSS base score greater than 4.0 are detected then the scanned IP addresses, hosts and Internet connected devices have passed the test and the report can be submitted to your acquiring bank.

If the report indicates 'Non Compliant' then the merchant or service provider must re mediate the identified problems and re-run the scan until compliancy is achieved.

What if I fail the PCI scan?

If your HackerGuardian PCI Scan Compliance Report indicates 'NOT COMPLIANT' then vulnerabilities with CVSS base score greater than 4.0 were discovered on your externally facing IP addresses. The accompanying Audit Report contains a detailed synopsis of each vulnerability prioritized by threat severity. Each discovered vulnerability is accompanied with solutions, expert advice and cross referenced links to help you fix the problem. You should fix all vulnerabilities identified as a 'Security Hole'.

Furthermore, each report contains a condensed, PCI specific, 'Mitigation Plan' - a concise, bulleted list of actions that you need to take to achieve compliance.

After completing the actions specified in the Mitigation Plan you should run another scan until the report returns a 'COMPLIANT' status.

Where can I find and complete the Self-Assessment Questionnaire?

HackerGuardian, in partnership with Panoptic Security, provide a free wizard that guides merchants and service providers through each stage of self-assessment questionnaire. More details on the wizard can be found here: here

Merchants have to answer all questions with 'Yes' or 'N/A to be considered PCI compliant. Answering 'No' to any question means the merchant or service provider is not compliant. The risk(s) identified by the questionnaire must be re mediated and the questionnaire retaken. After creating a user name and password, merchants can save their progress at any time. Following successful completion of the questionnaire, merchants will be provided with official certification that can be submitted to their acquirer.

Where can I find a PCI Approved Scanning Vendor capable of providing quarterly PCI vulnerability scans?

Right here!! Comodo HackerGuardian offers a range of PCI compliance services designed for merchants and service providers of all sizes. Click here to find out more.

What's the deadline for compliance/ When must I begin using the new PCI standards?

The Payment Card Industry Standards, Security Audit Procedures, Self-Assessment Questionnaire, and Security Scanning

Requirements are effective immediately.

What are the penalties for non-compliance with the PCI standards?

Validation and enforcement is the responsibility of the acquiring financial institution or payment processor.
For each instance of non-compliance, these organizations levy various penalties onto merchants and service providers which can include:

- Increased transaction processing fees
- Fines of more than $500,000 for serious breaches
- Suspension of credit card transaction processing abilities

Comodo HackerGuardian provides a range of services that make PCI compliance easy. Find out which service is right for you at www.hackerguardian.com.

Make it easy for me. What do I have to do to become compliant?

1. Complete the PCI Self-Assessment Questionnaire using our free, online wizard

- Preliminary questions will help you to determine which 'validation type' your company fits into and therefore of the 4 self assessments questionnaires you need to complete.
- Each of the questions is accompanied by expert help, information and advice that will help you to both interpret the question correctly and provide the appropriate answer
- Once the wizard is complete, you will receive:
  - A questionnaire summary detailing any control areas on which you failed compliance
  - A custom 'Remediation Plan' for your company containing a list of remedial actions that you need to take alongside links to recommended products and services that will help you resolve non-compliant areas.
  - A 'ready - to - submit' PCI DSS Self Assessment Questionnaire which will include your completed 'Attestation of Compliance'

2. Conduct a quarterly vulnerability scans on your externally facing IP addresses

If your organization is required to be compliant with section 11.2 of the PCI standard then you will also need to obtain quarterly vulnerability scans on your network.

HackerGuardian will conduct an in-depth audit of your network to detect vulnerabilities on your network and web-server. If your servers fail the test, you will find lots of helpful advisories in the scan report that will help you patch the security holes.

After your infrastructure passes the scan, HackerGuardian will automatically generate the PCI Compliance report that you need to send your acquiring bank as to demonstrate your compliance.

Find out more about HackerGuardian PCI Scanning Services

3. Send the completed questionnaire, attestation and the Scan Compliance report to your acquirer.

Both the PCI Scan Compliant report and the Annual Self Assessment Questionnaire should be turned into your merchant bank. Your merchant bank will then report back to the Payment Card Industry that your company is PCI Compliant.

Appendix 1- Acceptable Validation Documents

Country	Documentation	AKA	Notes
AIA	Articles of Incorporation		
AIA	Certificate of Incorporation		
ARG	Articles of Incorporation/Registration	El reglamento de Constitución de sociedad anónima/Matrícula	A translation of all documentation should be provided, if not already in English
ARG	Business Licence	La Licencia comercia	A translation of all documentation should be provided, if not already in English
AUS	Certificate of Registration of a Company		
AUS	Certificate of Registration of Business Name		
AUS	Certificate of Registration on Change of Name		
AUS	Copy of ASIC Registration		
BEL	Articles of Incorporation/Registration	Les articles d'Incorporation/d'Enregistrement	A translation of all documentation should be provided, if not already in English
BLZ	Certificate of Incorporation		
BLZ	Certificate of Incumbancy		
BRA	Copy of the Social Contract	Copia de contrato social	A translation of all documentation should be provided, if not already in English
BRA	National Business Registration Card	Cartao de Cadastro Nacional Da Pessoa Juridica	A translation of all documentation should be provided, if not already in English
CAN	Annual Declaration from the General Inspector of Financial Institutions	Declaration Annuelle de Inspectur general des institutions financieres.	A translation of all documentation should be provided, if not already in English
CAN	Business License		
CAN	Certificate of Incorporation	Certificat de constitution	A translation of all documentation should be provided, if not already in English

Country	Documentation	AKA	Notes
CAN	Vendor Permit	Permis de vendeur	A translation of all documentation should be provided, if not already in English
CHE	Articles of Incorporation		
CHE	Business License		
CHE	Extract from the Registry of Commerce	Extrait du Journal de la Registre du Commerce	A translation of all documentation should be provided, if not already in English
CZE	Business License	Vypis z obchodniho rejstriku, vedeneho Karjskym obchodnim soudem v Praze	A translation of all documentation should be provided, if not already in English
DEU	Certificate of trade index entry	Handelsregister	A translation of all documentation should be provided, if not already in English
DEU	Copy of Business Certificate	Gewerbeschein	A translation of all documentation should be provided, if not already in English
DEU	District Court Copy of Articles of Incorporation	Amstgericht kopie des Handelsregistereintrag im Handelsregister	A translation of all documentation should be provided, if not already in English
DEU	Official letter from the Federal bureau for finances	Bundesamt fur Finanzen	A translation of all documentation should be provided, if not already in English
DNK	Certificate of Incorporation	Sammenskrevet Resume	A translation of all documentation should be provided, if not already in English
FIN	Extract from the Register of Companies	Ote Kaupparekisterista	A translation of all documentation should be provided, if not already in English
FRA	Business Licence	Registre de Commerce	A translation of all documentation should be provided, if not already in English
FRA	Extracts from the register of commerce and societies.	Extrait du registre du commerce et des societes	A translation of all documentation should be provided, if not already in English
GBR	Articles of Association		
GBR	Articles of Incorporation/Registration		

Country	Documentation	AKA	Notes
GBR	Certificate of Incorporation on Change of Name		
GBR	Non Domestic Rating Notice		
GBR	Office of Fair Trading Standard Licence/Renewal		
GBR	VAT Certificate		
GRC	Certificate of Start Up of a Personal Enterprise		A translation of all documentation should be provided, if not already in English
GRC	Extract from the Business Registry of Athens		A translation of all documentation should be provided, if not already in English
IND	Certificate of Commencement of Business		A translation of all documentation should be provided, if not already in English
IND	Certificate of Incorporation		A translation of all documentation should be provided, if not already in English
IRL	Certificate of Incorporation		
IRL	Companies Registration Office certificate of Company Name Registration		
ISL	Certificate of Incorporation from Icelandic Register of Enterprises		A translation of all documentation should be provided, if not already in English
ISR	Custom & VAT Department: Certificate and License for Trading		A translation of all documentation should be provided, if not already in English
ISR	Ministry of Justice: Certification of an Incorporation of Company		A translation of all documentation should be provided, if not already in English
ITA	Proof of Existence of a Company released by the Chamber of Commerce in Italy	Visura Camerale	A translation of all documentation should be provided, if not already in English
JPN	Business Licence		A translation of all documentation should be provided, if not already in English
JPN	Seal Certificate		A translation of all documentation should be provided, if not already in

Country	Documentation	AKA	Notes
			English
MEX	Copy of Entry in the Federal Registration of Contributors	Inscripcion en el Registro Federak de Contribuyentes	A translation of all documentation should be provided, if not already in English
MEX	Company creation bill		A translation of all documentation should be provided, if not already in English
MEX	Mexican business license		A translation of all documentation should be provided, if not already in English
MEX	Mexican IRS card		A translation of all documentation should be provided, if not already in English
MEX	Cheque with company name		A translation of all documentation should be provided, if not already in English
MEX	Back accounts		A translation of all documentation should be provided, if not already in English
MEX	Passport or licence of the legal guardian of the company		A translation of all documentation should be provided, if not already in English
MLT	Certificate of Compliance		
NLD	Articles of Incorporation/Registration	Artikelen van Onderneming/Inschrijving	A translation of all documentation should be provided, if not already in English
NLD	Extract from the Commercial Register of the Chamber of Commerce and Industries for Amsterdam	Kamer Van Koophandel, Amsterdam	A translation of all documentation should be provided, if not already in English
NOR	Business Registration Certificate	Bronnoysundregistrene	A translation of all documentation should be provided, if not already in English
NZL	Certificate of Incorporation		
PAL	Letter from Chamber of Commerce & Industry		A translation of all documentation should be provided, if not already in English
PHL	Articles of Incorporation/Registration		A translation of all documentation should be

Country	Documentation	AKA	Notes
			provided, if not already in English
POL	Certificate of Registration in the Register of Economic Activities.	Ewidecji Dzialalnoscu Gospodanczej	A translation of all documentation should be provided, if not already in English
POL	Documentation from Department of Treasury	Urzad Skarbowy	A translation of all documentation should be provided, if not already in English
POL	REGON - Certificate of registration in the National Official Register of the Nationalised Industries Units	Krajowy Rejestr Urzedowy Podmiotow Gospodarki Marodowej	A translation of all documentation should be provided, if not already in English
PRI	Business Registration Certificate	Registro de Corp	
PRT	Collective Person Identification Card	Cartão de Identificação De Pessoa Colectiva	A translation of all documentation should be provided, if not already in English
SWE	Article of Incorporation		A translation of all documentation should be provided, if not already in English
SWE	Letter of Incorporation		A translation of all documentation should be provided, if not already in English
SWE	Patent Registration Documentation		A translation of all documentation should be provided, if not already in English
TUR	Certificate of Good Standing from Chamber of Commerce	Ticaret Odasi, Faaliyet Belgesi	A translation of all documentation should be provided, if not already in English
TUR	Company Signatory List	Imza	A translation of all documentation should be provided, if not already in English
TUR	Extract from Companies Gazeteer	Sicil Gazetesi	A translation of all documentation should be provided, if not already in English
TUR	Tax Form	Vergi Levhasi	A translation of all documentation should be provided, if not already in English
TUR	Turkish Id	Turkiye Cumhuriyeti Nufus Cuzdani	A translation of all documentation should be

Country	Documentation	AKA	Notes
			provided, if not already in English
UAE	Professional Licence		A translation of all documentation should be provided, if not already in English
USA	Sales & Use Tax Permit		
USA	Business License/Certificate		
USA	Business Registration Certificate		
USA	Certificate of Acceptance of Appointment by Resident Agent		
USA	Certificate of Assumed Business Name		
USA	Certificate of Authority		
USA	Certificate of Change of Resident Agent and/or Location of Registered Office		
USA	Certificate of Exempt Status		
USA	Certificate of Existence with Status in Good Standing		
USA	Certificate of Formation		
USA	Certificate of Incorporation		
USA	Certificate of Ownership for Unincorporated Business or Profession		
USA	Certificate of Payment of Business Tax		
USA	Certificate of Withholding Identification Number		
USA	Certificate/Articles of Amendment		
USA	Certificate/Articles of Organisation		
USA	Corporate Charter		
USA	Corporation Annual Report		
USA	Corporation Estimated Tax Form		
USA	Declaration of Proprietership or Partnership Registration		
USA	Employer Identification Number Application		
USA	Fictitious Business Name Statement		
USA	Filing endorsement		
USA	Filing receipt		
USA	General Excise Tax License		

Country	Documentation	AKA	Notes
USA	Merchant's Certificate of Registration		
USA	Notary Public Identification Card		
USA	Occupational Tax Certificate/Licence		
USA	Organization Action in Writing of Incorporation		
USA	Privilege License		
USA	Public Records Filing for a New Business Entity		
USA	Restatement and Revision of Partnership Agreement		
USA	Sellers Permit		
USA	Statement of Partnership Agreement		
USA	Trade Name Registration Form		
USA	Trade Name Renewal Form		
USA	Transaction Privilege Tax License		
USA	Zoning Permit		
ZAF	Amended Founding Statement		
ZAF	Certificate of change of name of company	Sertifikaat van verandering van naam van maatskappy	A translation of all documentation should be provided, if not already in English
ZAF	Certificate of Incorporation	Sertifikaat van Inlywing	A translation of all documentation should be provided, if not already in English
ZAF	Founding Statement		

Upon receipt of the relevant documentation, you should verify the information received correctly matches the information provided during application.

Questions:

Should you have any question regarding any application or would like assistance with the validation process, please contact docs-enquiries@comodogroup.com.

Appendix 2 - Comparison of Services

	PCI Scan Compliancy Service	Site Inspector Scanning	PCI Scan Compliancy Service Enterprise
Price	$249	$0	$399
90 Day Free Trial*	Yes	N/A	No
On Demand scanning	Yes	Yes	Yes
Max number of on-demand scans per quarter	10	Unlimited	Unlimited
Automatic Daily Scanning	No	Can be scheduled	Can be scheduled
Scans performed by MasterCard approved ASV	Yes	Yes	Yes
PCI scan compliance report	Yes	No	Yes
Free PCI questionnaire for submitting to acquiring bank	Yes	No	Yes
Schedule Scan Facility	Yes	Yes	Yes
Post Scan Audit Reports	Yes	Yes	Yes
Merge and Compare Audit Reports	No	No	Yes
Reports include vulnerability mitigation advice	Yes	Yes	Yes
Max number of IPs that scan be scanned	5	scans domains	20
Number of concurrent IP scans	10% of number of IP addresses included in the license. Maximum 25 scans.	scans domains	10% of number of IP addresses included in the license. Maximum 25 scans.
Secure web based reports and management	Yes	Yes	Yes
Executive Summary Reports	Yes	No	Yes
Number of vulnerability tests/plugins	Full Complement (over 30,000)	N/A	Full Complement (over 30,000)
Retest only on discovered vulnerabilities	Yes	No	Yes
Vulnerability tests updated on regular basis	Yes	Yes	Yes
Includes HackerProof trust mark certification	No	No	No
Test IP ranges	Yes	scans domains	Yes
Test all 65,535 IP ports	Targeted scan of 15,000 most commonly used ports	N/A	Yes

	PCI Scan Compliancy Service	Site Inspector Scanning	PCI Scan Compliancy Service Enterprise
Customize scans by:			
Individual Vulnerability Test	No	No	Yes
Vulnerability test family	No	No	Yes
Over 60 user configurable parameters	Yes	No	Yes
Most suitable for:	Merchants needing PCI compliance; Network Administrators requiring daily auditing Banking, insurance and other financial websites; Payment service providers	Website owners of all types that wish to verify to themselves and their customers that their site does not house malware	Corporate networks; Enterprises; Distributed I.T. infrastructures of all sizes; Network administrators; Health, Financial and Governmental organizations

* The 90 day free trial license is valid for only five scans over three IP address during the 90 day period.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,

Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: EnterpriseSolutions@Comodo.com

Comodo Security Solutions, Inc.

525 Washington Blvd.

Jersey City, NJ 07310

United States

Tel : +1.888.256.2608

Tel : +1.703.637.9361

For additional information on Comodo - visit http://www.comodo.com.