



# PCI DSS Jump Start

for FortiScan™ 4.0 MR2 Patch 3





eCommerce thrives because customers trust that vendors will keep their financial data safe. Points of sale (POS) have become increasingly intelligent and mobile.

If you are required to comply with PCI DSS standards for credit card data, and you manage many POS, a data center, or a colocation center that must be compliant, FortiScan can help.

Simply follow the instructions here, from start to finish!

## PCI DSS requirements

Payment Card Industry Data Security Standard (PCI DSS), defined by the [PCI Security Standards Council](#), is a set of data security requirements to which banks, online merchants, and Member Service Providers (MSPs) must adhere, enforcing the safe handling of card holder information.

To comply with the requirements, merchants and MSPs must:

- Annually conduct an on-site audit or complete the PCI Self-Assessment Questionnaire.
- Quarterly conduct vulnerability scans on all Internet-facing networks and systems. These scans must be performed by an approved scanning vendor. Vulnerability scans detect security threats associated with electronic commerce, and provide the bank, merchant, or MSP with a report demonstrating compliance status. Threats must be remediated.

To meet the second requirement, FortiScan can generate PCI technical and executive compliance reports that shows the pass or failure status for each host on your network.

## Download FortiScan

You might already have a physical FortiScan appliance.

But if you need the flexibility and resilience of a virtual machine, or if you aren't ready to commit to a physical appliance, you can download a 64-bit virtual machine version of FortiScan, called FortiScan-VM:

[http://www.fortinet.com/resource\\_center/product\\_downloads.html](http://www.fortinet.com/resource_center/product_downloads.html)

You can try FortiScan-VM for 15 days, worry-free. Stackable vCPU expansion licenses are available to grow with you.

Be sure to enable 64-bit addressing and hardware-assisted virtualization technology (VT) in your BIOS, map the vNICs, and size your vCPU and storage repository before powering on FortiScan-VM. Details are in the [FortiScan-VM Install Guide](#).

Once you have a virtual or physical FortiScan, you are ready to begin.

## Preparing your hosts to be scanned

Adjust your network topology and settings so that the PCI scan can reach its targets.

### **Hosts must be:**

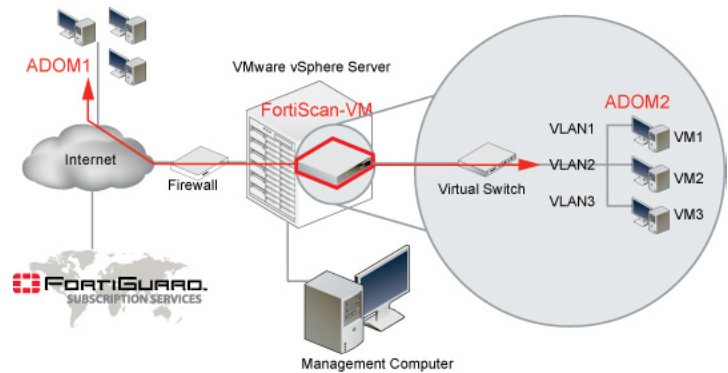
- powered on
- running their typical services
- have a static IP address / permanent DHCP reservation

To reduce the time required to discover live hosts, hosts should also be responsive to ARP or ICMP `ECHO_REQUEST` (ping) from FortiScan's IP address.

### **FortiScan should be placed on:**

- the Internet
- with POS and other clients on your private network
- any other network whose hosts access the computer whose PCI DSS compliance you are testing

Adjust firewall policies, add virtual IPs, and/or configure port forwarding if necessary for the scan to reach the target computer. But keep in mind that if you “soften” security for the scan to reach the target, some vulnerabilities and non-compliances might be false positives.



## Define your domains

First, define at least one administrative domain (ADOM). (If you are an MSSP, you may want to define a few: one for each customer, or one for each division of a large enterprise.)

ADOMs:

- **Restrict** your compliance scans to your domain
- **Define** which assets each FortiScan administrator can see and/or govern
- **Distinguish** computers on different parts of your network that use the same IP address



**Tip:** If you don't want to put computers with identical IP addresses into separate ADOMs, you can achieve a similar affect via a VPN.

Connect your FortiScan to a FortiGate. Next, establish a VPN between the FortiGate and the ADOM's computers. Finally, add each computer's remote IP from the VPN (**not** their identical ones) to the ADOM.

## To define an ADOM

- 1 Connect to FortiScan's web UI. If you are connecting directly to port1 and using its default IP address, the URL is:  
<https://192.168.1.1/>
- 2 Log in to the web UI as `admin`.  
(Other FortiScan administrator accounts cannot make new ADOMs.)
- 3 From *Current ADOM*, select *Global*.  
(Other ADOMs cannot configure new ADOMs.)
- 4 Go to *System > ADOM > ADOM*.
- 5 Click *Create New*.
- 6 Configure these settings:

**New Adom**

Name  (required)\*

Description

Configure  Inherit Global Configuration(Email Server Setting)

Asset Limit  (Min-Max:1-20000)\* Total Available Asset Number:19976

Asset Filters (required)

<b>GUI item</b>	<b>Description</b>
<b>Name</b>	Type a unique name for the administrative domain, such as <code>www.example.com</code> . The name cannot be longer than 11 characters, and cannot contain special characters, except underscores ( <code>_</code> ), hyphens ( <code>-</code> ), periods ( <code>.</code> ), and "at" symbols ( <code>@</code> ).
<b>Asset Limit</b>	Type the maximum number of assets that can belong to this ADOM. The total number of assets that can be supported by a FortiScan appliance varies by model. To prevent an ADOM from consuming this hardware limit and starving other ADOMs for resources, restrict the ADOM to a proportionate amount of the total. For details on the limits of each model, see the <a href="#">FortiScan Administration Guide</a> .

- 7 Next to the *Asset Filters* area, click *Create New*.  
A dialog should appear where you can define the IP address space that belongs to the ADOM.

## 8 Configure these settings:

The screenshot shows the 'New Asset Filters' dialog box. It features a title bar 'New Asset Filters'. Below the title bar is a 'Filter Name' text field. Underneath is the 'Asset IP' section, which contains two radio buttons: 'IP Value' and 'IP Range'. The 'IP Range' option is selected and highlighted with a red box. To the right of the 'IP Range' radio button are two text fields for IP addresses, with 'To:' between them. Below these fields is an 'IP Exceptions' list box, currently empty, with 'Add' and 'Delete' buttons to its right. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

<i>GUI item</i>	<i>Description</i>
<b>Filter Name</b>	Type a unique name for the asset filter, such as <code>server_farm1</code> or <code>pos1</code> .
<b>Asset IP</b>	Define the IP address space that belongs to the ADOM. Select either: <ul style="list-style-type: none"><li>• <b>IP Value</b> — In the text field to the right of this option, type an IP address that you want to include in the ADOM.</li><li>• <b>IP Range</b> — In the 2 text fields to the right of this option, type the first and last IP addresses in a range of IP addresses that you want to include in the ADOM. If you need to exclude one or more of the IP addresses from the IP range, click <i>Add</i> to configure <i>IP Exceptions</i>.</li></ul> <b>Note:</b> Computers do not need to be present at every IP address in the range. Live computers in this space will be detected later, during a discovery scan.

9 Click *OK* to return to the ADOM dialog.

10 Repeat the previous 2 steps for each set of IP addresses that you want to include in the ADOM.

11 Click the *Move Up* or *Move Down* buttons to change the order of IP address sets.

Entries are evaluated for a match from top to bottom. Position filter entries so that the **first** matching entry matching will include or exclude the IP address from the ADOM, whichever you intend.

12 Click *OK*.

The new ADOM is added to the list on *System > ADOM > ADOM*, and the drop-down list in *Current ADOM*. Administrator accounts can now be assigned to the new ADOM.

## Discover your domain's live targets

What if some IP addresses in your domain are unused? You don't want to waste time scanning for computers that aren't there.

To determine live IP addresses, run a discovery scan. This adds a list of your computers to your ADOM's asset inventory.

### To schedule a discovery scan

- 1 From *Current ADOM*, select an ADOM that is **not Global**.

The discovery scan will add new assets to that specific ADOM's asset inventory.

- 2 Go to *Asset > Discovery > Schedule*.
- 3 Click *Create New*.
- 4 Configure these settings:

**Create Asset Discovery (Map) Schedule**

Name: Asset\_Discovery\_20110509\_134550

**Target**

Scan Ports: TCP & UDP

Asset Group: [Please Select]

Domain: [Empty]

IP Range: [Empty]

**Schedule**

Run now

Run later

**Output Option**

File output:  HTML  PDF  MS Word  Text  MHT

Email/Upload: [Please Select]

OK Cancel

#### **GUI item**

#### **Description**

---

<b>Name</b>	The name of the discovery scan profile.
<b>Target</b>	

- |                   |   |
|-------------------|---|
| <b>Scan Ports</b> | Select which protocols will be used to determine whether a host exists at each address, either <i>TCP</i> , <i>UDP</i> , or <i>TCP &amp; UDP</i> .<br>Discovery scans use these protocols in this order:<br><ol style="list-style-type: none"> <li>1 ARP</li> <li>2 ICMP, including <code>ping</code> and <code>tracert</code></li> <li>3 TCP <i>SYN</i> and TCP <i>RST</i> (reset) to the port numbers of 20 common services</li> <li>4 UDP port 53, including DNS, reverse DNS (RDNS), &amp; DNS zone transfer</li> <li>5 CIFS</li> </ol> <b>Tip:</b> To improve performance, use only necessary protocols, and configure the host to be responsive to ARP and/or ICMP. |
| <b>IP Range</b>   | Type a range of IP addresses that will be included in the discovery scan.<br><b>Note:</b> The IP range must be within a single subnet, and cannot include IP addresses that are not allowed in the ADOM selected in <i>Current ADOM</i> . For details, see “ <a href="#">Define your domains</a> ” on <a href="#">page 3</a> .  |
| <b>Schedule</b>   | Select when to start the discovery scan, either: <ul style="list-style-type: none"> <li>• <b>Run Now</b> — Generate a report when the profile is saved, and any time that you click <i>Run Now</i> for this profile in the list of scan profiles. No scheduled reports will be generated.</li> <li>• <b>Run Later</b> — Generate a report at scheduled intervals. You must configure the <i>Start Date</i> and <i>Time</i>, and select the recurrence pattern (either <i>Daily</i>, <i>Weekly</i>, or <i>Monthly</i>).</li> </ul>   |

**5** Click *OK*.

When a scheduled network discovery scan job completes, discovered hosts are automatically imported into *Asset > Inventory > Asset Inventory*, where they appear in the *All Assets* and the *Unprotected* asset groups.

The name “Unprotected” indicates only that they do not have a FortiScan agent installed. This is okay if you only require quarterly PCI DSS compliance checks.

If you want continuous monitoring or patch and configuration deployment that an agent-based solution can provide, see the [FortiScan Administration Guide](#).

## Group hosts to be scanned

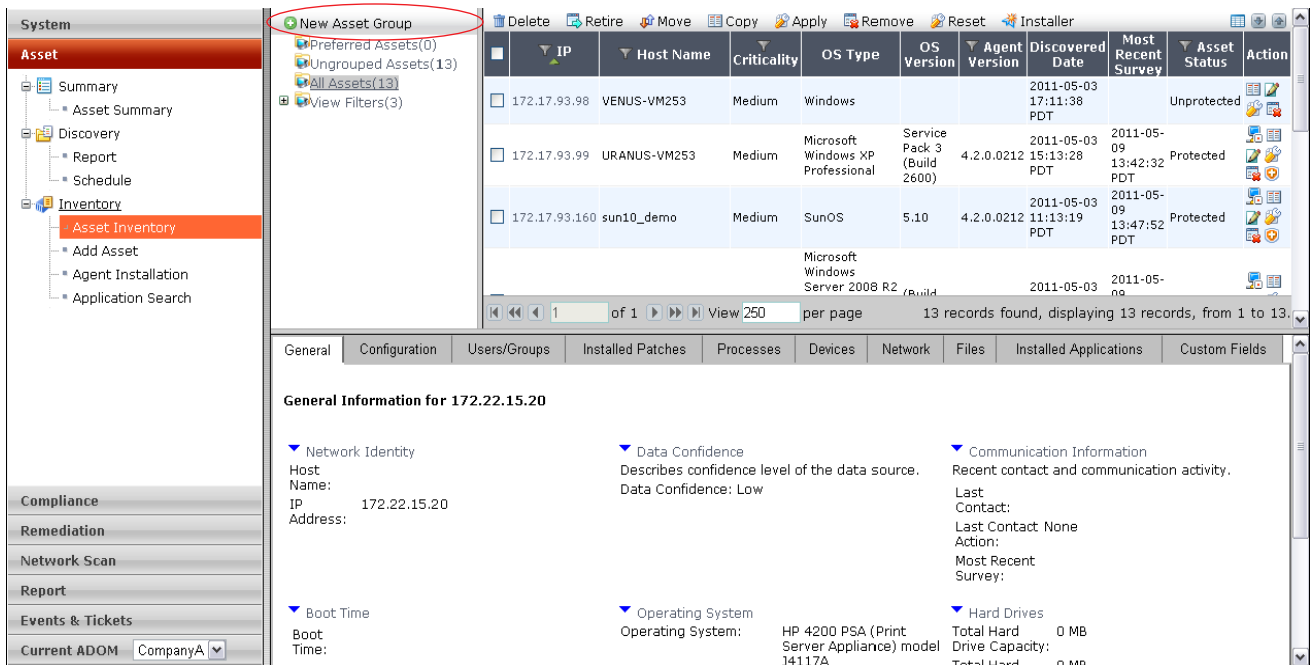
Do you want to scan all of your computers at once? Or do you want to scan them in batches?

If you do **not** want to scan them all at once, group your hosts into sets.

### To create an asset group

- 1 From *Current ADOM*, select an ADOM that is **not Global**.  
(Assets belong to specific ADOMs.)

2 Go to Asset > Inventory > Asset Inventory.



3 In the asset selection tree, click the *New Asset Group* button.

4 Configure the following:

**Create New Asset Group**

Name

Business Impact High

Asset Group Parent

- Preferred Assets(1)
- CompanyA\_assetGroup1(2)

**Group Default Authentication**

Windows Share(SMB)

SSH

Username   Enable Sudo

Password

RSA Private Key

DSA Private Key

SNMP v2c

**GUI item**                      **Description**

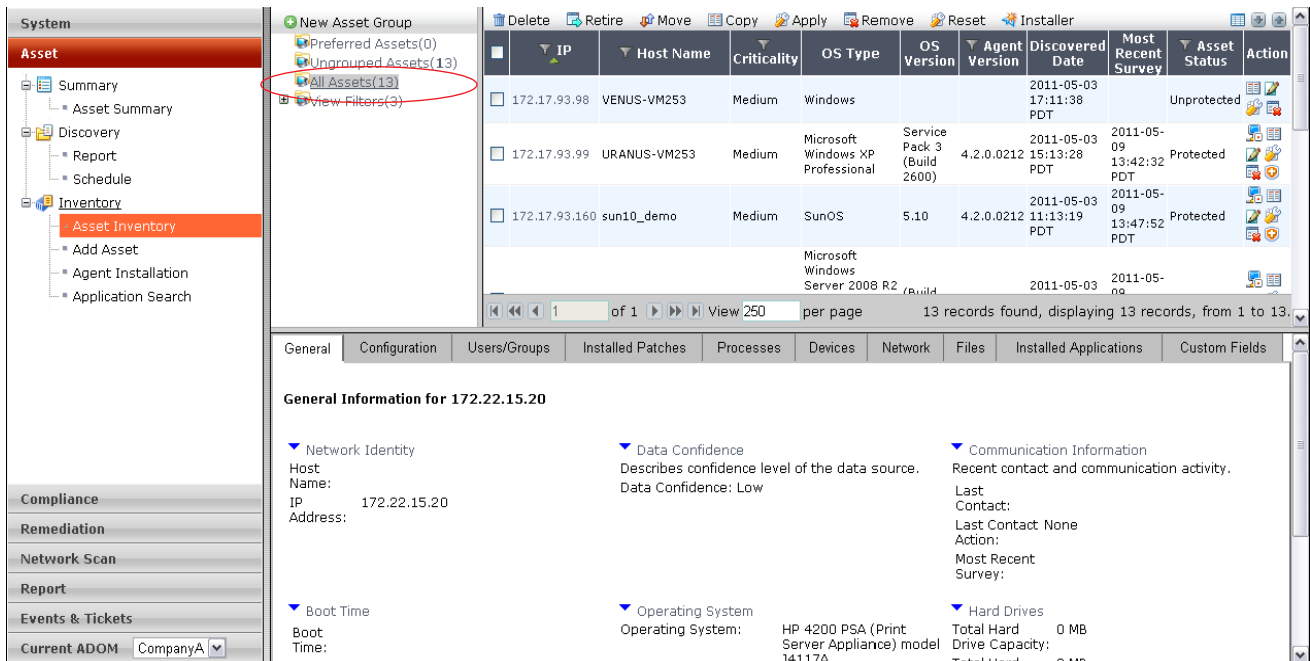
<b>Name</b>	Enter the name for the new asset group
<b>Asset Group Parent</b>	Select the parent group in which to include the new asset group. To create a top level group, select the <i>Preferred Assets</i> group as the parent. <b>Note:</b> Asset groups that are automatically created by the FortiScan appliance, such as <i>All Assets</i> , cannot be a group parent.

5 Click **OK**.

The **empty** new group appears in the asset selection tree under its parent group. Continue by adding assets to the group. (See “To add an asset to an asset group”.)

**To add an asset to an asset group**

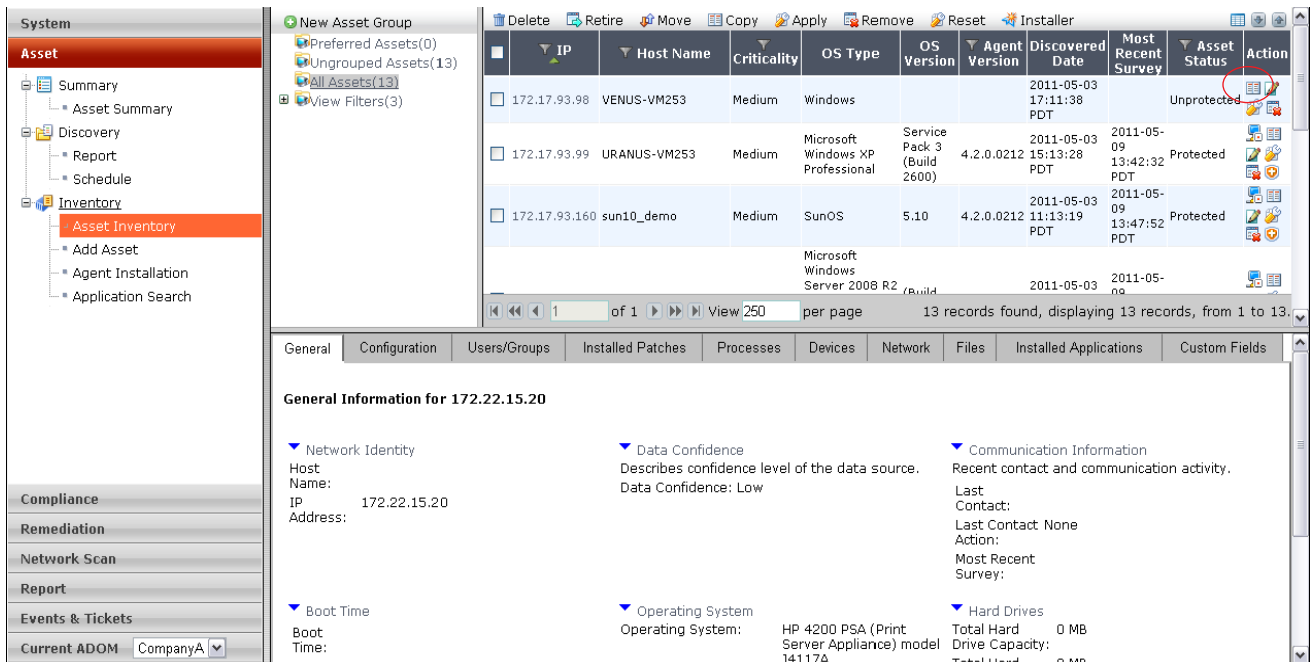
- 1 From *Current ADOM*, select an ADOM that is **not Global**.
- 2 Go to *Asset > Inventory > Asset Inventory*.



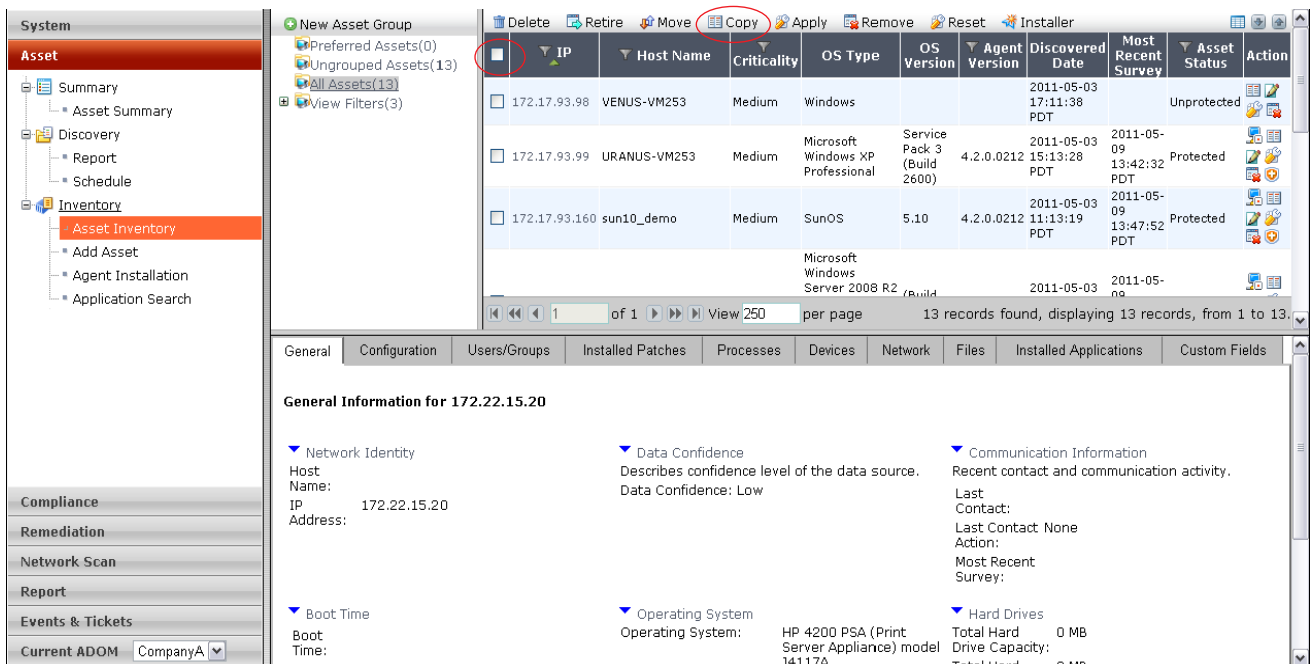
- 3 In the asset selection tree, click *All Assets*, *Ungrouped Assets*, or another group that already contains the asset.  
The contents of the group appear in the asset inventory pane, in the top right quadrant.

4 In the asset inventory pane, either:

- To add a single asset, in the row of the asset that you want to add, click the *Copy Asset/Group* icon.



- To add multiple assets, mark the check boxes for each asset that you want to add, then on the toolbar, click *Copy*.



The *Copy Asset* dialog appears in the asset editor pane.

- 5 In the dialog's *Asset Group Parent* tree, select the group to which you want to add the asset(s), and then click *OK*.

## Scheduling your PCI DSS scan

FortiScan can generate PCI reports according to whatever schedule you specify — no need to manually initiate them.



**Tip:** Time required to complete a remote vulnerability scan varies by:

- the number of target hosts
- the number of ports that you are scanning on each host
- whether the host responds quickly on those ports

For example, for a very comprehensive scan of many hosts that are not always responsive, the scan could take a couple of days to complete. For best results, wait for previous remote vulnerability scans to complete, and do not schedule scans concurrently.

- 1 Go to *Network Scan > Vulnerability Scan > Schedule*.
- 2 Click *Create New*.
- 3 Configure these settings:

GUI item	Description
<b>Name</b>	Type a name for the vulnerability scan report.
<b>Enable PCI Compliance</b>	Enable to use the pre-defined PCI DSS compliance scan profile. Enabling this option automatically selects the predefined PCI DSS scan profile ( <i>vcm_pci_profile</i> ) the <i>Profile</i> drop-down list. <i>Profile</i> then becomes read-only. Predefined scan profiles such as <i>vcm_pci_profile</i> are included with the firmware, and are updated by FortiGuard Vulnerability and Compliance Management service if you have subscribed.
<b>Asset Group</b>	Select which asset group to scan (see “Group hosts to be scanned” on page 7).

### Schedule

Select either:

- **Run Now** — Select to specify an on-demand scan and report. A scan will run and a report will be generated immediately after the schedule is saved, and also whenever the *Run Now* icon is manually clicked thereafter. (Reports will **not** be automatically periodically generated.) This is the default.
- **Run Later** — Select to have scan reports automatically generated at regular intervals. Also configure the times and dates of the recurring schedule.

### Output Option

#### File output

Mark the check boxes of the PCI DSS report file formats that you want. HTML is the format available as part of the GUI, and cannot be disabled.

#### Email/Upload

To have the report delivered to an e-mail address or FTP server, enable this option and enter the appropriate information.

#### 4 Click OK.

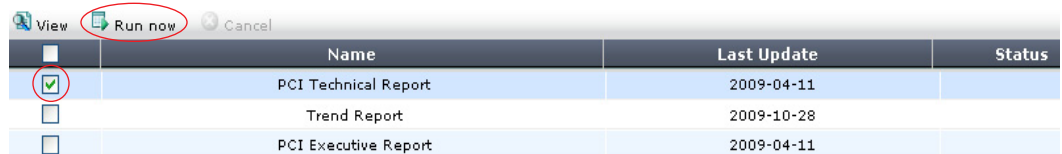
FortiScan will begin the scan now if you configured that. Otherwise, it will begin at the scheduled time. When the scan is complete, results will appear in *Network Scan > Vulnerability Scan > Report*. FortiScan generates two compliance reports, a *PCI Executive Report* and a *PCI Technical Report*, based on severity levels predefined by Fortinet.

## Generating your PCI DSS reports

Compliance report templates are pre-defined report formats designed to conform to PCI DSS requirements. If you subscribe to the FortiGuard Vulnerability and Compliance Management service, predefined templates are automatically updated.

### To generate a PCI DSS compliance report

- 1 From *Current ADOM*, select the name of an ADOM that is **not Global**.
- 2 Go to *Network Scan > Compliance Report > Template*.
- 3 In the row corresponding to the report that you want to generate, mark its check box, then click *Run now*.



<input type="checkbox"/>	Name	Last Update	Status
<input checked="" type="checkbox"/>	PCI Technical Report	2009-04-11	
<input type="checkbox"/>	Trend Report	2009-10-28	
<input type="checkbox"/>	PCI Executive Report	2009-04-11	

#### 4 Configure these settings:

Run Compliance Report

Report Name:

Report Title:

Asset Group:

**Period Scope**

Start Time:  End Time:

**Output Option**

File output:  HTML  PDF  MS Word  Text  MHT

Email/Upload

OK Cancel

<b>GUI item</b>	<b>Description</b>
<b>Report Name</b>	Type a report file name as it will appear in <i>Network Scan &gt; Compliance Report &gt; Report</i> . The date and time will be appended to the end of the name each time a compliance report is generated.
<b>Report Title</b>	Type a title that will appear inside the report. This field is automatically populated depending on the type of template you choose.
<b>Asset Group</b>	Select an asset group. The report results will be limited to the hosts defined in the asset group.
<b>Period Scope</b>	Select a start and end time. The report results will be limited to the time period you specify.
<b>Output Option</b>	
<b>File Output</b>	Select the formats in which the report will be generated. HTML is the default format. Any or all other available formats may be enabled.
<b>Email/Upload</b>	To have the report delivered to an e-mail address or FTP server, select this option and select the output settings or create a new one.

#### 5 Click OK.

The list of report templates appears again. To determine whether the report is in progress or complete, refresh the page and update the *Status* column by clicking the *Template* submenu. The scan is complete when the *Status* column is blank.

## Using your PCI DSS reports

Once you have generated your PCI DSS reports, review them for non-compliances.

### To view the list of non-compliant hosts

- 1 From *Current ADOM*, select the name of an ADOM that is **not Global**.  
(This is the ADOM whose report you will be viewing.)

- 2 Go to *Network Scan > Compliance Report > Report*.
- 3 Click the report's name to view the HTML version of the report. (If you generated the report in any additional file formats, you can click the link in the *Format* column to view one of those formats.)
- 4 In the *PCI Status* section, if any host's *Last Scan* is *Failed*, correct that computer to be compliant.

## PCI Status

PCI Status		
Live IP Addresses Scanned	Security Risk Rating	PCI Status
172.16.100.231	4	Failed
172.16.100.178	0	Passed
172.16.100.179	0	Passed

**Table 1: PCI Technical Report contents**

GUI item	Description
<b>Report Summary</b>	
<b>Created</b>	The date and time network map report was generated.
<b>Total Hosts</b>	The IP addresses or IP range of the computers that were live and responding during the scan.
<b>Summary From Date</b>	The starting date and time of the report generation.
<b>Summary To Date</b>	The ending date and time of the report generation.
<b>VM Engine Version</b>	The FortiGuard Vulnerability and Compliance Management engine version number and date of last update. This is updated via the FortiGuard Distribution Network if you are a FortiGuard Vulnerability Management service subscriber.
<b>VM Plugins Version</b>	The FortiGuard Vulnerability and Compliance Management module version number and date of last update. This is updated via the FortiGuard Distribution Network if you are a FortiGuard Vulnerability and Compliance Management service subscriber.
<b>PCI Status</b>	
<b>IP Addresses</b>	The IP address of the host that was scanned.
<b>Failed Times</b>	The number of times the host failed the PCI compliance scan.
<b>Passed Times</b>	The number of times the host passed the PCI compliance scan.
<b>PCI Disabled</b>	The number of times the host passed the PCI compliance scan with the PCI option disabled in scan schedule.
<b>Total Scanned Times</b>	The total number of times that FortiScan has scanned the host.
<b>Last Scan</b>	The status of the last scan. A PCI compliance status of <i>Passed</i> for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. A PCI compliance status of <i>Failed</i> for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the <a href="#">PCI Security Standards Council</a> , was detected on the host.
<b>Host Details</b>	The top 10 vulnerable hosts by vulnerabilities and by times.

**Table 1: PCI Technical Report contents**

<b>Vulnerability Detail</b>	The total number of vulnerabilities detected are presented by severity, category, and date. The top 20 vulnerabilities are also listed.
<b>Host</b>	All services and vulnerabilities found for each host. The vulnerabilities that cause the host to fail compliance are highlighted. This option is not available for PCI Executive Reports.
<b>Appendix</b>	Information about the PCI status and vulnerability levels.

**To resolve a host’s non-compliance**

- 1 In the *Hosts* section of the report, click the blue disclosure arrow next to the host’s IP address. This will reveal a list of vulnerability scans of that host.
- 2 Click the blue arrow next to a vulnerability scan date to reveal the list of discovered problems.
- 3 After the list of open ports, severity level and category summary, and OS fingerprint, in the *Vulnerability Information* subsection, click the blue arrow next to each severity level (*High, Medium, Low, or Information*) to expand the list of vulnerabilities at each level.
- 4 Resolve each problem by doing one of the suggested solutions for each vulnerability.

**Vulnerability Information**

High Total Vulnerabilities 3

(1) FID: 51 Title: Solans rpc.statd rpc Call Relaying Vulnerability

Risk Level	High
Port	111 (TCP)
Category	RPC
CVSS Score	10.0
CVE-ID	CVE-1999-0493 CVE-1999-0019 CVE-1999-0018
Bugtraq ID	
Vendor Reference	
IPS Signature	
Description	The rpc.statd utility is a daemon which co-operates with rpc.statd daemons on other hosts to provide a status monitoring service.
Impact	This servers has a long history of security holes,so we suggest that you disable this service.
Solution	Disable this service
Compliance	Not Applicable

(2) FID: 4192 Title: Apache mod\_proxy\_ftp Wildcard Characters Cross-Site Scripting

Risk Level	High
Port	80 (TCP)
Category	Web Server
CVSS Score	4.3
CVE-ID	CVE-2008-2939
Bugtraq ID	30560
Vendor Reference	Apache2.2 Apache2.0
IPS Signature	Apache Mod Proxy Ftp Wildcard Characters.XSS
Description	Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.
Impact	Successful exploitation could lead to cross-site scripting attacks if requests contain globbing characters.
Solution	Note that the remote web server may not actually be affected by these vulnerabilities. VM did not try to determine whether the affected modules are in use or to check for the issues themselves. Refer to the Apache Web site for more details. <a href="http://httpd.apache.org/security/vulnerabilities_20.html">http://httpd.apache.org/security/vulnerabilities_20.html</a> <a href="http://httpd.apache.org/security/vulnerabilities_22.html">http://httpd.apache.org/security/vulnerabilities_22.html</a>
Compliance	Not Applicable



**Tip:** FortiScan can automatically fix many of the vulnerabilities it can detect, significantly shortening your response time. For details, see the *FortiScan Administration Guide*.

## Your compliance “to do” list

Your PCI DSS reports contain the information that you need to resolve issues to bring your organization into compliance.

What if you want to divide the work among multiple people?

FortiScan can automatically assign tickets and track completion of your compliance work. It can even resolve some issues automatically. For details, see the *FortiScan Administration Guide*.

## **FortiScan 4.0 MR2 Patch 3 PCI DSS Jump Start**

10 January 2012 • 4th Edition

Copyright© 2012 Fortinet, Inc. All rights reserved. Contents and terms are subject to change by Fortinet without prior notice. Reproduction or transmission of this publication is encouraged.

Fortinet®, FortiGate®, FortiGuard®, FortiAnalyzer®, FortiClient®, FortiMail®, FortiManager®, FortiOS®, and TalkSwitch® are registered trademarks of Fortinet, Inc., in the United States and/or other countries. Other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners.

<b>Technical Documentation</b>	<a href="http://docs.fortinet.com">http://docs.fortinet.com</a>
<b>Knowledge Base</b>	<a href="http://kb.fortinet.com">http://kb.fortinet.com</a>
<b>Training</b>	<a href="http://training.fortinet.com">http://training.fortinet.com</a>
<b>Technical Support</b>	<a href="https://support.fortinet.com">https://support.fortinet.com</a>

Please report errors or omissions to:  
[techdoc@fortinet.com](mailto:techdoc@fortinet.com)