Easy-to-Use PCI Kit to Enable PCI Compliance Audits

Configuration Guide

Version 2.0 and Above

Table of Contents

Executive Summary

All organizations that handle payment card data must meet the requirements of the PCI DSS. ForeScout's CounterACT addresses 8 out of 12 PCI requirements. The CounterACT PCI Kit is easy to set up, and provides the reports to help you during a PCI audit.

About This Guide

The straightforward procedure for CounterACT PCI Kit setup and report generation is presented step-by-step in this guide. In addition, suggested steps for improving the level of PCI compliance using CounterACT automatic remediation and other tools are reviewed in the appendices.

What Is PCI?

The major players of the payment card industry (PCI) joined forces to create the Security Standards Council, of which ForeScout is a committee member. The PCI Council established and maintains the PCI data security standard (DSS), whose purpose is to ensure that information about cardholders and their transactions is secure and protected from data breach. All companies that handle payment card data are obliged to meet this standard or risk penalty.

ForeScout CounterACT

ForeScout CounterACT is the leading NAC solution, in use at global production networks of many Fortune 500 corporations. CounterACT is a clientless, out-of-band network appliance with a strong policy engine to detect, monitor, report and enforce corporate network access control policies.

PCI Requirements Addressed by the ForeScout PCI Kit

PCI Requirement 1

Install and maintain a firewall configuration to protect cardholder data.

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system's e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Requirement	Definition	ForeScout PCI Kit Solution
1	Install and maintain a firewall configuration to protect cardholder data	Monitors the firewall function by detailing all actual access made to the Card Holder Data Server Zone.
1.1.5	Documented list of services and ports necessary for business.	Provides a list of open TCP and UDP ports found open on PCI servers.
1.3.9	Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	Identifies Windows host without an active personal firewall.
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	Identifies all traffic attempts from the Card Holder Data Zone outside of the DMZ.
1.5	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	Detects hosts which can access the Internet without active NAT masquerading.

PCI Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Requirement	Definition	CounterACT Solution
2.2.1	Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	Verifies that Web, Database and DNS Servers are dedicated to their primary function.
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices specified function).	Detects potentially insecure FTP, Telnet and NetBIOS services on PCI Servers.

PCI Requirement 5

Use and regularly update anti-virus software or programs.

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

Requirement	Definition	CounterACT Solution
5.1	Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers). Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.	Detects Windows hosts without an installed anti-virus application.
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	Detects Windows hosts without an anti-spyware application.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Detects Windows hosts without an active up-to-date anti-virus application.

PCI Requirement 6

Develop and maintain secure systems and applications.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

Requirement	Definition	CounterACT Solution
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Identifies hosts without latest known security patches installed.
6.3.2	Separate development, test, and production environments.	Identifies all traffic attempts between PCI Development, Test and Production Zones.
6.3.3	Separation of duties between development, test, and production environments.	Identifies users attempting to access servers which they are not granted access to by their Active Directory group.

PCI Requirement 7

Restrict access to cardholder data by business need-to-know.

This requirement ensures critical data can only be accessed by authorized personnel.

Requirement	Definition	CounterACT Solution
7	Restrict access to cardholder data by business need-to-know.	Identifies users attempting to access cardholder information which they are not granted access to by their Active Directory group.

PCI Requirement 8

Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Requirement	Definition	CounterACT Solution
8.1	Identify all users with a unique user name before allowing them to access system components or cardholder data.	Detects all users on the network. This list can be examined to verify usernames are unique.
8.5.7	Communicate password procedures and policies to all users who have access to cardholder data.	Presents the password procedure to all the users that attempt to access the Card Holder Data Zone.

PCI Requirement 11

Regularly test security systems and processes.

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

Requirement	Definition	CounterACT Solution
11.1a	Test security controls, limitations, network connections and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	Detects access attempts by guests to the network. It will allow users to login to the network using HTTP login. It will block guests' access to the Card Holder servers
11.1b	Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	Detects NAT (potentially wireless) devices.
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Performs monthly vulnerability scan.
11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	Detects malicious activity using CounterACT Threat Protection engine.

PCI Requirement 12

Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

Requirement	Definition	CounterACT Solution
12	A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.	Presents the company's Information Security policy to all employees and requires employees to acknowledge that they have read and understood it. The policy URL is entered during the PCI template setup. The message is shown once a year.

Deploying CounterACT

Deploy the CounterACT appliances so that traffic going into and out of the PCI zones is monitored. Monitoring traffic to and from the Card Holder Data zone, and the Servers zone is extremely important. Understanding the zones is extremely important for a successful deployment. For further details about PCI zones, see Appendix 4: About PCI Zones.

Several of the following items are normally configured via the Initial Setup Wizard that runs when you startup CounterACT the first time. Before you proceed further, verify the following items required by the PCI template are configured.

- **Asset Classification** – If you have not already done so, run the Asset Classification template to organize your hosts into groups that are used by the PCI template policies. The template is found in the Policy Manager window.
- **LDAP Settings** – Make sure the following LDAP fields are configured in the CounterACT Options>Plugins>User Directory Plugin window: Server Address, Base DN (Fully Qualified Domain Name), and NetBIOS Domain Aliases.
- **LDAP User Groups –** The policies generated by the PCI template monitor user access to various servers in the network. Users with access rights to different PCI zones need to be grouped in the following LDAP groups:
  - *Card Holder Data*: Users with access rights to Card Holder Data servers.
  - *Production*: Users with access rights to the Production zone.
  - *Development*: Users with access rights to the Development zone.
  - *Test*: Users with access rights to the Test zone.
- **Host Property Scanner** – The HPS plugin should be configured so CounterACT can inspect network hosts using Domain credentials. SecureConnector should be deployed on hosts not manageable by the HPS. HPS parameters are found in Options>Host Property Scanner. The policies generated by the PCI template include optional predefined actions (disabled by default) that assist in deploying SecureConnector where needed.
- **Corporate Policies –** PCI compliance requires corporate policies for Password Change and Information Security. The PCI template will request the URLs where these policies are described.

How to Use the ForeScout PCI Kit

Step-by-step Instructions for PCI Kit Setup and PCI Report Generation

1. *Verify That You Have the Required Information*

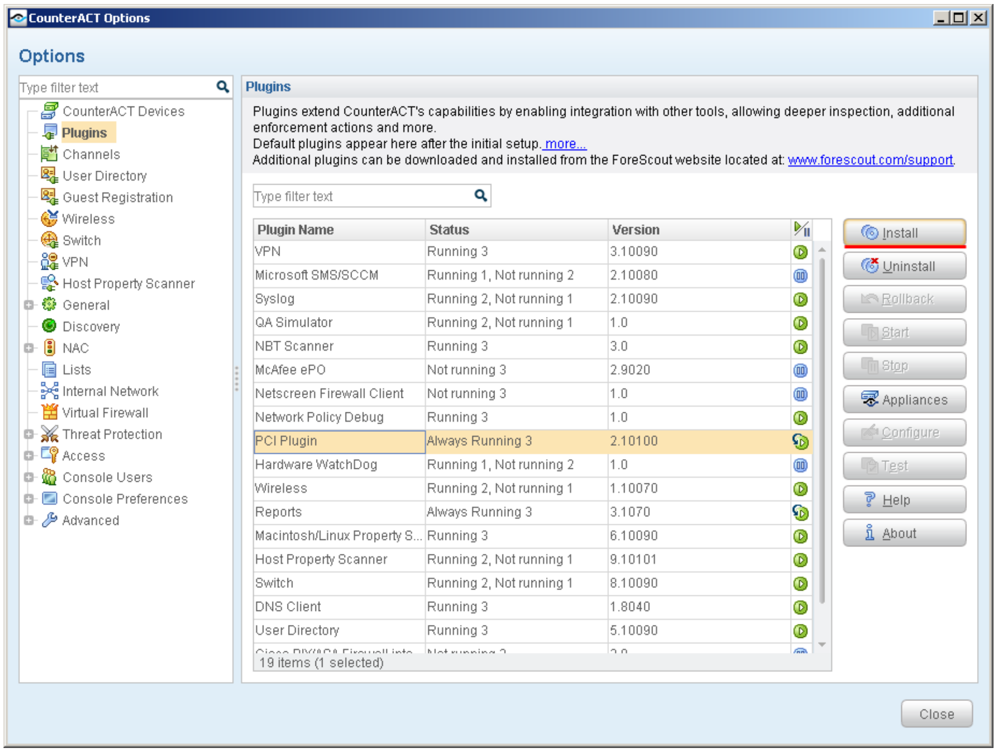
See Appendix 1: PCI Compliance Kit Checklist for details about the information you need to work with the compliance kit.

2. *Start CounterACT*

Double-click the CounterACT icon, and log in.

3. *Install the PCI Plugin*

Select **Options** at the top of the Console main screen to open the Options window.



Plugins extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more.
Default plugins appear here after the initial setup. more...
Additional plugins can be downloaded and installed from the ForeScout website located at: www.forescout.com/support.

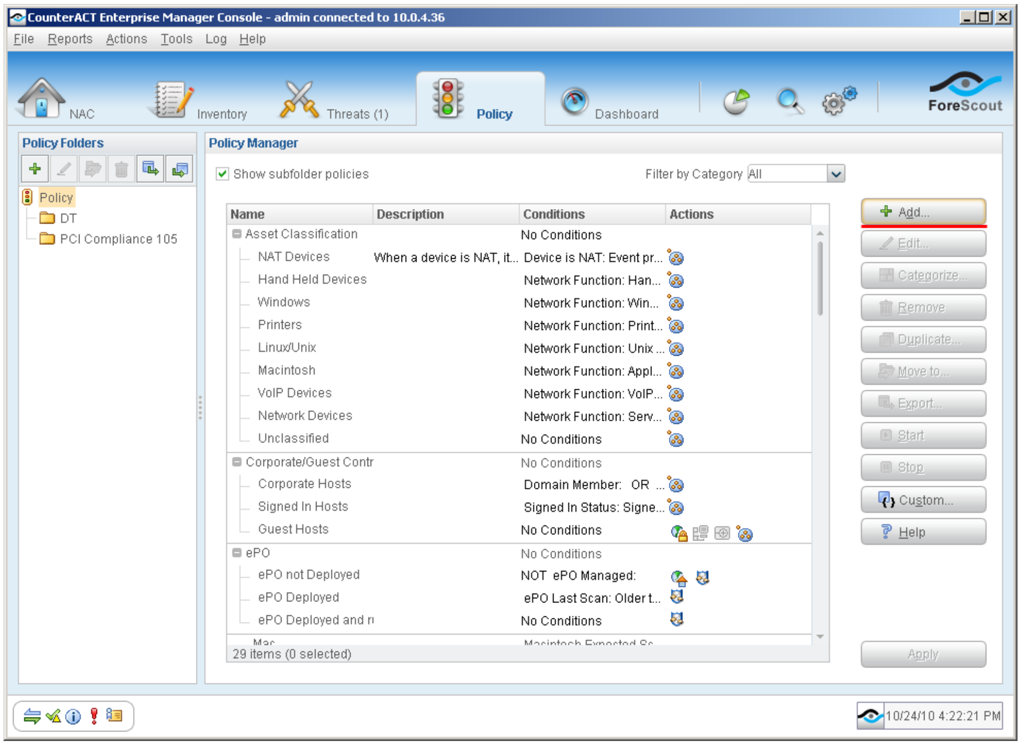
Plugin Name	Status	Version
VPN	Running 3	3.10090
Microsoft SMS/SCCM	Running 1, Not running 2	2.10080
Syslog	Running 2, Not running 1	2.10090
QA Simulator	Running 2, Not running 1	1.0
NBT Scanner	Running 3	3.0
McAfee ePO	Not running 3	2.9020
Netscreen Firewall Client	Not running 3	1.0
Network Policy Debug	Running 3	1.0
PCI Plugin	Always Running 3	2.10100
Hardware WatchDog	Running 1, Not running 2	1.0
Wireless	Running 2, Not running 1	1.10070
Reports	Always Running 3	3.1070
Macintosh/Linux Property S...	Running 3	6.10090
Host Property Scanner	Running 2, Not running 1	9.10101
Switch	Running 2, Not running 1	8.10090
DNS Client	Running 3	1.8040
User Directory	Running 3	5.10090

19 items (1 selected)

In the Options window, select **Plugins** on the left, then select **Install** on the right, then browse to the provided plugin FSP file and select it.

4. *Start the Policy Wizard*

Select **Policy** at the top of the Console main screen to open the Policy Manager. Select **Add** on the right side to start the wizard.



☑ Show subfolder policies

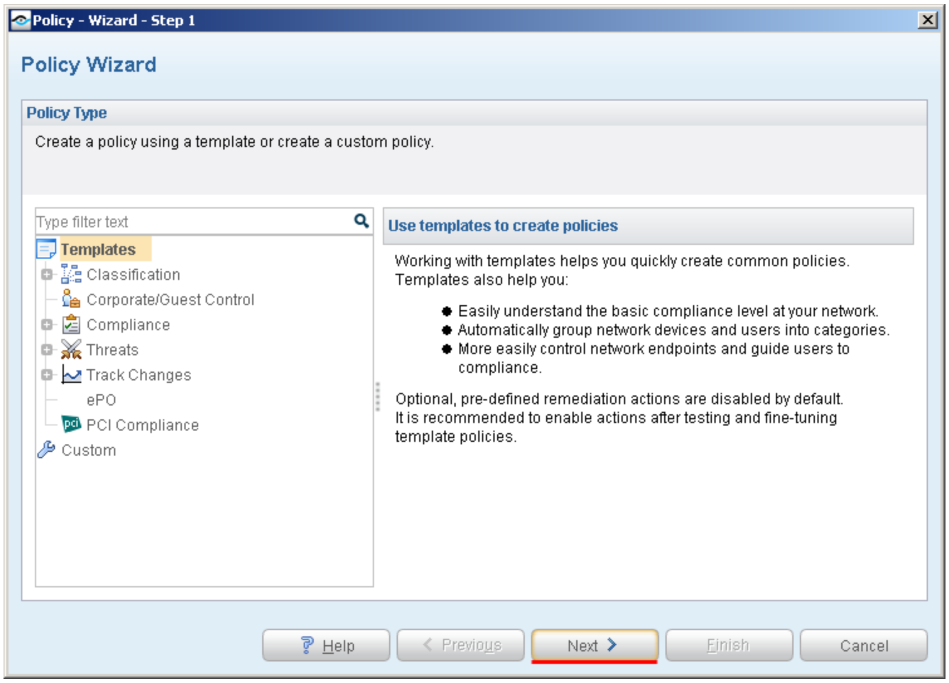
Filter by Category All

Name	Description	Conditions	Actions
⊟ Asset Classification		No Conditions	
NAT Devices	When a device is NAT, it...	Device is NAT: Event pr...	
Hand Held Devices		Network Function: Han...	
Windows		Network Function: Win...	
Printers		Network Function: Print...	
Linux/Unix		Network Function: Unix ...	
Macintosh		Network Function: Appl...	
VoIP Devices		Network Function: VoIP...	
Network Devices		Network Function: Serv...	
Unclassified		No Conditions	
⊟ Corporate/Guest Contr		No Conditions	
Corporate Hosts		Domain Member: OR ...	
Signed In Hosts		Signed In Status: Signe...	
Guest Hosts		No Conditions	
⊟ ePO		No Conditions	
ePO not Deployed		NOT ePO Managed:	
ePO Deployed		ePO Last Scan: Older t...	
ePO Deployed and r		No Conditions	
Mac		Macintosh Expected Sc	

29 items (0 selected)

5. *Generate PCI Policies and Segments Using the PCI Template*

In the Policy Wizard, select the **PCI Compliance** template and then select **Next**.



Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

Use templates to create policies

Working with templates helps you quickly create common policies. Templates also help you:

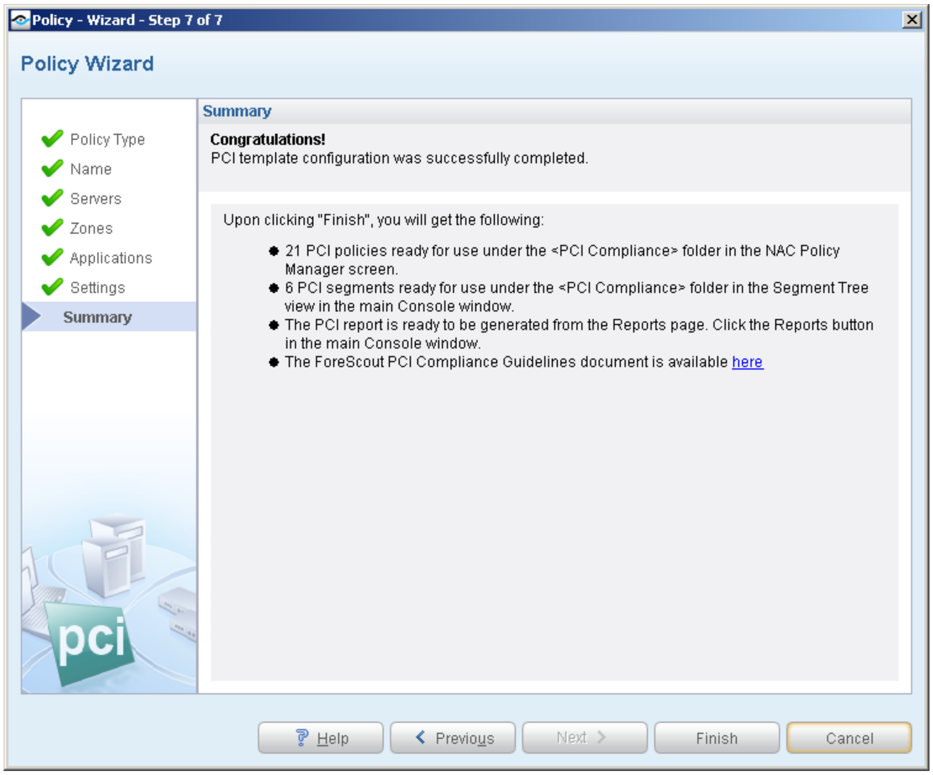
- Easily understand the basic compliance level at your network.
- Automatically group network devices and users into categories.
- More easily control network endpoints and guide users to compliance.

Optional, pre-defined remediation actions are disabled by default. It is recommended to enable actions after testing and fine-tuning template policies.

In the Policy wizard, follow the on-screen instructions to configure:

– Name of folder under which the PCI policies and segments will reside

- IP ranges of the PCI servers and zones
- Domain parameters
- Names of the LDAP user groups that have access to the PCI zones: Cardholder Data, Production, Test and Development.
- Corporate Policy URLs with the Password Change Policy and the Information Security Policy
- Corporate-approved anti-virus and anti-spyware vendors



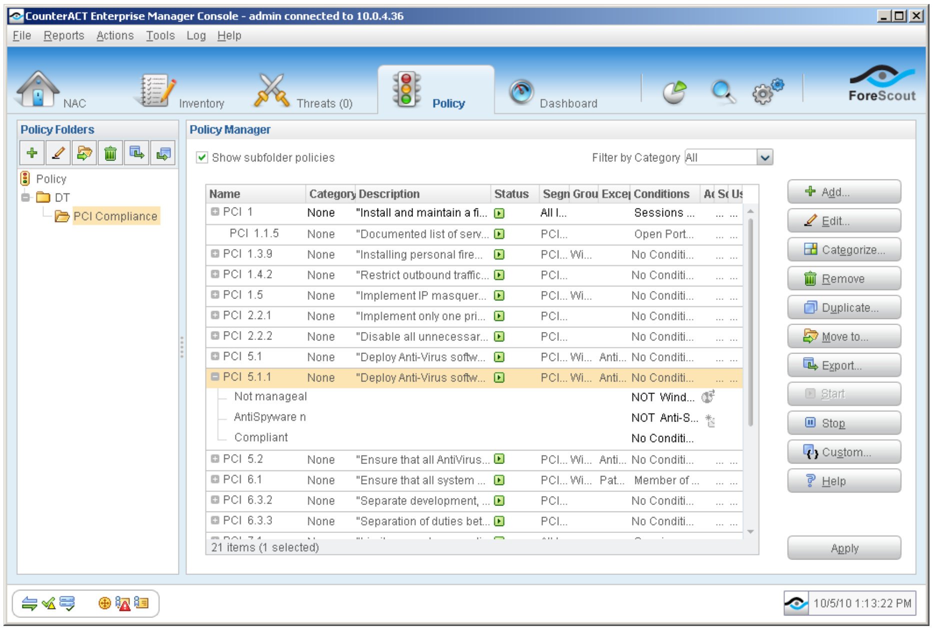
Summary

Congratulations!
PCI template configuration was successfully completed.

Upon clicking "Finish", you will get the following:

- 21 PCI policies ready for use under the <PCI Compliance> folder in the NAC Policy Manager screen.
- 6 PCI segments ready for use under the <PCI Compliance> folder in the Segment Tree view in the main Console window.
- The PCI report is ready to be generated from the Reports page. Click the Reports button in the main Console window.
- The ForeScout PCI Compliance Guidelines document is available here

CounterACT automatically generates over twenty PCI policies, with each policy named after its respective PCI requirement. The policies are arranged under the folder you specified; select the folder to view the policies.



☑ Show subfolder policies

Filter by Category All

Name	Category	Description	Status	Segn	Grou	Excep	Conditions	Ac	Sc	Us
⊞ PCI 1	None	"Install and maintain a fi...	▶	All I...			Sessions ...	...	...	
PCI 1.1.5	None	"Documented list of serv...	▶	PCI...			Open Port...	...	...	
⊞ PCI 1.3.9	None	"Installing personal fire...	▶	PCI...	Wi...		No Conditi...	...	...	
⊞ PCI 1.4.2	None	"Restrict outbound traffic...	▶	PCI...			No Conditi...	...	...	
⊞ PCI 1.5	None	"Implement IP masquer...	▶	PCI...	Wi...		No Conditi...	...	...	
⊞ PCI 2.2.1	None	"Implement only one pri...	▶	PCI...			No Conditi...	...	...	
⊞ PCI 2.2.2	None	"Disable all unnecessar...	▶	PCI...			No Conditi...	...	...	
⊞ PCI 5.1	None	"Deploy Anti-Virus softw...	▶	PCI...	Wi...	Anti...	No Conditi...	...	...	
⊟ PCI 5.1.1	None	"Deploy Anti-Virus softw...	▶	PCI...	Wi...	Anti...	No Conditi...	...	...	
Not manageal							NOT Wind...			
AntiSpyware n							NOT Anti-S...			
Compliant							No Conditi...			
⊞ PCI 5.2	None	"Ensure that all AntiVirus...	▶	PCI...	Wi...	Anti...	No Conditi...	...	...	
⊞ PCI 6.1	None	"Ensure that all system ...	▶	PCI...	Wi...	Pat...	Member of ...	...	...	
⊞ PCI 6.3.2	None	"Separate development, ...	▶	PCI...			No Conditi...	...	...	
⊞ PCI 6.3.3	None	"Separation of duties bet...	▶	PCI...			No Conditi...	...	...	

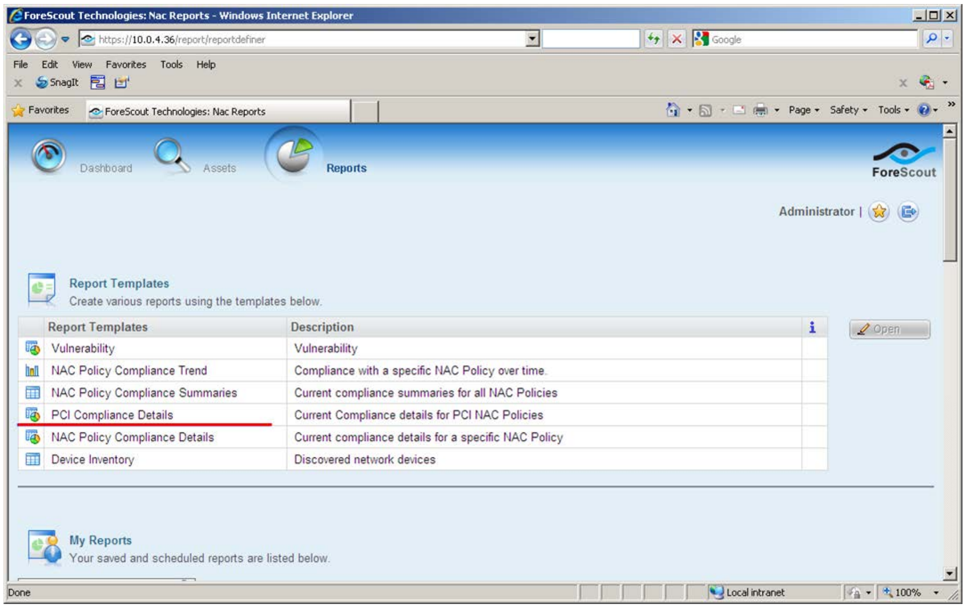
21 items (1 selected)

The PCI template automatically defines network segments under the folder you specified. To view the segments, select **Segment Manager** from the Tools menu in the Console main screen.

6. *Generate the PCI Compliance Report*

🗎 *Before generating the PCI report, it is recommended to review the PCI policy detections on the Console main screen and fine-tune the policies where needed.*

Select **Reports** at the top of the Console main screen to open the Reports web page. Select **PCI Compliance** to generate the report.


ForeScout Technologies: Nac Reports - Windows Internet Explorer
https://10.0.4.36/report/reportdefiner
Google
File Edit View Favorites Tools Help
SnagIt
Favorites
ForeScout Technologies: Nac Reports
Page Safety Tools
Dashboard
Assets
Reports
ForeScout
Administrator |
Open
Done
Local intranet
100%

Report Templates

Create various reports using the templates below.

Report Templates	Description
Vulnerability	Vulnerability
NAC Policy Compliance Trend	Compliance with a specific NAC Policy over time.
NAC Policy Compliance Summaries	Current compliance summaries for all NAC Policies
PCI Compliance Details	Current Compliance details for PCI NAC Policies
NAC Policy Compliance Details	Current compliance details for a specific NAC Policy
Device Inventory	Discovered network devices

My Reports

Your saved and scheduled reports are listed below.

When the generation page appears, you can select the PCI requirements to appear in the report. You can also schedule the report to run regularly at a specified time and have it sent by email.

To generate the report, select **Generate Report Now** at the bottom of the page. The PCI report is described in the next section.

Review the report and follow the guidelines in the appendices to remediate where you need to improve your PCI compliance level to better prepare yourself for the PCI audit.

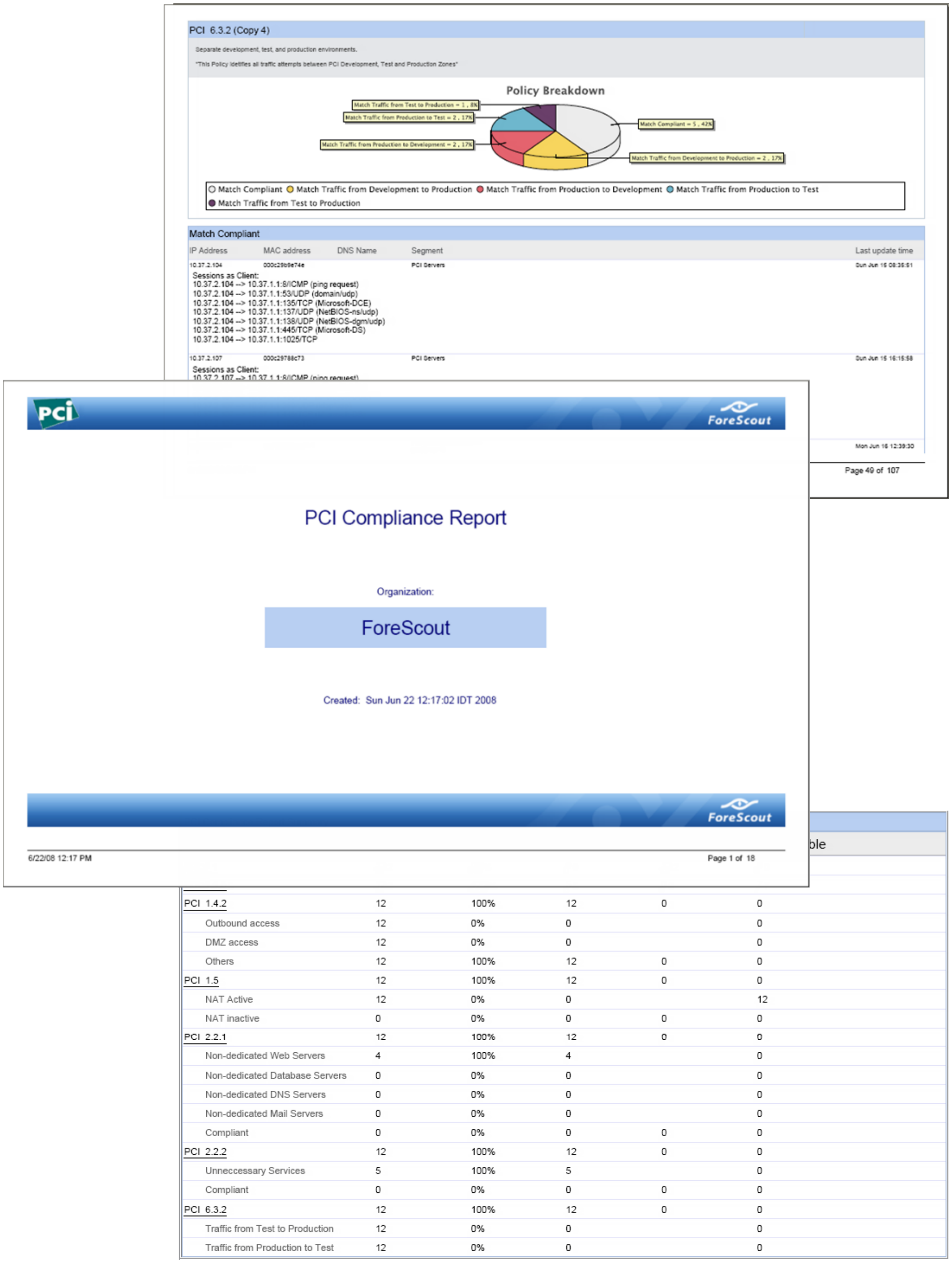
7. ***Deliver the PCI Report to the PCI Assessor***

The PCI Compliance Report is now ready for the PCI Assessor. Schedule, print or email the PCI report and provide it to your Assessor.

Improve your PCI compliance level by following the guidelines in the appendices, according to the audit results.

The ForeScout PCI Compliance Report

The PCI report shows network and device information required for a PCI audit. The report is organized according to the PCI requirements, with each section beginning with the relevant PCI requirement number.



PCI 6.3.2 (Copy 4)

Separate development, test, and production environments.

"This Policy idetifies all traffic attempts between PCI Development, Test and Production Zones"

Policy Breakdown

Match Traffic from Test to Production = 1 , 8%
Match Traffic from Production to Test = 2 , 17%
Match Traffic from Production to Development = 2 , 17%
Match Compliant = 5 , 42%
Match Traffic from Development to Production = 2 , 17%
○ Match Compliant
● Match Traffic from Development to Production
● Match Traffic from Production to Development
● Match Traffic from Production to Test
● Match Traffic from Test to Production

Match Compliant

IP Address	MAC address	DNS Name	Segment	Last update time
10.37.2.104	000c29b9e74e		PCI Servers	Sun Jun 15 08:35:51
10.37.2.107	000c29788c73		PCI Servers	Sun Jun 15 16:15:58
				Mon Jun 16 12:39:30

```
Sessions as Client:
10.37.2.104 --> 10.37.1.1:8/ICMP (ping request)
10.37.2.104 --> 10.37.1.1:53/UDP (domain/udp)
10.37.2.104 --> 10.37.1.1:135/TCP (Microsoft-DCE)
10.37.2.104 --> 10.37.1.1:137/UDP (NetBIOS-ns/udp)
10.37.2.104 --> 10.37.1.1:138/UDP (NetBIOS-dgm/udp)
10.37.2.104 --> 10.37.1.1:445/TCP (Microsoft-DS)
10.37.2.104 --> 10.37.1.1:1025/TCP
```

```
Sessions as Client:
10.37.2.107 --> 10.37.1.1:8/ICMP (ping request)
```

Page 49 of 107

PCI Compliance Report

Organization:

ForeScout

Created: Sun Jun 22 12:17:02 IDT 2008

6/22/08 12:17 PM

Page 1 of 18

ble

PCI 1.4.2	12	100%	12	0	0
Outbound access	12	0%	0		0
DMZ access	12	0%	0		0
Others	12	100%	12	0	0
PCI 1.5	12	100%	12	0	0
NAT Active	12	0%	0		12
NAT inactive	0	0%	0	0	0
PCI 2.2.1	12	100%	12	0	0
Non-dedicated Web Servers	4	100%	4		0
Non-dedicated Database Servers	0	0%	0		0
Non-dedicated DNS Servers	0	0%	0		0
Non-dedicated Mail Servers	0	0%	0		0
Compliant	0	0%	0	0	0
PCI 2.2.2	12	100%	12	0	0
Unneccessary Services	5	100%	5		0
Compliant	0	0%	0	0	0
PCI 6.3.2	12	100%	12	0	0
Traffic from Test to Production	12	0%	0		0
Traffic from Production to Test	12	0%	0		0

Appendix 1: PCI Compliance Kit Checklist

To perform a complete PCI Audit, fill the checklist below prior to using the PCI Kit.

Item	Description
DMZ	Servers facing the Internet.
Cardholder Data Zone	Servers holding payment card data.
PCI Servers Zone	Other servers participating in the payment application(s).
PCI Production Zone	All clients of the payment application(s).
Test Zone	A segment in which the application(s) are tested before going into production. Specify an unused IP range if PCI application testing environment is not implemented.
Development Zone	A segment used to develop the payment application(s). Specify an unused IP range if development environment is not implemented.
Personal Firewall	Personal firewall(s) required to run on desktops and servers.
Anti-Virus	Anti-virus application(s) approved for use on desktops and servers.
Anti-Spyware	Anti-spyware application(s) approved for use on desktops and servers.
Admin Email	The email of the person administering PCI compliance.
Authentication Server Address	The IP address of the LDAP (ActiveDirectory) server to be used for authenticating guests (default extracted automatically out of the User Directory plugin configuration).
Domain Name	The Windows fully qualified domain name (default extracted automatically out of the User Directory plugin configuration).
NetBIOS Domain	The Windows NetBIOS Domain name (default extracted automatically out of the User Directory plugin configuration).
LDAP Card Holder Data Group	The name of the LDAP (ActiveDirectory) group that must include every user accessing the CHD zone.
LDAP Production Group	The name of the LDAP (ActiveDirectory) group that must include every user accessing the Production zone.
LDAP Test Group	The name of the LDAP (ActiveDirectory) group that must include every user accessing the Test zone.
LDAP Development Group	The name of the LDAP (ActiveDirectory) group that must include every user accessing the Development zone.
Cardholder Password Procedure and Policies URL	A URL page containing the password procedure and policies of which users accessing the CHD zone must be aware.
Company Information Security URL	A URL page containing the company Accepted Use Policy of which all users must be aware.

Appendix 2: How to Use the ForeScout PCI Kit to Improve the Level of PCI Compliance

The PCI report contains useful information that can be used to detect and help deal with hosts that are not in compliance with the PCI specification. The table below goes section-by-section through the report, explaining how to use the PCI Kit not merely to audit PCI, but also to remediate, improve and help achieve compliance.

PCI Requirement 1

Report Section	Contains	How to Improve PCI Compliance Level
1.1.5	**A list of open TCP and UDP ports.**	**Review the list of open ports, and close all ports that are unnecessary for business.**
1.3.9	**A list of Windows host without active personal firewalls.**	**Review the list of hosts without a firewall, and implement a firewall on all hosts that have direct connectivity to the Internet.**
1.4.2	**A list of all traffic attempts from the Card Holder Data Zone (CHDZ) out to the Demilitarized Zone (DMZ).**	**Restrict traffic from the Card Holder Data Zone (CHDZ) to the Demilitarized Zone (DMZ); you can do this by activating the predefined firewall action in this policy (see Appendix 5). Afterwards, review the list of traffic attempts in the Console main screen (select the PCI 1.4.2 policy to filter for relevant hosts) to verify access restrictions are sufficient.**
1.5	**A list of hosts without active NAT masquerading.**	**Implement IP masquerading using technologies such as PAT or NAT. Review the list of hosts without active NAT masquerading, and remediate them as required.**

PCI Requirement 2

Report Section	Contains	How to Improve PCI Compliance Level
2.2.1	**A list of Web, Database, DNS and Mail Servers that are NOT dedicated to their primary function.**	**Review the list of non-dedicated servers and close unnecessary ports to make sure the servers are dedicated to their original role.**
2.2.2	**A policy that detects potentially insecure FTP, Telnet and NetBIOS services on PCI Servers.**	**Review the list of available services and disable all unnecessary and insecure services and protocols (services and protocols not directly required to perform the devices specified function).**

PCI Requirement 5

Report Section	Contains	How to Improve PCI Compliance Level
5.1	A list of Windows hosts without an installed anti-virus application.	Review the list of hosts without anti-virus applications, and install the corporate approved anti-virus application. Several methods of remediation are available in the predefined actions in this policy, ready for you to activate the desired combination (see Appendix 5). Options include sending an email to inform the Network Administrator, asking the user via email or HTTP hijack to contact the Help Desk, and hijacking the host and preventing network access until compliance is reached. And for hosts that are not manageable, a predefined action is available to install SecureConnector so they can be managed.
5.1.1	A list of Windows hosts without an installed anti-spyware application.	Review the list of hosts without an anti-spyware application and install the application. Automatic remediation options are identical to those in 5.1 above.
5.2	A list of Windows hosts without an active up-to-date anti-virus application.	Review the list of hosts without up-to-date anti-virus protection and update them. Automatic remediation options includes those are identical to those in 5.1 above, and also include the option of automatic, seamless update of the anti-virus directly from the Internet.

PCI Requirement 6

Report Section	Contains	How to Improve PCI Compliance Level
6.1	A list of hosts without the latest known security patches installed.	Review the list of hosts without the latest patches, and update those hosts. Several methods of remediation are available in the predefined actions in this policy, ready for you to activate the desired combination (see Appendix 5). Options include asking the user via email to perform Windows Update, or initiating a Windows update with the Microsoft server or from a local WSUS server. And for hosts that are not manageable, a predefined action is available to install SecureConnector so they can be managed.
6.3.2	A list of traffic attempts between the Development, Test and Production Zones.	Activate the predefined virtual firewall actions to separate the Development, Test and Production environments (see Appendix 5). Review the list of traffic attempts provided in the report to verify access restrictions are sufficient.

6.3.3	A list of users attempting to access servers which they are not granted access to by their Active Directory group.	Activate the predefined virtual firewall actions to separate duties between the Development, Test and Production environments (see Appendix 5). Review the list of traffic attempts provided in the report to verify access restrictions are sufficient.

PCI Requirement 7

Report Section	Contains	How to Improve PCI Compliance Level
7	A list of users attempting to access cardholder information which they are not granted access to by their Active Directory group.	Review the list of access attempts to verify that the Active Directory groups you previously setup are sufficiently restricting access to cardholder information. For efficient remediation, you can activate the predefined action defined in the policy (see Appendix 5). This action enacts a virtual firewall that blocks unauthorized users from accessing the Production Zone.

PCI Requirement 8

Report Section	Contains	How to Improve PCI Compliance Level
8.1	A list of all users detected on the network. This list can be examined to verify usernames are unique	Review the list of usernames and verify that each individual has a username, and that usernames are unique.

PCI Requirement 11

Report Section	Contains	How to Improve PCI Compliance Level
11.1a	A list of access attempts by guests to the network.	Review the list annually to assure the ability to adequately identify and to stop any unauthorized access attempts. A predefined action is available to automatically require users to login to the network using HTTP login. This blocks guest access to the Card Holder services. To remediate, activate this action (see Appendix 5).
11.1b	Al list of NAT (potentially wireless) devices.	Review the list annually to assure the ability to adequately identify and to stop any unauthorized access attempts via wireless devices.

11.2	**A list of found vulnerabilities.**	**Review the list at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).**
11.4	**A list of detected malicious activity.**	**Review the list on a regular basis.** **A predefined action is available in the policy to automatically send an email to the administrator when a malicious activity is detected. The Threat Protection engine can be set to automatically block malicious sources. To remediate, activate this action (see Appendix 5).**

PCI Requirement 12

Report Section	Contains	How to Improve PCI Compliance Level
12	**A policy with a predefined action for exposing users to company policies on a regular basis.**	**A predefined action is available to hijack hosts and require users to confirm that they have read the relevant company policy. To remediate, activate this action (see Appendix 5).**

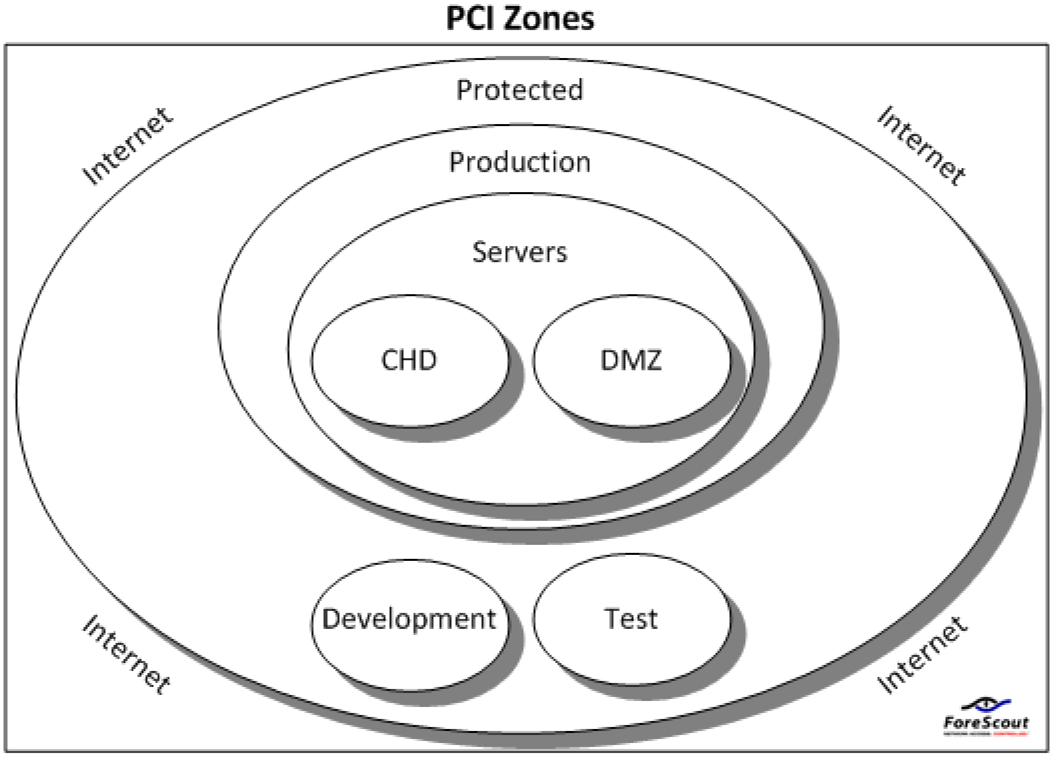
Appendix 3: Addressing the Remaining PCI Requirements

Requirements not directly addressed by ForeScout's CounterACT PCI Kit can be handled using standard technologies, procedures and documentation as described below.

Requirement	Description	How to Comply
3	**Protect stored cardholder data** Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed and not sending PAN in unencrypted e-mails.	Use encryption software to encipher cardholder data. Develop and enforce policies that limit storage of cardholder data to instances where it is absolutely necessary. NOTE: Encryption software can also be used to fulfill requirement 8.4 regarding password encryption.
4	**Encrypt transmission of cardholder data across open, public networks.** Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.	Similar to requirement 3, use encryption software to encipher text as it is sent over risky connections. Develop and enforce a policy of not sending unencrypted PANs by email.
9	**Restrict physical access to cardholder data** Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.	Setup systems for controlling and monitoring physical access to devices with sensitive information, including remote backup storage and devices in transit.
10	**Track and monitor all access to network resources and cardholder data** Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.	Use time synchronization software such as the Windows Time Service to synchronize critical system clocks to meet requirement 10.4. Use audit trail software to secure and store audit trails to meet requirements 10.5 and 10.7. Review logs every day to meet requirement 10.6.

Appendix 4: About PCI Zones

The PCI DSS divides the network hosts into various zones. To fulfill PCI requirements, traffic into and out of these zones needs to monitored, especially traffic into and out of the CHD and Servers zones. For more information about CounterACT deployment, refer to the CounterACT Installation Guide.



PCI zones include:

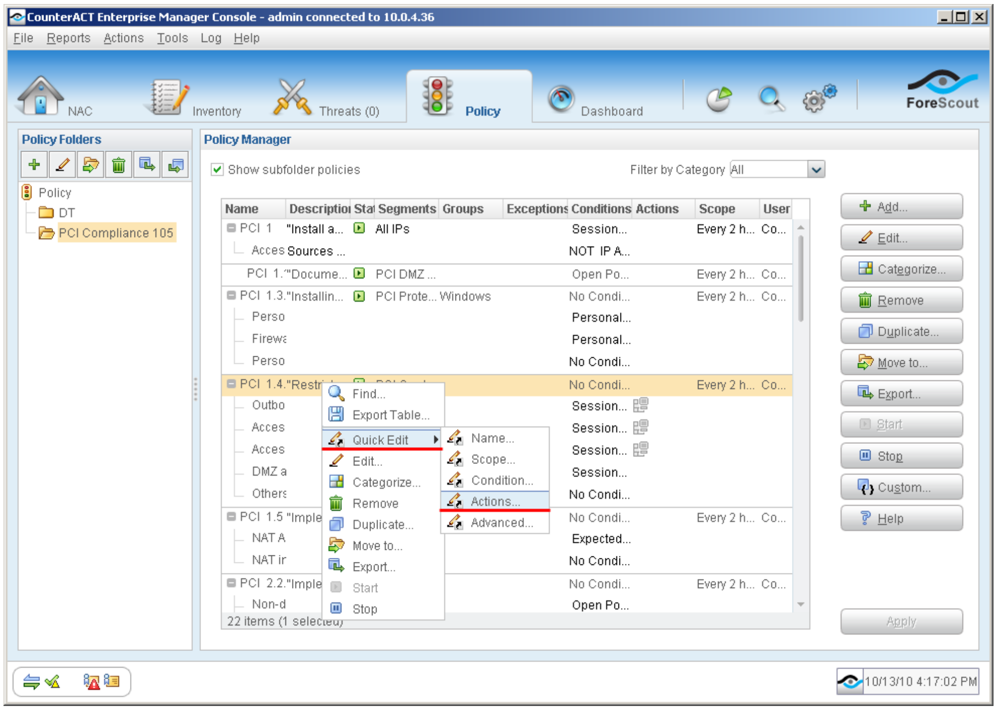
- **Card Holder Data (CHD) Zone** – Servers that contain card holder data, which is defined as the magnetic stripe or the Primary Account Number (PAN), plus one or more of the following: cardholder name, expiration date and service code.
- **De-militarized Zone (DMZ)** – Servers accessible from the Internet.
- **Servers Zone** – This zone includes the CHD, DMZ and Production servers.
- **Production Zone** – In addition to the contents of the Servers zone, this zone includes non-server devices in Production (such as clients).
- **Development Zone** – Used for Development, this zone must be separate from the Production zone, though it may overlap with the Test zone.
- **Test Zone** – Used for QA, this zone must be separate from the Production zone.
- **Protected Zone** – The sum of the Production, Development and Test zones.
- **Internet Zone** – This zone is everything outside the Protected zone.

Appendix 5: Activating Predefined Actions in PCI Policies

Several PCI polices include optional predefined actions to help with remediation. The actions are disabled by default, and you can easily activate them as described here.

1. ***Start the Policy Wizard***

   Select **Policy** at the top of the Console main screen to open the Policy Manager.



☑ Show subfolder policies   Filter by Category All

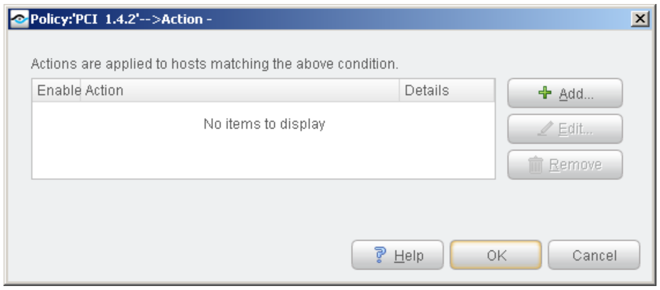
Name	Descriptio	Sta	Segments	Groups	Exceptions	Conditions	Actions	Scope	User
PCI 1	"Install a...	▶	All IPs			Session...		Every 2 h...	Co...
Acces	Sources ...					NOT IP A...			
PCI 1.	"Docume...	▶	PCI DMZ ...			Open Po...		Every 2 h...	Co...
PCI 1.3.	"Installin...	▶	PCI Prote...	Windows		No Condi...		Every 2 h...	Co...
Perso						Personal...			
Firewa						Personal...			
Perso						No Condi...			
PCI 1.4.	"Restr					No Condi...		Every 2 h...	Co...
Outbo						Session...	▦		
Acces						Session...	▦		
Acces						Session...	▦		
DMZ a						Session...			
Others						No Condi...			
PCI 1.5	"Imple					No Condi...		Every 2 h...	Co...
NAT A						Expected...			
NAT ir						No Condi...			
PCI 2.2.	"Imple					No Condi...		Every 2 h...	Co...
Non-d						Open Po...			

22 items (1 selected)

Select your PCI Compliance folder in the left pane to view your PCI policies. Policies with predefined actions show icons in the **Actions** column. Right-click a row, select **Quick Edit**, and then select **Actions**.

2. ***Activate the Predefined Actions***

   Select the checkbox next to the actions that you want to activate, and select **OK**.



Actions are applied to hosts matching the above condition.

Enable Action	Details
No items to display	

Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2015. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

May 2015