



# PCI DSS 1.2 Wireless Compliance Report

For: Demo Corp

From: Jul 27, 2009 3:17 PM

To: Aug 26, 2009 3:17 PM

At: Demo Corp

A Report by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043

[www.airtightnetworks.com](http://www.airtightnetworks.com)



# Table of Contents

<b>RESULT SUMMARY</b> .....	3
<b>RECOMMENDED ACTIONS</b> .....	5
<b>CATEGORIZED VIOLATIONS SUMMARY</b> .....	7
PCI GUIDELINE - REQUIREMENT 1.2 .....	7
<i>Non-authorized Client Connections</i> .....	7
<i>Misbehaving Clients</i> .....	8
<i>Rogue Access Points</i> .....	8
<i>Open Authorized Access Points</i> .....	9
PCI GUIDELINE - REQUIREMENT 2.1.1 .....	10
<i>Open Authorized Access Points</i> .....	10
PCI GUIDELINE - REQUIREMENT 2.2 .....	11
<i>Authorized AP using Vulnerable SSID</i> .....	11
<i>WEP Authorized Access Points</i> .....	12
PCI GUIDELINE - REQUIREMENT 4.1.1 .....	12
<i>Open Authorized Access Points</i> .....	13
<i>WEP Authorized Access Points</i> .....	13
PCI GUIDELINE - REQUIREMENT 12.9 .....	14
<i>Honey-pot Attack</i> .....	14
<i>MAC Spoofing</i> .....	15
<b>ABOUT THIS REPORT</b> .....	17

## Result Summary

**Report Generated On:** Aug 26 2009, 03:17 PM (GMT -0700)

**Scan Duration:**

From: Jul 27, 2009 3:17 PM

To: Aug 26, 2009 3:17 PM

**Wireless Scanners - Total: 8**

Approximate area scanned for wireless vulnerabilities: 160000 sq. ft

You can add more scanners for covering additional airspace if necessary.

**Wireless Devices Detected - Total:** Access Points - 127 Clients - 2405

Relevant PCI DSS 1.2 requirements	How this report helps	Violations Count
Requirement 1.2: Build a firewall configuration that restricts connections between untrusted networks and the cardholder data environment.	This report provides a list of untrusted wireless devices that may open backdoors to cardholder data environment. These devices may allow unauthorized access to cardholder data bypassing wired firewalls.	13
Requirement 2.1.1: For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	This report identifies authorized wireless access points using vendor default SSIDs or security configuration.	1
Requirement 2.2: Develop configuration standards for all system components (including any wireless access points & clients). It also requires the institution to assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening procedures.	This report authorized wireless access points and clients whose current configuration is vulnerable vis-à-vis newly discovered and known vulnerabilities.	9
Requirement 4.1.1: Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	This report provides a list of threat-posing wireless access points and clients communicating without security or using flawed, insecure encryption methods such as WEP.	3

Relevant PCI DSS 1.2 requirements	How this report helps	Violations Count
<ul style="list-style-type: none"> <li>- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</li> <li>- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</li> </ul>		

The use of Wireless IPS sets up the processes to satisfy the following PCI DSS 1.2 requirements. Automatic intrusion prevention and alerting should be turned on to meet requirements marked with \*.

Relevant PCI DSS 1.2 requirements	How Wireless IPS helps
Requirement 6.2: Establish a process to identify newly discovered security vulnerabilities and update configuration standards accordingly.	Generating and reviewing contents of this report periodically will help identify newly discovered vulnerabilities that can be acted upon.
Requirement 10.5.4: Write logs for external facing technologies (including wireless networks) onto the internal LAN.	The Wireless IPS server engine securely maintains logs of all wireless activity. The logs cannot be viewed or altered without proper authorization and they can be used as audit trails.
Requirement 11.1: Test for presence of wireless access points by using a wireless analyzer at least quarterly or use a wireless IDS/IPS to identify all wireless devices in use.	Wireless scanners continuously monitor all wireless devices in use and automatically update the list of wireless devices maintained by the Wireless IPS server whenever new devices are discovered.
Requirement 11.2: Run network vulnerability scans quarterly and after any significant change in the network.	Wireless scanners automatically scan the network 24x7 for wireless vulnerabilities. This report provides a list of wireless vulnerabilities discovered during the reporting period. This report can be generated on demand or at scheduled intervals.
Requirement 11.4: Use of network intrusion detection and prevention system to monitor network traffic and alert personnel of suspected compromises.*	Despite having strong wired security measures, intrusions can happen through wireless. Enabling automatic prevention using Wireless IPS will not only continuously monitor and log wireless threats, but also raise alerts and block wireless intrusion attempts.
Requirement 12.9: Implement an incident response plan. Be prepared to respond immediately to a security breach.*	Wireless scanners automatically monitor the network 24x7 and instantly detect any unauthorized wireless activity. Incident response can be done either manually or automatically by enabling automatic intrusion prevention.

---

## Recommended Actions

Wireless vulnerability assessment is an iterative process. Since wireless environments change dynamically, it is recommended that you conduct a PCI wireless compliance assessment at least once every 15 days. Archive the PCI wireless compliance assessment reports. Establish an ongoing wireless security program to fix the top vulnerabilities and improve your network's wireless security posture.

Refer to the *Categorized Violations Summary* section to learn about remedial actions corresponding to specific wireless vulnerabilities in your network. Remedial actions can be broadly classified into:

- **Manual:** These solutions require human intervention, e.g., changing device configuration, upgrading the firmware.
- **Automatic:** These solutions lessen the burden on the system administrators by providing 24x7 monitoring, intrusion detection and prevention capabilities, e.g., using software on wireless clients to manage how they behave and connect, wireless network security solutions that detect and automatically block anomalous activities or attacks.

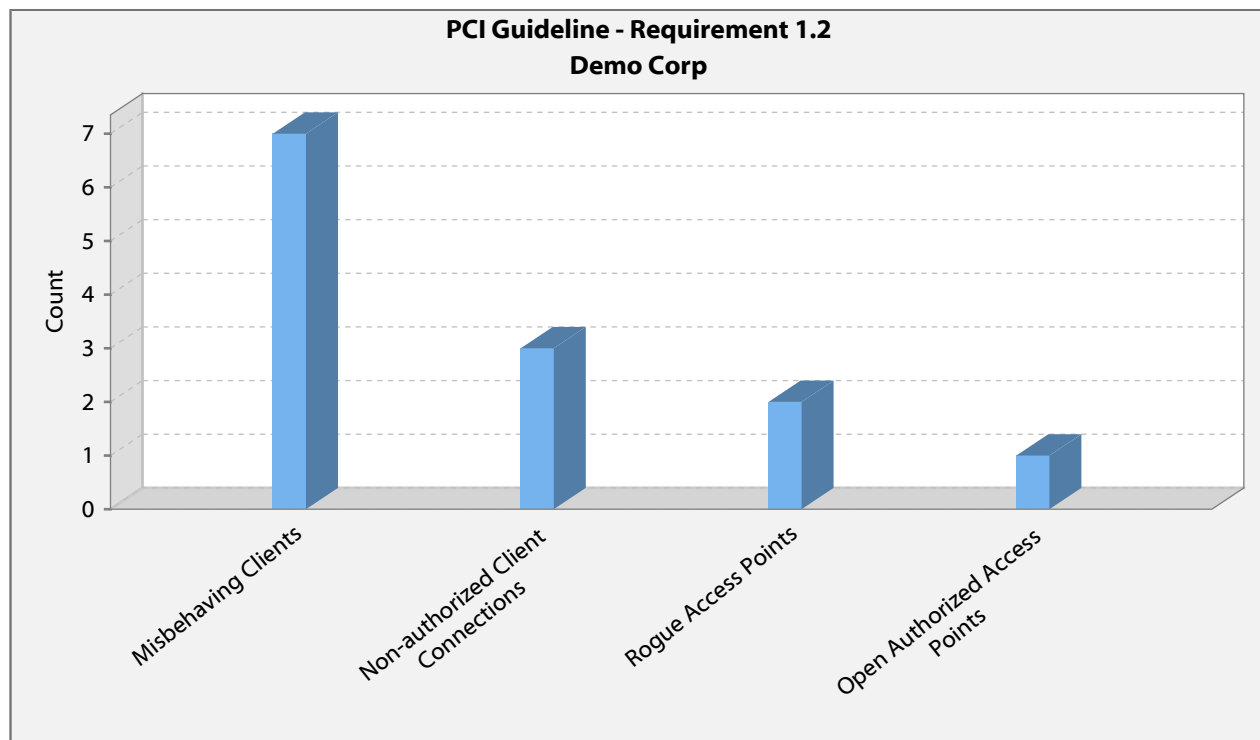


## Categorized Violations Summary

## Categorized Violations Summary

### PCI Guideline – Requirement 1.2

Relevant PCI DSS guideline	Violations Count	Violations
Build a firewall configuration that restricts connections between untrusted networks and the cardholder data environment.	13	Non-authorized Client Connections (3) Misbehaving Authorized Clients (7) Rogue Access Points (2) Open Authorized Access Points (1)



#### Non-authorized Client Connections

**Severity:** Critical

**Threat:** An unauthorized client connecting to your authorized AP indicates a potential malicious attempt to break into your corporate network by wireless access. This vulnerability may lead to unauthorized access to cardholder data in violation of requirement 1.2.

**Remediation:** Manually check if the SSID of APs on your network is not the same as the one used on your neighbors' networks. Also, configure and enforce an authentication policy between authorized APs and authorized clients.

For automatically blocking any unauthorized connections to your network, consider using a wireless security solution.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID	Security
6th Floor	Proxim_53:4D:1C	802.11b/g	anw	802.11i
1st Floor	Netgear_D5:B2:9E	802.11b/g/n	shack	Open
Demo	D-Link_E8:D2:CB	802.11b/g	ccc_net	WEP

**Misbehaving Clients****Severity:** Critical

**Threat:** Authorized clients that associate with an external or a threat posing AP (e.g., rogue AP) are likely to bypass your firewalls and content (URL, malware, spam) filter policies. Such misbehaving clients can lead to reduced productivity, liability for illegal content flowing through your network, or leak sensitive data. This vulnerability may lead to leakage of cardholder data in violation of requirement 1.2.

**Remediation:** Check the wireless settings on your authorized clients and ensure they are configured to connect only to your authorized SSID. A wireless client management software can help in enforcing your security policies and regulating how your clients connect wirelessly.

If you do not want to touch your clients, consider using a wireless security solution for automatically blocking authorized clients from connecting to external or threat-posing APs.

**Device(s) Involved:**

Location	Device Name	MAC Address	Protocol
Store@Cherry Hill	Cisco_11:41:40	00:17:DF:11:41:40	802.11b/g
6th Floor	Intel_01:E8:99	00:1C:BF:01:E8:99	802.11b/g
6th Floor	MARY L	00:12:F0:97:AB:B3	802.11b/g
6th Floor	Intel_3F:01:83	00:13:CE:3F:01:83	802.11b/g
6th Floor	Intel_92:0B:A6	00:19:D2:92:0B:A6	802.11b/g
6th Floor	MIKE FARLEY	00:1B:77:81:35:4E	802.11b/g
6th Floor	Intel_28:E5:C1	00:1B:77:28:E5:C1	802.11b/g

**Rogue APs****Severity:** High

**Threat:** Rogue APs are unauthorized APs connected to your corporate network in violation of your security policies. Outsiders can enter the corporate network using these Rogue APs as wireless backdoors. This vulnerability may lead to unauthorized access to cardholder data in violation of requirement 1.2.

**Remediation:** Use wireless security solutions for automatically blocking wireless access to Rogue APs. Locate the Rogue AP and physically disconnect it from your corporate network.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID	Security
Store@Cherry Hill	Netgear_7E:F8:5B	802.11b/g		WPA
6th Floor	Cisco-Linksys_F4:80:E8	802.11b/g/n	Alice	WEP

### Open Authorized APs

**Severity:** High

**Threat:** Installing authorized APs without any security is a severe violation of WLAN best practices. An open AP is a backdoor through which malicious users can enter the network to which it is connected, eavesdrop on over-the-air data, or conduct illegal activities which may entail liability to the owner of the network. Open APs not only compromise the security of your entire network, but open your network to even inadvertent, unauthorized usage. This vulnerability may lead to unauthorized access to cardholder data in violation of requirements 1.2. Detected device configuration is also not compliant with requirements 2.1.1 and 4.1.1.

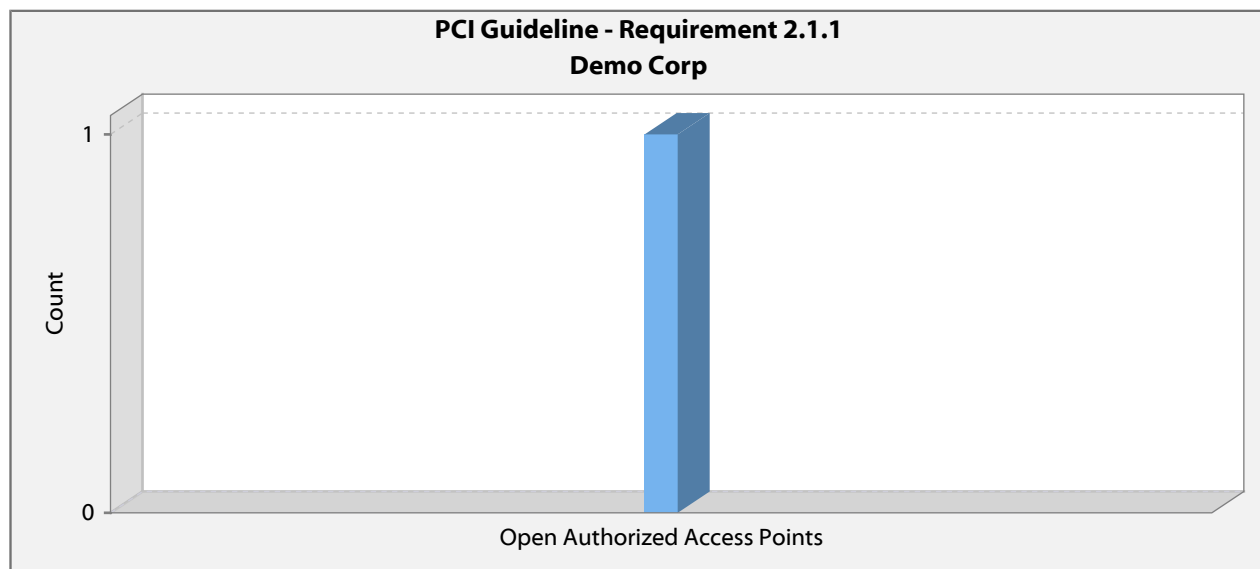
**Remediation:** Disconnect your open APs from the network and check if any unauthorized devices established connection with your open APs during the assessment. Redeploy your APs with strong encryption like WPA2 to protect your WiFi traffic against eavesdropping and prevent outsiders from entering your network.

### Device(s) Involved:

Location	Device Name	Protocol	SSID
1st Floor	Netgear_D5:B2:9E	802.11b/g/n	shack

## PCI Guideline – Requirement 2.1.1

Relevant PCI DSS guideline	Violations Count	Violations
For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	1	Open Authorized Access Points (1)



### Open Authorized APs

**Severity:** High

**Threat:** Installing authorized APs without any security is a severe violation of WLAN best practices. An open AP is a backdoor through which malicious users can enter the network to which it is connected, eavesdrop on over-the-air data, or conduct illegal activities which may entail liability to the owner of the network. Open APs not only compromise the security of your entire network, but open your network to even inadvertent, unauthorized usage. This vulnerability may lead to unauthorized access to cardholder data in violation of requirements 1.2. Detected device configuration is also not compliant with requirements 2.1.1 and 4.1.1.

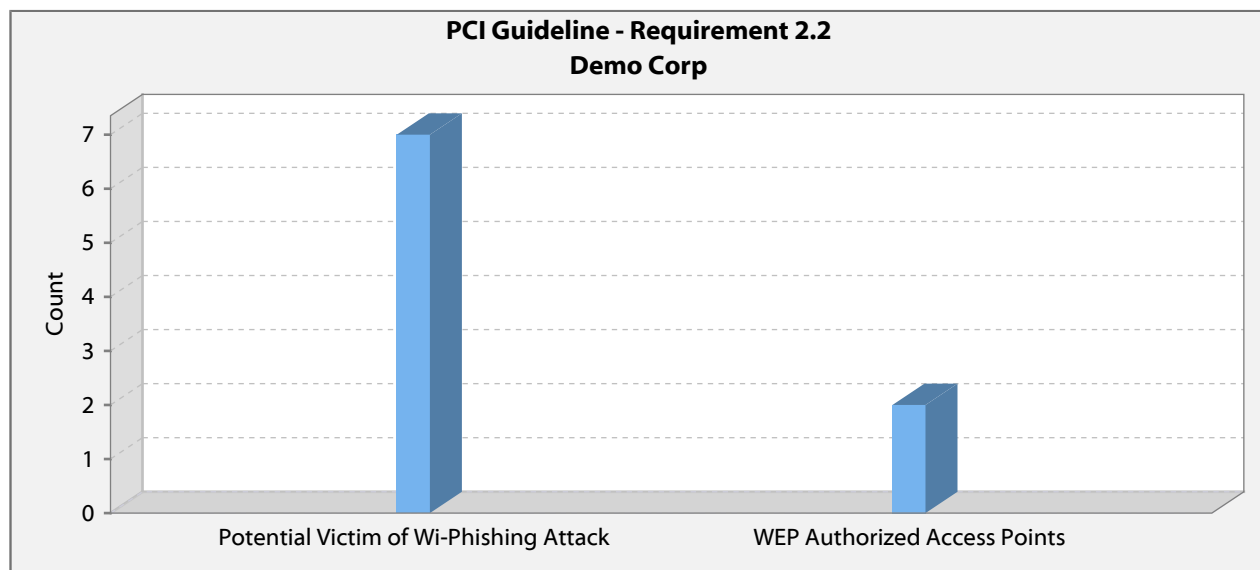
**Remediation:** Disconnect your open APs from the network and check if any unauthorized devices established connection with your open APs during the assessment. Redeploy your APs with strong encryption like WPA2 to protect your WiFi traffic against eavesdropping and prevent outsiders from entering your network.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID
1st Floor	Netgear_D5:B2:9E	802.11b/g/n	shack

**PCI Guideline – Requirement 2.2**

Relevant PCI DSS guideline	Violations Count	Violations
Develop configuration standards for all system components (including any wireless access points & clients). It also requires the institution to assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening procedures.	9	Phishing Attack(7) WEP Authorized Access Points(2)



**Potential Victim of Wi-Phishing Attack**

**Severity:** Medium

**Threat:** In Wi-Phishing, hackers use common or factory-default SSIDs to lure clients to unwittingly connect to their AP instead of the authorized WLAN. Clients probing for these common SSIDs are prime candidates for a Wi-Phishing attack. Detected device configuration is not compliant with requirement 2.2.

**Remediation:** Locate the client and remove entries of vulnerable SSIDs from the client’s preferred networks list, so it does not probe for those networks. A wireless client management software can help in enforcing your security policies and regulating how your clients behave and connect wirelessly.

**Device(s) Involved:**

Location	Device Name	MAC Address
6th Floor	MARY L	00:12:F0:97:AB:B3
6th Floor	DELLA L	00:19:D2:92:0A:D3
6th Floor	Intel_3F:01:83	00:13:CE:3F:01:83
6th Floor	Intel_92:09:E6	00:19:D2:92:09:E6
6th Floor	Intel_92:0B:A6	00:19:D2:92:0B:A6
6th Floor	Intel_62:30:43	00:1C:BF:62:30:43
6th Floor	Intel_28:E5:C1	00:1B:77:28:E5:C1

**WEP Authorized APs****Severity:** Medium

**Threat:** It is well known that the Wired Equivalent Privacy (WEP) encryption is broken and can be easily exploited to steal sensitive data and possibly to enter your network. Detected device configuration is not compliant with requirements 2.2 and 4.1.1.

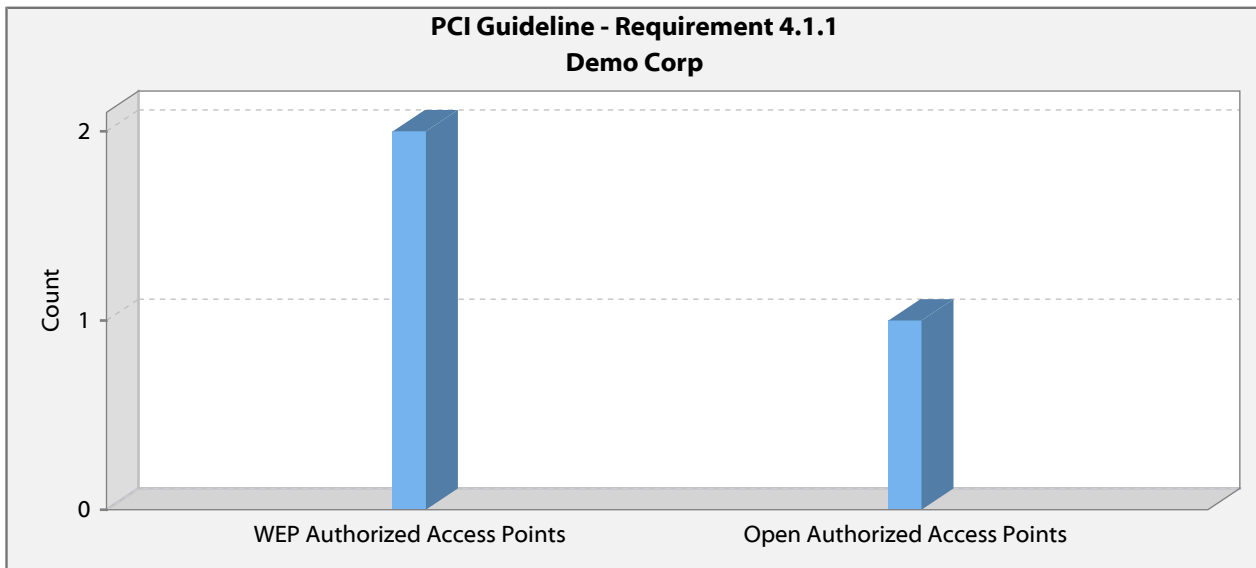
**Remediation:** Upgrade the encryption capabilities of all your WiFi APs and clients to use strong encryption like WPA2 and protect your WiFi traffic from eavesdropping. At least upgrade the devices using WEP to filter out weak IVs.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID
6th Floor	Buffalo_2B:0C:1B	802.11b/g	spectra
Demo	D-Link_E8:D2:CB	802.11b/g	ccc_net

**PCI Guideline – Requirement 4.1.1**

Relevant PCI DSS guideline	Violations Count	Violations
<p>Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.</p> <ul style="list-style-type: none"> <li>- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</li> <li>- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</li> </ul>	3	<p>Open Authorized Access Points (1) WEP Authorized Access Points(2)</p>



### Open Authorized APs

**Severity:** High

**Threat:** Installing authorized APs without any security is a severe violation of WLAN best practices. An open AP is a backdoor through which malicious users can enter the network to which it is connected, eavesdrop on over-the-air data, or conduct illegal activities which may entail liability to the owner of the network. Open APs not only compromise the security of your entire network, but open your network to even inadvertent, unauthorized usage. This vulnerability may lead to unauthorized access to cardholder data in violation of requirements 1.2. Detected device configuration is also not compliant with requirements 2.1.1 and 4.1.1.

**Remediation:** Disconnect your open APs from the network and check if any unauthorized devices established connection with your open APs during the assessment. Redeploy your APs with strong encryption like WPA2 to protect your WiFi traffic against eavesdropping and prevent outsiders from entering your network.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID
1st Floor	Netgear_D5:B2:9E	802.11b/g/n	shack

### WEP Authorized APs

**Severity:** Medium

**Threat:** It is well known that the Wired Equivalent Privacy (WEP) encryption is broken and can be easily exploited to steal sensitive data and possibly to enter your network. Detected device configuration is not compliant with requirements 2.2 and 4.1.1.

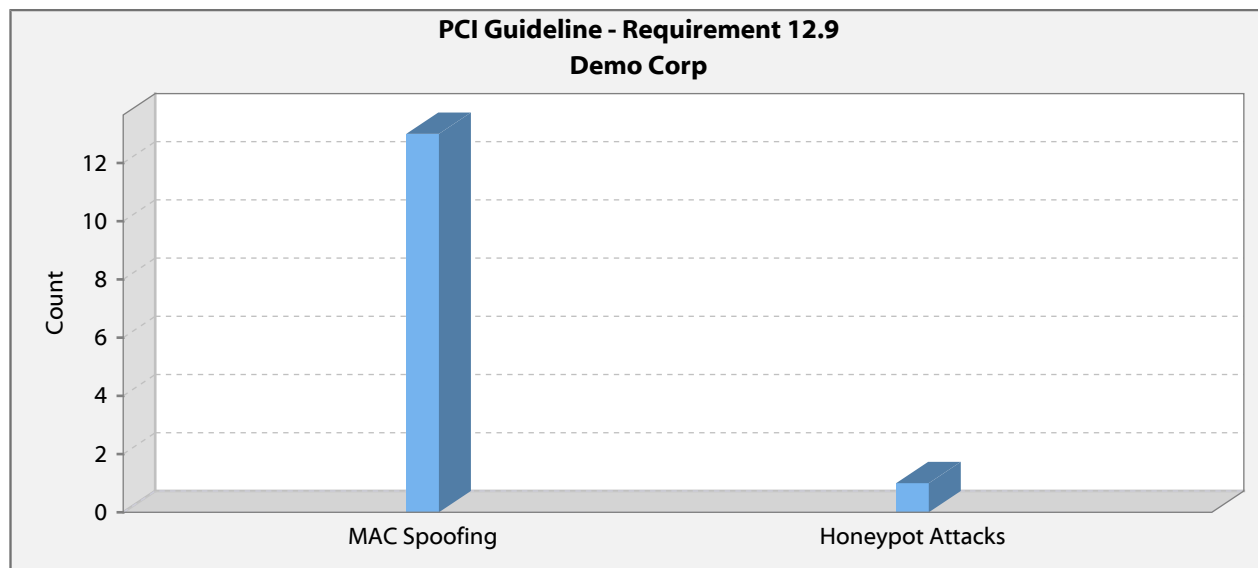
**Remediation:** Upgrade the encryption capabilities of all your WiFi APs and clients to use strong encryption like WPA2 and protect your WiFi traffic from eavesdropping. At least upgrade the devices using WEP to filter out weak IVs.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID
6th Floor	Buffalo_2B:0C:1B	802.11b/g	spectra
Demo	D-Link_E8:D2:CB	802.11b/g	ccc_net

**PCI Guideline – Requirement 12.9**

Relevant PCI DSS guideline	Incidents count	Incidents detected
Implement an incident response plan. Be prepared to respond immediately to a security breach.	14	Honeypot Attacks (1) Mac Spoofing (13)



**Honeypot Attacks**

**Severity:** Critical

**Threat:** External APs with authorized SSIDs are called Honeypots or Evil Twins. Honeypots can lure authorized clients into an inadvertent association, which is a major security threat. Your clients may unwittingly provide confidential information (e.g., password); the honeypot can launch a man-in-the-middle attack and insert itself into authorized communication or it can scan the client for vulnerabilities. A response mechanism to address this vulnerability is required as per requirement 12.9.

**Remediation:** Try to locate the honeypot using a wireless location tracking solution and physically remove it. Consider using a wireless security solution for automatically blocking your authorized clients from connecting to the honeypot.

**Device(s) Involved:**

Location	Device Name	Protocol	SSID	Security
6th Floor	06:40:96:B4:C0:46	802.11b/g/n	Test-Peap-Defcon17	WPA

**MAC Spoofing**

**Severity:** Critical

**Threat:** Detection of MAC spoofing indicates that a hacker has knowledge about the MAC addresses of your authorized devices and is using it maliciously. Your network security is potentially breached or prone to a denial-of-service attack. A response mechanism to address this vulnerability is required as per requirement 12.9.

**Remediation:** Use wireless security solutions for automatically blocking malicious devices that can use spoofed MAC addresses to enter your network or launch other attacks.

**Related Event(s):**

Event Location	Start Date And Time	Event Details
6th Floor	Aug 23, 2009 8:17:25 PM	Spoofing of MAC address [00:0D:0B:2B:0C:1B] of Authorized AP [Buffalo_2B:0C:1B] is in progress.
6th Floor	Aug 6, 2009 9:43:54 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 6, 2009 8:32:05 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 5, 2009 2:29:51 PM	Client RF signature anomaly detected for Client [DELLA L]
6th Floor	Aug 5, 2009 4:29:36 PM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 5, 2009 9:36:28 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 5, 2009 8:17:07 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 4, 2009 5:32:43 PM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 4, 2009 1:36:51 PM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 4, 2009 2:36:31 PM	Client RF signature anomaly detected for Client [DELLA L]
6th Floor	Aug 4, 2009 10:34:36 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]
6th Floor	Aug 4, 2009 10:24:57 AM	Client RF signature anomaly detected for Client [DELLA L]

Event Location	Start Date And Time	Event Details
6th Floor	Aug 4, 2009 7:51:56 AM	Client RF signature anomaly detected for Client [Intel_92:0B:A6]

## About This Report

Payment Card Industry Data Security Standard (PCI DSS) Version 1.2 published in October 2008 defines recommended security controls for protecting cardholder data. PCI DSS was defined by a consortium of credit card companies, including VISA and MasterCard. The requirements of the PCI Standard apply to all members, merchants and service providers that store, process or transmit cardholder data.





The following sections from PCI DSS, Version 1.2 are relevant from the perspective of protecting cardholder data from unauthorized wireless access. This report is intended to be simply an aide to review PCI DSS 1.2 compliance of WLAN deployments. It is not meant to automatically fulfill PCI DSS 1.2 requirements related to your WLAN network. Consult a PCI Qualified Security Auditor (QSA) for obtaining compliance certification.


Relevant PCI DSS Guidelines	How this report helps?
<u>Requirement 1.2</u> : Build a firewall configuration that restricts connections between untrusted networks and the cardholder data environment.	This report provides a list of untrusted wireless devices that may open backdoors to cardholder data environment. These devices may allow unauthorized access to cardholder data bypassing wired firewalls.
<u>Requirement 2.1.1</u> : For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	This report identifies authorized wireless access points using vendor default SSIDs or security configuration.
<u>Requirement 2.2</u> : Develop configuration standards for all system components (including any wireless access points & clients). It also requires the institution to assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening procedures.	This report authorized wireless access points and clients whose current configuration is vulnerable vis-à-vis newly discovered and known vulnerabilities.
<u>Requirement 4.1.1</u> Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. <ul style="list-style-type: none"> <li>- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</li> <li>- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</li> </ul>	This report provides a list of threat-posing wireless access points and clients communicating without security or using flawed, insecure encryption methods such as WEP.

The use of Wireless IPS sets up the processes to satisfy the following PCI DSS 1.2 requirements. Automatic intrusion prevention and alerting should be turned on to meet requirements marked with \*.

Relevant PCI DSS Guidelines	How Wireless IPS helps
<u>Requirement 6.2:</u> Establish a process to identify newly discovered security vulnerabilities and update configuration standards accordingly.	Generating and reviewing contents of this report periodically will help identify newly discovered vulnerabilities that can be acted upon.
<u>Requirement 10.5.4:</u> Write logs for external facing technologies (including wireless networks) onto the internal LAN.	The Wireless IPS server engine securely maintains logs of all wireless activity. The logs cannot be viewed or altered without proper authorization and they can be used as audit trails.
<u>Requirement 11.1:</u> Test for presence of wireless access points by using a wireless analyzer at least quarterly or use a wireless IDS/IPS to identify all wireless devices in use.	Wireless scanners continuously monitor all wireless devices in use and automatically update the list of wireless devices maintained by the Wireless IPS server whenever new devices are discovered.
<u>Requirement 11.2:</u> Run network vulnerability scans quarterly and after any significant change in the network.	Wireless scanners automatically scan the network 24x7 for wireless vulnerabilities. This report provides a list of wireless vulnerabilities discovered during the reporting period. This report can be generated on demand or at scheduled intervals.
<u>Requirement 11.4:</u> Use of network intrusion detection and prevention system to monitor network traffic and alert personnel of suspected compromises.*	Despite having strong wired security measures, intrusions can happen through wireless. Enabling automatic prevention using Wireless IPS will not only continuously monitor and log wireless threats, but also raise alerts and block wireless intrusion attempts.
<u>Requirement 12.9:</u> Implement an incident response plan. Be prepared to respond immediately to a security breach.*	Wireless scanners automatically monitor the network 24x7 and instantly detect any unauthorized wireless activity. Incident response can be done either manually or automatically by enabling automatic intrusion prevention.

The report contains: (1) *Result Summary*, (2) *Categorized Violations Summary* for all vulnerabilities that were detected, and (3) *Recommended Actions* that you need to take for remediation and for improving your network's security posture. The results are based on your airspace scanned using AirTight Networks' pre-configured wireless scanners. The table below classifies vulnerabilities based on their severity and urgency of response.

Severity level	Type	Description
 5	Critical	<b>Security breach or wireless malpractice detected!</b> An intruder may have entered your network; sensitive data is exposed; or your users are bypassing your security policy control (e.g., firewalls, and URL, spam, and malware filters).
 4	High	Known vulnerabilities those ignore basic security measures and naturally expose your network and data assets even to inadvertent unauthorized access.
 3	Medium	Vulnerabilities that violate best practices and can lead to unauthorized usage of your network resources or hackers with medium expertise and knowledge of published exploits can exploit these vulnerabilities in minutes.
 2	Low	Hackers can collect information about your network and may use it to discover other vulnerabilities; high expertise needed to exploit these vulnerabilities.

Severity level	Type	Description
 1	Probable	Potential vulnerabilities that may pose a threat.

**Critical severity:** Occurrence of a critical severity demands your urgent attention. It is raised when malpractices in wireless usage, anomalous activities or attacks are detected in your airspace and your entire network's security is potentially at risk. Few examples of instances with critical severity: authorized users connecting to external or rogue APs, outsiders connecting to your authorized APs, authorized users participating in ad hoc networks, network and data exposed by open or WEP connections, MAC spoofing, honeypot attack, denial of service (DoS) attack.

**High severity:** Ignoring basics of wireless security leads to these vulnerabilities that give outsiders easy access to your network and data assets and a security breach is imminent; deliberate effort to hack into your network is not necessary. Few examples of high severity vulnerabilities are: using "out-of-box" settings (e.g., no security, default password) on your WiFi devices, rogue APs installed on your network, your authorized devices are in ad hoc mode.

**Medium severity:** Violating WLAN best practices usually results in these vulnerabilities. Few examples are: using the broken Wired Equivalent Privacy (WEP) encryption standard on your WiFi devices, and lack of policies to control how and to which WLANs your WiFi clients can connect. Hackers can break through your weak security settings, or lure users to connect to them (e.g., honeypots) gaining access to sensitive data or backdoor entry into your network.

**Low severity:** These vulnerabilities leak information about your WLAN configuration and attract unwarranted attention from outsiders to your network, or attract your authorized users to connect to external WLANs, e.g., APs using vulnerable SSIDs. Hackers can use such information to discover and exploit other vulnerabilities in your network.

**Probable:** These are potential vulnerabilities that may pose limited threat to security or performance of your network. You should manually verify the existence and credibility of these probable threats. For instance: an extraordinary number of wireless frame errors indicate a potential jamming attack or inadvertent interference from another RF source; a large number of broadcast messages indicate a potential attack or misconfiguration.