



PCI DSS 2.0 Wireless Compliance Report

For: AirTight Networks

From: Dec 6, 2010 3:17:07 AM

To: Jan 5, 2011 3:17:07 AM

At: Demo Corp

A Report by AirTight Networks, Inc.

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

www.airtightnetworks.com



Table of Contents

REPORT SUMMARY	3
RECOMMENDED ACTIONS	5
CATEGORIZED VIOLATIONS SUMMARY	7
PCI GUIDELINE - REQUIREMENT 1.2	7
<i>Unauthorized Client Connections</i>	8
<i>Mis-associating Authorized Clients</i>	10
<i>Adhoc Mode</i>	12
<i>Rogue Access Points</i>	14
<i>Open Authorized Access Points</i>	16
<i>Soft or Windows 7 Virtual WiFi APs</i>	18
PCI GUIDELINE - REQUIREMENT 2.1.1	20
<i>Open Authorized Access Points</i>	21
<i>Authorized AP using Vulnerable SSID</i>	23
PCI GUIDELINE - REQUIREMENT 2.2	25
<i>Potential Victim of Wi-Phishing Attack</i>	26
<i>WEP Authorized Access Points</i>	28
<i>Misconfigured Authorized AP</i>	30
PCI GUIDELINE - REQUIREMENT 4.1.1	32
<i>Open Authorized Access Points</i>	33
<i>WEP Authorized Access Points</i>	35
PCI GUIDELINE - REQUIREMENT 12.9	37
<i>Honey-pot Attack</i>	38
ABOUT THIS REPORT	40

Report Summary

Report Generated On: Jan 5 2011, 03:17:07 AM (GMT -0800)

Scan Duration:

From: Dec 6, 2010 3:17:07 AM

To: Jan 5, 2011 3:17:07 AM

Wireless Scanners - Total: 27

Approximate area scanned for wireless vulnerabilities: 540000 sq. ft

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

Wireless Devices Detected - Total: Access Points - 1030 Clients - 8558

Relevant PCI DSS 2.0 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.	35
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.	7
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.	18
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.	10

Relevant PCI DSS 2.0 requirements	How this report helps	Violations Count
<ul style="list-style-type: none"> - For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. - For current wireless implementations, it is prohibited to use WEP after June 30, 2010. 		

The use of Wireless IPS sets up the processes to satisfy the following PCI DSS 2.0 requirements. Automatic intrusion prevention and alerting should be turned on to meet requirements marked with *.

Relevant PCI DSS 2.0 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.

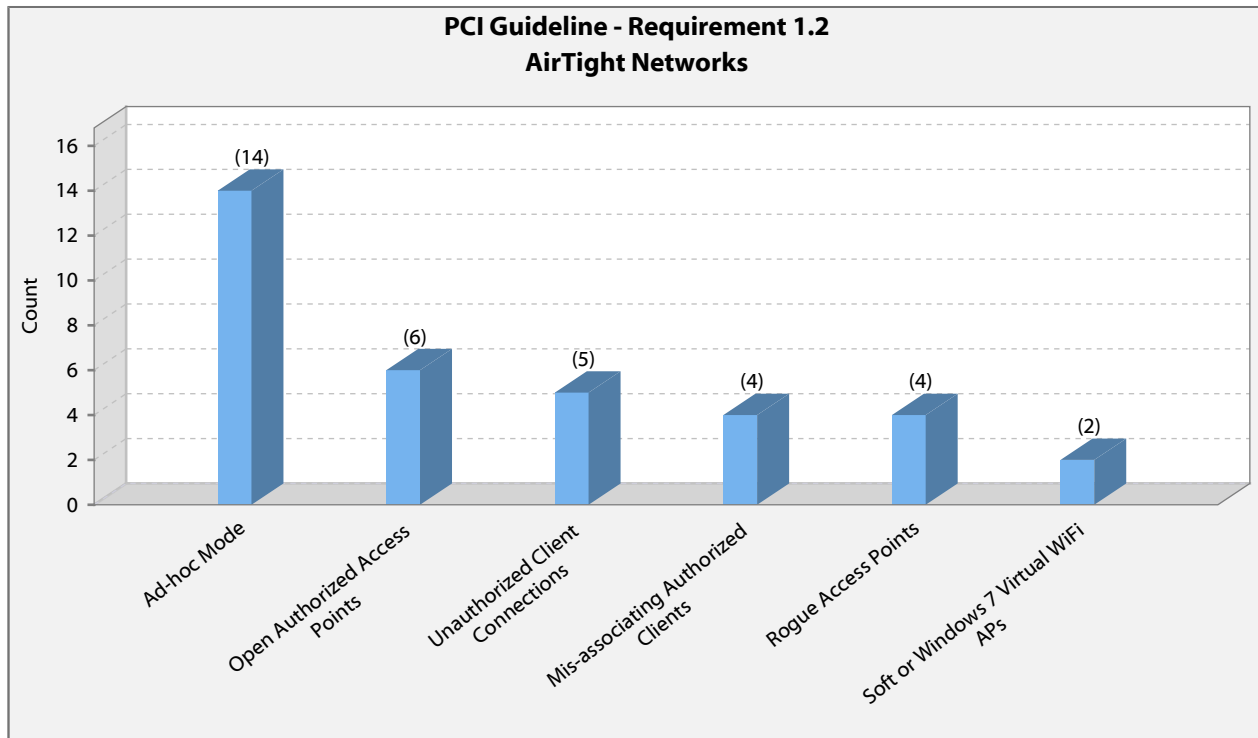


Categorized Violations Summary

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.	35	Unauthorized Client Connections (5) Mis-associating Authorized Clients (4) Adhoc Mode (14) Rogue Access Points (4) Open Authorized Access Points (6) Soft or Windows 7 Virtual WiFi APs(2)



Unauthorized 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
Data Center	D-Link_E8:D2:CB	802.11b/g	ccc_net	WEP
Floor 1	Buffalo_2B:0C:1B	802.11b/g	airtightguest	WPA
DataCenter	D-Link_EA:42:19	802.11b/g/n	Rsignia	802.11i, WPA
Pittsburgh	HP-Procurve_B3:22:90	802.11b/g	Guardia Forest Treasure	802.11i
Foster City (Bay Area)	Home-D-Link_05:0C:70	802.11b/g/n	Yahoo..!!	802.11i

Mis-associating Authorized 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
Demo Corp	Intel_28:E5:C1	00:1B:77:28:E5:C1	802.11b/g
Pittsburgh	Liteon_05:76:56	00:22:5F:05:76:56	802.11b/g
Fort Lauderdale Office	Gemtek_09:BB:49	00:26:82:09:BB:49	802.11b/g
Fort Lauderdale Office	HP0026555FDFF2	00:26:55:5F:DF:F2	802.11b/g

Ad-hoc Mode

Severity: High

Threat: Authorized clients in ad hoc connection mode are likely infected with viral SSIDs and can inadvertently compromise your entire network's security by accepting direct connections. Unauthorized clients can enter your network through such connections, while authorized clients can bypass your security policy control (e.g., firewalls, and URL, spam, and malware filters). This vulnerability may lead to unauthorized access to cardholder data in violation of requirement 1.2.

Remediation: You should locate the clients and before redeploying them, manually change the configuration of your clients to prevent them from operating in ad-hoc mode.

Consider using a wireless client management software for enforcing your security policies and ensuring that clients only connect in the infrastructure mode to authorized APs.

Device(s) Involved:

Location	Device Name	MAC Address	SSID
Show Floor	Intel_81:DB:8F	00:1F:3B:81:DB:8F	Free Public WiFi
Show Floor	Apple_0D:D7:71	F8:1E:DF:0D:D7:71	Free Public WiFi
Show Floor	Apple_B7:B0:7A	D8:30:62:B7:B0:7A	Free Public WiFi
Show Floor	Apple_C8:C9:7A	7C:6D:62:C8:C9:7A	Free Public WiFi
Show Floor	Apple_D6:DE:60	7C:6D:62:D6:DE:60	Free Public WiFi
Show Floor	Apple_6A:05:09	90:84:0D:6A:05:09	Free Public WiFi
Show Floor	Apple_C8:21:DC	00:26:B0:C8:21:DC	Free Public WiFi
Show Floor	Apple_1A:87:B4	7C:6D:62:1A:87:B4	Free Public WiFi
Show Floor	Apple_DB:BD:26	34:15:9E:DB:BD:26	hpsetup
Show Floor	Apple_3A:6A:09	F8:1E:DF:3A:6A:09	Free Public WiFi
Show Floor	Apple_5B:CD:6D	90:84:0D:5B:CD:6D	Wireless Network
Show Floor	Apple_C9:86:8A	00:26:B0:C9:86:8A	Free Public WiFi
Show Floor	Apple_DC:48:BA	00:23:6C:DC:48:BA	Free Public WiFi
Gaylord National Exhibit	Hon-Hai_1D:DC:AE	00:16:CF:1D:DC:AE	FreeWiFi

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 a wireless intrusion prevention system (WIPS) 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
Boston	3Com_8D:B8:00	802.11b/g	BlackPearl2	802.11i
DataCenter	Ruckus_0A:D9:F9	802.11b/g	lodgenet	Open
Pittsburgh	HTC_06:4D:D9	802.11b/g	HTC network	802.11i
Fort Lauderdale Office	Belkin_1D:C6:B3	802.11b/g	CorporateAP	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
Regional Office	Cisco-Linksys_E8:24:2C	802.11a	linksys-a
Show Floor	Guest AP	802.11b/g	public_access
Marietta	Linksys_B3:D4:D5	802.11b only	d433
Fort Lauderdale Office	Cisco-Linksys_99:01:A1	802.11b/g	linksys-g
Fort Lauderdale Office	Cisco-Linksys_99:01:A0	802.11a	linksys-a
Gaylord National Exhibit	Buffalo_63:92:32	802.11a	buff-5

Soft or Windows 7 Virtual WiFi APs

Severity: High

Threat: A Soft AP is a WiFi client device such as a laptop operating as an access point. A Soft AP connected to your enterprise network, for instance, through Ethernet or WiFi (using Windows 7 Virtual WiFi) can share its enterprise network access with other unauthorized devices. Using a Soft AP as backdoor, outsiders can bypass your wired security measures and gain access to private enterprise network and sensitive data. This vulnerability can lead to unauthorized access to cardholder data environment in violation of requirement 1.2.

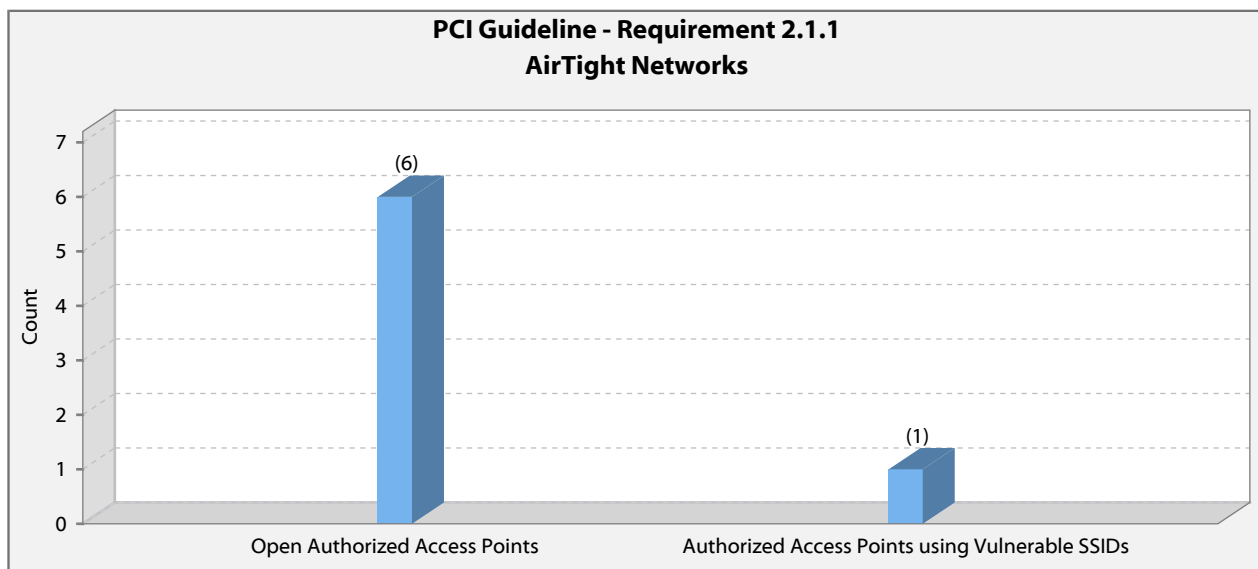
Remediation: Use a wireless intrusion prevention system (WIPS) to automatically block unauthorized access to the Soft AP. If the Soft AP is an authorized client, you may want to allow it to connect to the enterprise network, but block it from sharing the enterprise network access with other devices. You can also use a WIPS to track the physical location of the client device operating as a Soft AP.

Device(s) Involved:

Location	Device Name	MAC Address
Pittsburgh	HTC_06:4D:D9	38:E7:D8:06:4D:D9
Pittsburgh	Schala	00:02:6F:44:90:D6

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.	7	Open Authorized Access Points (6) Authorized Access Points using Vulnerable SSIDs(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
Regional Office	Cisco-Linksys_E8:24:2C	802.11a	linksys-a
Show Floor	Guest AP	802.11b/g	public_access
Marietta	Linksys_B3:D4:D5	802.11b only	d433
Fort Lauderdale Office	Cisco-Linksys_99:01:A1	802.11b/g	linksys-g
Fort Lauderdale Office	Cisco-Linksys_99:01:A0	802.11a	linksys-a
Gaylord National Exhibit	Buffalo_63:92:32	802.11a	buff-5

Authorized APs using Vulnerable SSIDs

Severity: Low

Threat: An authorized AP with a commonly used (e.g., factory-default) SSID is more likely to attract attention from hackers or inadvertently from outsiders with their devices usually probing for these SSIDs. Detected device configuration is not compliant with requirement 2.1.1.

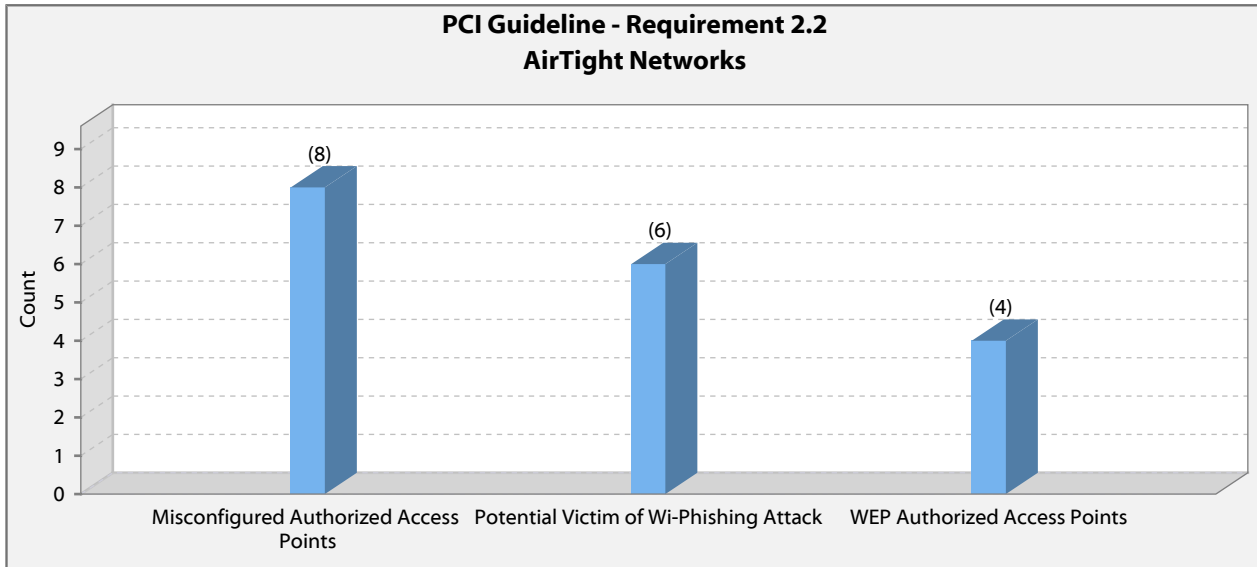
Remediation: Manually change the SSID setting on your AP to a custom SSID that is not commonly used. Then make sure your clients are also properly configured with the custom SSID.

Device(s) Involved:

Location	Device Name	Protocol	SSID	Security
Fort Lauderdale Office	Cisco-Linksys_99:01:A1	802.11b/g	linksys-g	Open

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.	18	Phishing Attack(6) WEP Authorized Access Points(4) Misconfigured Authorized Access Points(8)



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
Demo Corp	Intel_28:E5:C1	00:1B:77:28:E5:C1
Pittsburgh	Liteon_05:76:56	00:22:5F:05:76:56
Foster City (Bay Area)	Apple_8D:8D:92	00:21:E9:8D:8D:92
Conklin Office	7C:C5:37:62:0A:68	7C:C5:37:62:0A:68
Conklin Office	SEIBOII	00:16:6F:6D:5B:6E
Conklin Office	F0:B4:79:64:B3:FC	F0:B4:79:64:B3:FC

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
Data Center	D-Link_E8:D2:CB	802.11b/g	ccc_net
Floor 1	Proxim_53:4D:1B	802.11b/g	7Q3I6
Marietta	Hewlett-Packard_F6:A5: 83	802.11b/g	desosnso
Floor 1	Cisco_C7:3D:A0	802.11b/g	WOS

Misconfigured Authorized APs

Severity: Low

Threat: Settings on an Authorized AP violate your configuration policies. Policy noncompliant devices may be vulnerable. Detected device configuration is not compliant with requirement 2.2.

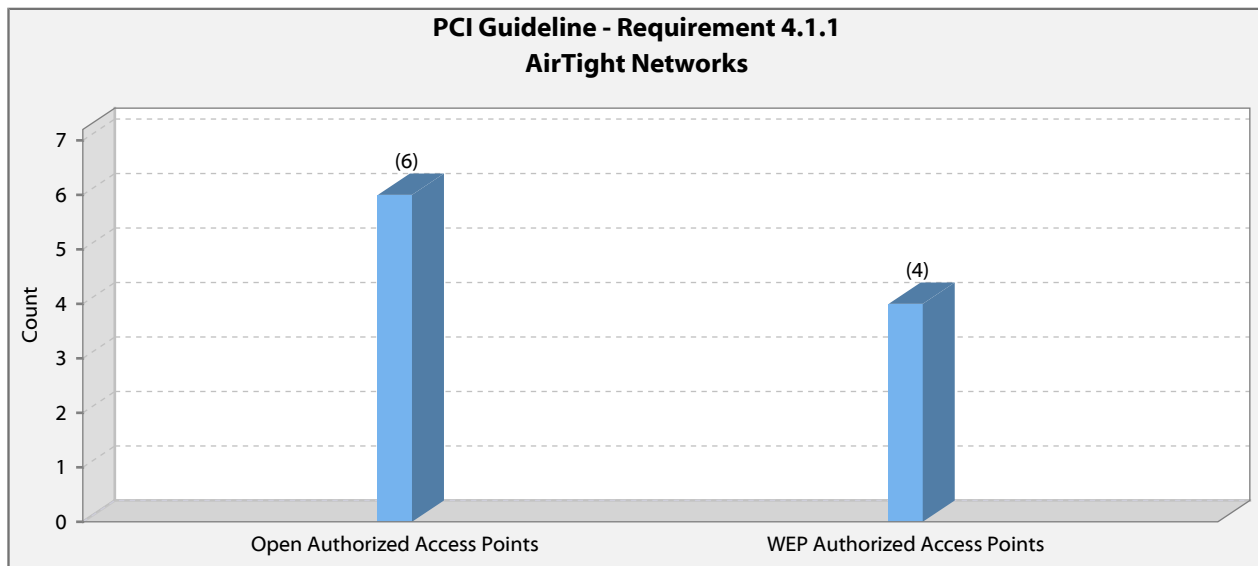
Remediation: Manually fix the configuration on this authorized AP to ensure that it is compliant with your configuration policies.

Device(s) Involved:

Location	Device Name	Protocol	SSID	Security
San Jose	D-Link_B5:62:89	802.11b/g	CorporateWiFi	802.11i
Regional Office	Cisco-Linksys_E8:24:2D	802.11b/g	yale	WPA
Floor 1	Buffalo_2B:0C:1B	802.11b/g	airtightguest	WPA
Floor 1	Proxim_53:4D:1B	802.11a	Guardia Forest Treasure	802.11i
Marietta	Cisco-Linksys_56:84:2E	802.11b/g	joel_307	802.11i
DataCenter	D-Link_EA:42:19	802.11b/g/n	Rsignia	802.11i, WPA
Floor 1	Belkin_AA:6A:A1	802.11b/g/n	ID10T	802.11i
Floor 1	Cisco-Linksys_3B:A5:23	802.11b/g	TrynHackme	802.11i

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"> - For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. - For current wireless implementations, it is prohibited to use WEP after June 30, 2010. 	10	<p>Open Authorized Access Points (6) WEP Authorized Access Points(4)</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
Regional Office	Cisco-Linksys_E8:24:2C	802.11a	linksys-a
Show Floor	Guest AP	802.11b/g	public_access
Marietta	Linksys_B3:D4:D5	802.11b only	d433
Fort Lauderdale Office	Cisco-Linksys_99:01:A1	802.11b/g	linksys-g
Fort Lauderdale Office	Cisco-Linksys_99:01:A0	802.11a	linksys-a
Gaylord National Exhibit	Buffalo_63:92:32	802.11a	buff-5

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.

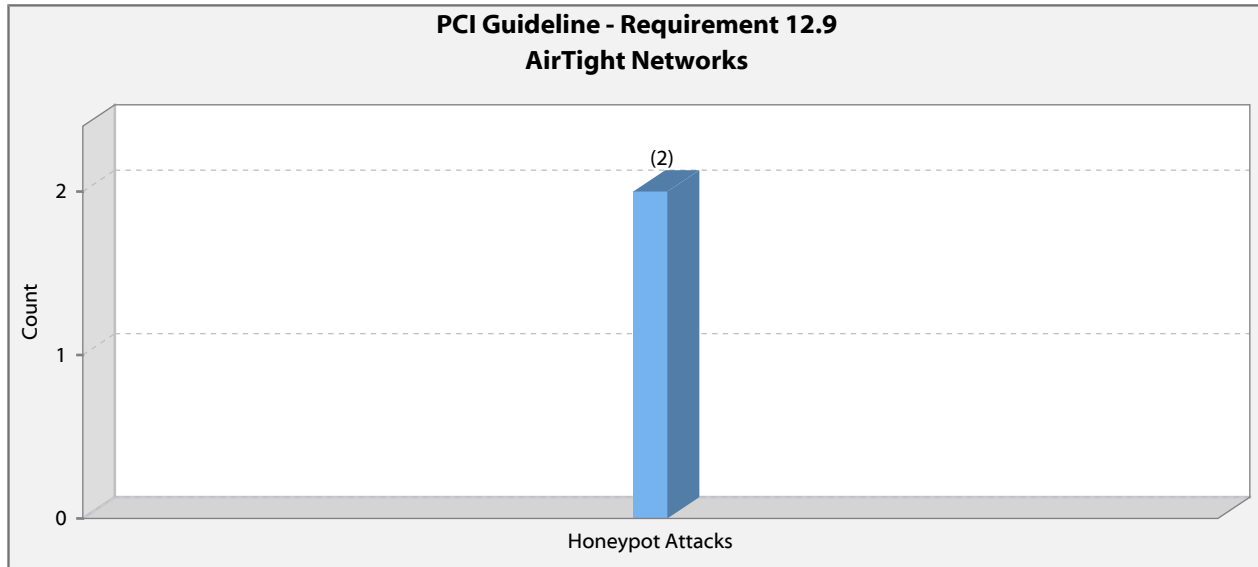
Remediation: Upgrade the encryption capabilities of all your WiFi APs and clients to use strong encryption like WPA2 and protect your WiFi traffic from eavesdropping. At least upgrade the devices using WEP to filter out weak IVs.

Device(s) Involved:

Location	Device Name	Protocol	SSID
Data Center	D-Link_E8:D2:CB	802.11b/g	ccc_net
Floor 1	Proxim_53:4D:1B	802.11b/g	7Q3I6
Marietta	Hewlett-Packard_F6:A5: 83	802.11b/g	desosnso
Floor 1	Cisco_C7:3D:A0	802.11b/g	WOS

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.	2	Honeypot Attacks (2)



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
Boston	66:2A:2F:53:7C:99	802.11b/g	2WIRE889	--
Pittsburgh	Xerox_00:00:90	802.11b/g	Guardia Forest Treasure	--

About This Report

Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 published in October 2010 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 2.0 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 2.0 compliance of WLAN deployments. It is not meant to automatically fulfill PCI DSS 2.0 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"> - For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. - For current wireless implementations, it is prohibited to use WEP after June 30, 2010. 	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 2.0 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) *Report 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	Security breach or wireless malpractice detected! 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.