

Payment Card Industry Data Security Standard (PCI DSS) Compliance Report

Designated Official: _____

Time Period: Wednesday, July 29, 2009 9:23:53 AM

What is PCI Data Security Standard?

The PCI Data Security Standard, or PCI DSS, is a set of comprehensive requirements for enhancing payment account data security. It was originally developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate broad cooperation in security measures for payment cards on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Participating businesses must comply with 12 “best practice” requirements for wired and wireless networks and validate their compliance periodically.

Who and what is affected by PCI Data Security Standard?

The PCI DSS applies to all businesses that store, process, or transmit cardholder data over networks, including wireless networks. In addition, the standards apply to all **system components** that include all **network components, servers, and applications** included within or connected to a cardholder data environment.

What network components are affected by PCI Data Security Standard?

Network components affected by PCI Data Security Standard include, but are not limited to, wireless access points, firewalls, switches, and routers as well as network and security appliances.

What servers are affected by PCI Data Security Standard?

Servers affected by the PCI DSS include Web, database, authentication, DNS, e-mail, proxy, and NTP (Network Time Protocol) servers.

What applications are impacted by PCI Data Security Standard?

All purchased and custom applications, including internal and external Web applications, that interface cardholder data or that are connected to the same network as cardholder data.

AirMagnet PCI Data Security Standard Compliance Reports

The PCI DSS contain several architectural directives designed to secure cardholder data on wired and wireless networks. Each directive requires affected merchants and service providers to implement security “best practices” to comply with the standard. Toward that end, AirMagnet WiFi Analyzer satisfies the PCI DSS requirements affecting WLANs and ensures that wireless devices interfacing or connecting to systems containing cardholder data are secure.

AirMagnet technology automates performance and security monitoring of devices in WLANs to report deficiencies and vulnerabilities and comply with PCI DSS requirements. AirMagnet Compliance Reports map PCI DSS requirements to AirMagnet alarms that are triggered when the wireless analyzer identifies performance deficiencies or security vulnerabilities that threaten non-compliance with the standard.

AirMagnet Compliance Reports match alarms in the WLAN with PCI DSS requirements and report the status of compliance for all wireless devices connected to the cardholder data network. The integrated algorithms identify root cause problems affecting compliance and supply expert advice to mitigate and resolve them.

AirMagnet Disclaimer

AirMagnet System Level and Device Level Compliance Reports provide information to assist its customers in determining whether they are in compliance with various standards, laws and regulations applicable to wireless networks and devices operating in the unregulated radio frequencies (2.4 - 5 GHz). It is intended to assist customers in identifying wireless networks and devices not in compliance with security frameworks such as FISMA (Federal Information Security Management Act) and US federal regulations implementing laws such as GLBA (Gramm, Leach, Bliley Act), HIPAA (Health Information Portability and Accountability Act), Sarbanes Oxley Act 2002, and more.

AirMagnet is **not** responsible for an organization's compliance with industry standards or legal regulations. AirMagnet should be used by organizations as an aid in satisfying the organization's compliance requirements for standards, laws, and regulations.

AirMagnet operation is limited to wireless networks and devices operating in the unregulated radio frequencies (2.4 - 5 GHz). It operates and reports on networks and devices that use wireless technologies. It does **not** apply to wire-line networks and devices **not** operating in the wireless spectrum.



1/ System Level Compliance Report

This report summarizes your network's overall compliance with the PCI (Payment Card Industry) Data Security Standard version 1.2 (Release: October 2008). The report details AirMagnet Analyzer's compliance and mitigation strategy by the specific requirement.

PCI Data Security Standards	Compliance
<p>1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations. This complies with PCI DSS Requirement 1.1.1 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer automatically identifies hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS, as well as dozens of wireless intrusions and hacking strategies, including rogue devices, Denial-of-Service attacks, Dictionary Attacks, Faked APs, RF Jamming, “Stumbler” tools, and more.</p>
<p>1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks. This complies with PCI DSS 1.1.2 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer reports the location of access points, client stations, and rogue devices operating in the entity's infrastructure. Analyzer also offers a convenient “Find Tool” that quickly tracks down rogue APs and non-complying devices that compromise network security threats to cardholder data.</p>
<p>6.2.b. Verify that process to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found. This complies with PCI DSS Requirement 6.2 for wireless connections and configurations.</p>	<p>All AirMagnet products are eligible for free technical support for up to one year from the date of purchase. Technical support includes software updates and upgrades that identify and help mitigate new vulnerabilities in the WLAN. Customers can renew their technical support contract on an annual basis</p>
<p>11.1.a Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices. This complies with PCI DSS Requirement 11.1 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer identifies all wireless devices in use in the WLAN and enables an entity to designate APs for client access to identify rogue devices operating without approval</p>
<p>11.2.a Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans. This complies with PCI DSS 11.2 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer can quickly find any change in the WLAN by automatically identifying hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS issues, as well as dozens of wireless intrusions and hacking strategies, including rogue devices, Denial-of-Service attacks, Dictionary Attacks, Faked APs, RF Jamming, “Stumbler” tools, and more.</p>



<p>11.2.c. Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained. This complies with PCI DSS Requirement 11.2 for wireless connections and configurations.</p>	<p>Laptop WiFi Analyzer can be operated on demand to automatically identify hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS, as well as dozens of wireless intrusions and hacking strategies, including Rogue devices, Denial-of-Service attacks, Dictionary Attacks, Faked APs, RF Jamming, "Stumbler" tools, and many more. AirMagnet also generates detailed compliance reports for the PCI DSS that provides a step-by-step pass/fail assessment of each section of the standard that can be archived and compared to previous scan results.</p>
<p>12.1.2 Establish, publish, maintain, and disseminate a security policy that includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment. This complies with PCI DSS Requirement 12.1.2 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer has the ability to create and manage policies to augment an entity's security policy by identifying and reporting threats and vulnerabilities in the WLAN and on wireless devices on an annual or ongoing basis. The security alarms generated by the AirWISE expert engine have proved powerful in WLAN security event management and analysis to identify threats and alert the appropriate personnel.</p>
<p>12.2.a. Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements. This complies with PCI DSS Requirement 12.2 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer can be used on a daily basis to assesses the WLAN and wireless device security for evolving threats and vulnerabilities and send alerts to identified staff.</p>
<p>12.3.2 Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (e.g., token). This complies with PCI DSS Requirement 12.3.2 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer helps develop usage policies for wireless networks and devices by monitoring access point authentication and encryption schemes and reviewing WLAN usage by AP and client station.</p>
<p>12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices. This complies with PCI DSS Requirement 12.3.3 for wireless connections and configurations.</p>	<p>AirMagnet WiFi Analyzer helps develop and implement usage policies for wireless networks and devices by identifying all wireless devices in the WLAN. After labeling all appropriate wireless devices, Analyzer will identify rogue devices and alert the appropriate personnel to take action.</p>

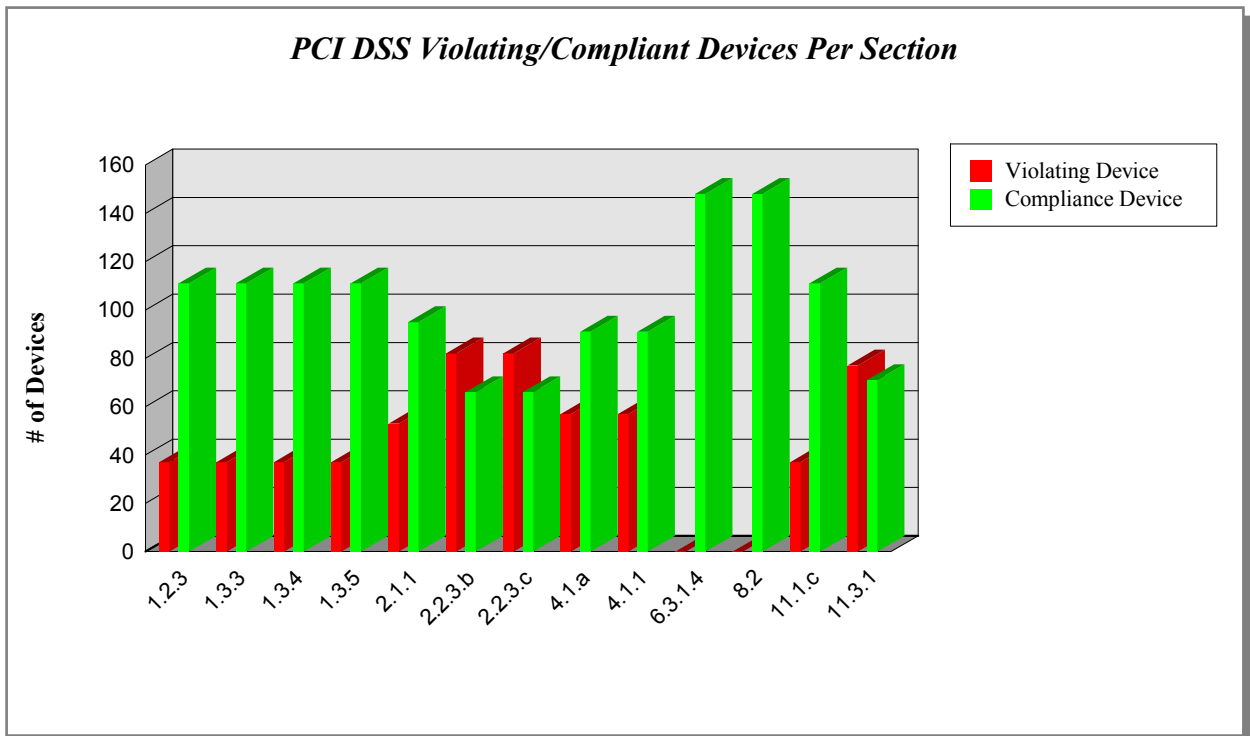
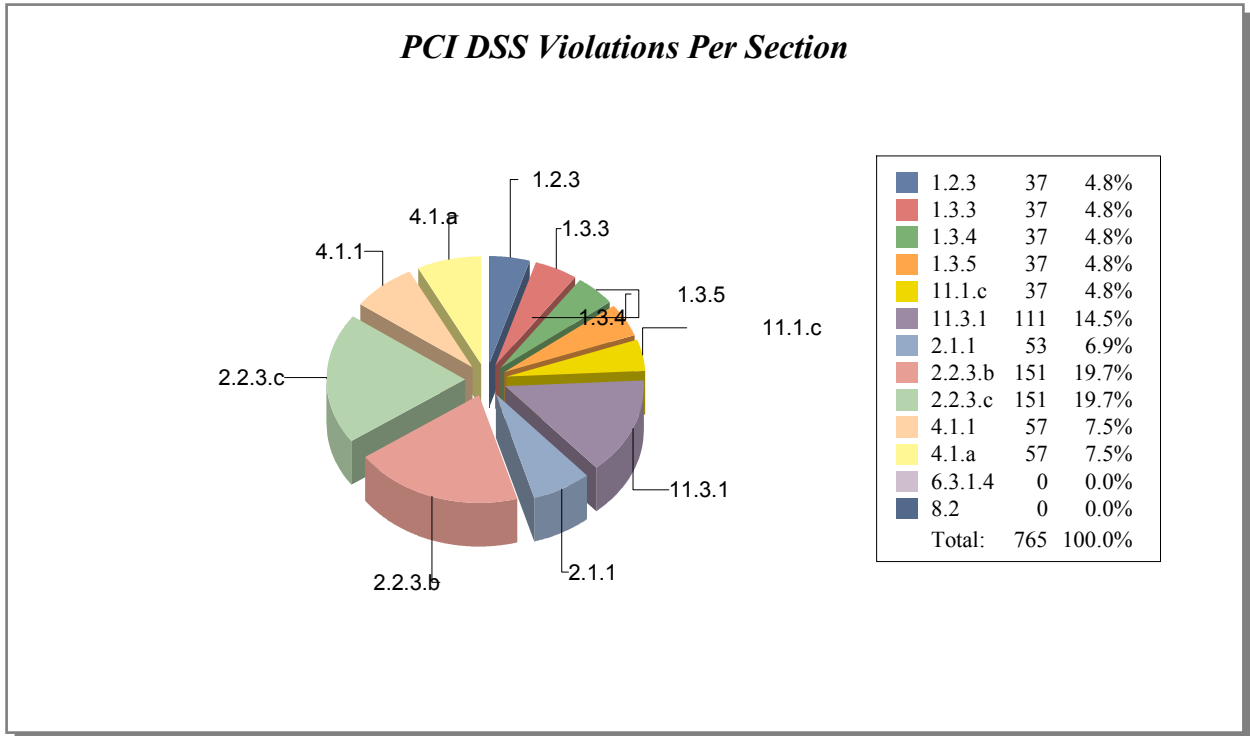


12.3.7 Verify that the usage policies require a list of company-approved products. This complies with PCI DSS Requirement 12.3.7 for wireless connections and configurations	AirMagnet WiFi Analyzer records and identifies APs and wireless products approved to operate in the WLAN.
12.9.6 Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. This complies with PCI DSS Requirement 12.9.6 for wireless connections and configurations	AirMagnet WiFi Analyzer is updated regularly with information on wireless vulnerabilities. The AirMagnet AirWISE analytical engine provides current, context-driven and case-specific advice for problem identification and resolution to help maintain and update an incident response plan.



2/ Policy Level Compliance Report

This report summarizes your network's compliance on a per-policy basis, showing you the total number of devices that are in compliance or violation of each and every policy in the PCI Data Security Standard.



PCI DSS	Policy Violation	# Violating Devices	# Compliance Devices	Compliance %
Testing Procedure 1.2.3 Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. This complies with PCI DSS Requirement 1.2.3 for wireless connections and configurations.	37	37	111	75.00%
Testing Procedure 1.3.3 Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment. This complies with PCI DSS Requirement 1.3.3 for wireless connections and configurations.	37	37	111	75.00%
Testing Procedure 1.3.4 Verify that internal addresses cannot pass from the Internet into the DMZ. This complies with PCI DSS Requirement 1.3.4 for wireless connections and configurations.	37	37	111	75.00%
Testing Procedure 1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ. This complies with PCI DSS Requirement 1.3.5 for wireless connections and configurations.	37	37	111	75.00%
Testing Procedure 2.1.1 Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (e.g., AES): Encryption keys were changed from default; default SNMP community strings on wireless devices were changed; default passwords, passphrases on access points were changed; firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (e.g, WPA, WPA2); other security-related wireless vendor defaults, if applicable. This complies with PCI DSS Requirement 2.1.1 for wireless connections and configurations.	53	53	95	64.19%
Testing Procedure 2.2.3.b Verify that common security parameter settings are included in system configuration standards.	151	82	66	44.59%
Testing Procedure 2.2.3.c For a sample of system components, verify that common security parameters are set appropriately. This complies with PCI DSS Requirement 2.2.3 for wireless connections and configurations.	151	82	66	44.59%
Testing Procedure 4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks: Verify that strong encryption is used during data transmission; select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit; Verify that only trusted SSL/TLS keys/certificates are accepted; verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) This complies with PCI DSS Requirement 4.1 for wireless connections and configurations.	57	57	91	61.49%



Testing Procedure 4.1.1 For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (e.g., IEEE 802.11i) are used to implement strong encryption for authentication and transmission. This complies with PCI DSS Requirement 4.1.1 for wireless connections and configurations.	57	57	91	61.49%
Testing Procedure 6.3.1.4 Validation of secure communications. This complies with PCI DSS Requirement 6.3.1.4 for wireless connections and configurations.	0	0	148	100.00%
Testing Procedure 8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: Obtain and examine documentation describing the authentication method(s) used; for each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). This complies with PCI DSS Requirement 8.2 for wireless connections and configurations.	0	0	148	100.00%
Testing Procedure 11.1 c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected. This complies with PCI DSS Requirement 11.1 for wireless connections and configurations.	37	37	111	75.00%
Testing Procedure 11.3.1 Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems. This complies with PCI DSS Requirement 11.3.1 for wireless connections and configurations.	111	77	71	47.97%



PCI Data Security Standard			
AirMagnet Alarms	# Violating Devices	# Compliance Devices	Compliance Status
[§ 1.2.3]Testing Procedure 1.2.3. Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. This complies with PCI DSS Requirement 1.2.3 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
[§ 1.3.3] Testing Procedure 1.3.3 Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment. This complies with PCI DSS Requirement 1.3.3 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
[§ 1.3.4] Testing Procedure 1.3.4 Verify that internal addresses cannot pass from the Internet into the DMZ. This complies with PCI DSS Requirement 1.3.4 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
[§ 1.3.5] Testing Procedure 1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ. This complies with PCI DSS Requirement 1.3.5 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
[§ 2.1.1] Testing Procedure 2.1.1 Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (e.g., AES): Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions; default SNMP community strings on wireless devices were changed; default passwords, passphrases on access points were changed; firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (e.g, WPA, WPA2); other security-related wireless vendor defaults, if applicable. This complies with PCI DSS Requirement 2.1.1 for wireless connections and configurations.			
AP broadcasting SSID	53	95	64.19%
[§ 2.2.3.b] Testing Procedure 2.2.3.b Verify that common security parameter settings are included in system configuration standards.			
Station with open WLAN connection	1	147	99.32%
	2	146	98.65%
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%



AP broadcasting SSID	53	95	64.19%
Device unprotected by TKIP	57	91	61.49%
DoS: De-Auth broadcast attack	1	147	99.32%
[§ 2.2.3.c] Testing Procedure 2.2.3.c For a sample of system components, verify that common security parameters are set appropriately. This complies with PCI DSS Requirement 2.2.3 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
AP broadcasting SSID	53	95	64.19%
DoS: De-Auth broadcast attack	1	147	99.32%
Station with open WLAN connection	1	147	99.32%
Device unprotected by TKIP	57	91	61.49%
	2	146	98.65%
[§ 4.1.a] Testing Procedure 4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks: Verify that strong encryption is used during data transmission; select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit; Verify that only trusted SSL/TLS keys/certificates are accepted; verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) This complies with PCI DSS Requirement 4.1 for wireless connections and configurations.			
Device unprotected by TKIP	57	91	61.49%
[§ 4.1.1] Testing Procedure 4.1.1 For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (e.g., IEEE 802.11i) are used to implement strong encryption for authentication and transmission. This complies with PCI DSS Requirement 4.1.1 for wireless connections and configurations.			
Device unprotected by TKIP	57	91	61.49%
[§ 11.1.c] Testing Procedure 11.1 c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected. This complies with PCI DSS Requirement 11.1 for wireless connections and configurations.			
Unauthorized AP by ACL detected	34	114	77.03%
Unauthorized client by ACL detected	3	145	97.97%
[§ 11.3.1] Testing Procedure 11.3.1 Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems. This complies with PCI DSS Requirement 11.3.1 for wireless connections and configurations.			
Station with open WLAN connection	1	147	99.32%
Device unprotected by TKIP	57	91	61.49%
AP broadcasting SSID	53	95	64.19%

Notes:

- 1) By default, your network fails to comply with the Payment Card Industry (PCI) Data Security Standard if one of the devices violates any of its policy sections.
- 2) Channel specific policy violations will not be included in the Device-Specific Compliance Report.
- 3) AirMagnet has enabled alarms relevant to the PCI Data Security Standard in its Policy Compliance Reports. Disabling any alarms tied to the Reports will degrade their effectiveness and result in a wireless network that does not comply with the respective industry regulations.



3/ Device-Specific Compliance Report

This report contains detailed information about devices in compliance or violation of the PCI Data Security Standard. It checks the devices against each and every provision in the Directive to show what policy sections are violated or upheld to. It lists all wireless devices deployed on your WLAN. The devices can be sort by MAC address, media type, SSID, or vendor.

Device Information	PCI Data Security Standard Policy Sections													Compliance %	
	MAC Address-Media	1.2.3	1.3.3	1.3.4	1.3.5	2.1.1	2.2.3.b	2.2.3.c	4.1.a	4.1.1	6.3.1.4	8.2	11.1.c		11.3.1
00:13:E8:06:F5:E1-a Channel: ? Intel QA-AirPort-jav		P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:90:4B:BD:FC:3A-g Channel: ? GemTek QA-AirPort-jav		P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:14:6A:07:3B:B0-g Channel: 11 Cisco QACiscoVoice		F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:A0:F8:E7:EE:0D-g Channel: 1 Symbol 188		P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:0F:34:A7:78:14-g Channel: 1 Cisco QAVOFI		P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:21:6A:40:20:24-g Channel: 1 Intel Air2		F	F	F	F	P	F	F	P	P	P	P	F	P	46.15%
00:20:A6:52:8F:65-g Channel: ? Proxim meru-eng		P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1F:3B:11:9D:03-g Channel: ? Intel meru-eng		P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:15:F9:57:A0:22-a Channel: 40 Cisco AirMagnetGuest		P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%



00:11:5C:4D:E8:41-g Channel: 1 Cisco AirMagnetGuest	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:0F:34:A7:78:13-g Channel: 1 Cisco QASpectralink	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:A0:F8:E7:EE:0C-g Channel: 1 Symbol meru-eng	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
06:06:C9:AA:ED:CF-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:0E:35:C0:35:7D-g Channel: ? Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1C:BF:CE:29:C4-g Channel: 40 Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:19:D2:D6:4B:AE-g Channel: 1 Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:12:17:DB:88:81-g Channel: ? Cisco-linksys QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:0B:6B:B0:18:F1-g Channel: ? Wistron Neweb QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1D:7D:45:50:DE-g Channel: ? GIGABYTE QA-AirPort-jav	P	P	P	P	P	F	F	P	P	P	P	P	F	76.92%
00:1F:3C:C7:91:8E-a Channel: ? Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%



00:15:F9:57:A0:21-a Channel: 40 Cisco AirMagnetGuest	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:17:DF:A6:5B:DC-a Channel: 56 Cisco QA-1250-WIFI-TM	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:11:5C:4D:E8:40-g Channel: 1 Cisco Air2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:0F:34:A7:78:12-g Channel: 1 Cisco QAVocera	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
06:06:C9:CC:75:0B-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:16:6F:31:0B:0A-a Channel: 40 Intel AirMagnetGuest	F	F	F	F	P	F	F	P	P	P	P	F	P	46.15%
00:1D:E0:8C:CD:A9-g Channel: ? Intel AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:02:6F:20:0C:6B-g Channel: ? Senao QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:15:F9:57:A0:20-a Channel: 40 Cisco Air2	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:15:F9:57:95:41-a Channel: 44 Cisco AirMagnetGuest	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:13:80:43:15:2F-a Channel: 157 Cisco QACiscoVoice	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%



00:0F:34:A7:78:11-g Channel: 1 Cisco QACisco-2	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
06:06:C9:B0:AE:4C-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:17:DF:A7:EA:30-g Channel: 8 Cisco WIFI-EURO-GN	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:1A:70:40:B3:C4-g Channel: 9 Cisco-linksys QA-linksysN-jav	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:0D:0B:4F:5E:00-g Channel: 9 Buffalo qatest'sắ	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:15:F9:57:95:40-a Channel: 44 Cisco Air2	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:13:80:43:15:2E-a Channel: 157 Cisco QACisco-2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:0F:34:A7:78:10-g Channel: 1 Cisco QACiscoVoice	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:A0:F8:E9:62:ED-g Channel: ? Symbol meru-eng	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
06:24:C9:4C:F3:E9-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:02:6F:20:2E:0D-a Channel: ? Senao AM__Test	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%



00:1F:3C:C2:41:7A-a Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:15:2D-a Channel: 157 Cisco QAVocera	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%	
06:06:C9:D9:0C:9F-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%	
06:06:C9:5F:F5:52-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%	
00:1E:2A:DC:0C:22-g Channel: ? Netgear hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%	
00:0B:6B:B0:AE:4C-g Channel: ? Wistron Neweb hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%	
00:40:96:B4:7D:E4-g Channel: ? Cisco AM__Test	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%	
00:15:6D:84:0D:9D-a Channel: ? Ubiquiti QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%	
00:90:7A:03:D2:5F-g Channel: ? SpectralLink QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%	
00:13:80:43:15:24-g Channel: 6 Cisco QAVOFI	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%	
00:13:80:43:15:2C-a Channel: 157 Cisco QASpectralink	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%	



06:24:C9:B0:0E:B1-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:22:FA:38:B3:FA-a Channel: ? hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:40:96:A1:96:4E-g Channel: ? Cisco hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:90:4B:CC:75:0B-g Channel: ? GemTek hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:A0:F8:9E:A7:29-g Channel: ? Symbol hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:16:EA:5F:F5:52-g Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:E8:68:00:A5-g Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:15:23-g Channel: 6 Cisco QASpectralink	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%
00:14:A8:53:4C:64-g Channel: 9 Cisco QAVOFI	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:15:F9:57:93:92-a Channel: 36 Cisco QAVOFI	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:15:F9:57:9E:92-a Channel: 40 Cisco QAVOFI	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%



00:13:80:43:15:2B-a Channel: 157 Cisco QAVOFI	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%
00:14:69:06:76:84-a Channel: 36 Cisco QAVOFI	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1F:F3:BA:9E:11-a Channel: 36 QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:11:55-g Channel: ? Cisco QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:0B:86:28:68:00-g Channel: 1 Aruba aram	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:F1:AF:1B:90-g Channel: 3 Cisco Kam-Test	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:13:80:43:15:22-g Channel: 6 Cisco QAVocera	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:11:5C:44:5E:B1-g Channel: 7 Cisco AirMagnetGuest	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:14:A8:53:4C:63-g Channel: 9 Cisco TS-1200-SH	P	P	P	P	F	F	F	P	P	P	P	P	F	69.23%
00:15:F9:57:93:91-a Channel: 36 Cisco AirMagnetGuest	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%
00:15:F9:57:9E:91-a Channel: 40 Cisco AirMagnetGuest	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%



06:24:C9:BB:28:A5-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:14:69:06:76:83-a Channel: 36 Cisco TS-1200-SH	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:22:FA:CF:2B:B6-a Channel: ? QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:16:EA:5F:D3:2C-g Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:40:96:B5:66:46-g Channel: ? Cisco meru-eng	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:15:21-g Channel: 6 Cisco QACisco-2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:11:5C:44:5E:B0-g Channel: 7 Cisco Air2	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:0F:B5:57:0E:52-g Channel: 10 Netgear Air2	F	F	F	F	P	F	F	P	P	P	P	F	P	46.15%
00:14:A8:53:4C:62-g Channel: 9 Cisco Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:15:F9:57:93:90-a Channel: 36 Cisco Air2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:15:F9:57:9E:90-a Channel: 40 Cisco Air2	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%



06:24:C9:C7:91:8E-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
06:24:C9:A1:96:4E-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:13:80:43:11:54-g Channel: 11 Cisco QA-1200-32	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:14:69:06:76:82-a Channel: 36 Cisco meru-eng	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
06:06:C9:4C:F3:E9-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:1C:BF:44:7F:43-g Channel: ? Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:21:5D:74:AC:1E-g Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:11:53-g Channel: ? Cisco QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1C:BF:52:12:E1-a Channel: 44 Intel Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:40:96:AA:ED:CF-g Channel: ? Cisco Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:80:43:15:20-g Channel: 6 Cisco QACiscoVoice	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%



00:12:17:FA:CA:80-g Channel: 6 Cisco-linksys Linksys'test	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:14:A8:53:4C:61-g Channel: 9 Cisco TS-1200-AK12345678901 2345	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:6A:07:3B:BF-a Channel: 161 Cisco QACiscoVoice	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:69:06:76:81-a Channel: 36 Cisco QACisco-2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:E8:BB:28:A5-a Channel: 40 Intel AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:16:EA:5F:0A:36-a Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1C:F0:D9:0C:9F-g Channel: ? D-Link Air2	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1F:1F:0B:8C:C4-g Channel: 1 Edimax anygate	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:A8:53:4C:60-g Channel: 9 Cisco TS-1200-AA	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
00:14:6A:07:3B:BE-a Channel: 161 Cisco QACisco-2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:69:06:76:80-a Channel: 36 Cisco TS-1200-AA	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%



06:24:C9:B5:66:46-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:13:80:43:11:52-g Channel: 11 Cisco QA-1200-30	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:1C:BF:81:36:80-g Channel: ? Intel QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:11:5C:4D:E8:F1-g Channel: 4 Cisco AirMagnetGuest	F	F	F	F	F	F	F	P	P	P	P	F	F	30.77%
00:11:50:05:97:1F-g Channel: 6 Belkin AM_Test	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:A5:31:F2:E4-g Channel: 6 GemTek default	P	P	P	P	F	F	F	F	F	P	P	P	F	53.85%
06:24:C9:BA:9E:11-a Channel: 36 QAVocera	F	F	F	F	P	F	F	P	P	P	P	F	P	46.15%
00:14:6A:07:3B:BD-a Channel: 161 Cisco QAVocera	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
06:24:C9:45:50:DE-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:0C:E6:9D:B2:08-a Channel: 36 Meru meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:13:80:43:11:51-g Channel: 11 Cisco QA-1200-26	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%



00:12:F0:1A:51:96-g Channel: ? Intel AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:22:69:0D:B3:98-g Channel: 1 Hon Hai Precision AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:21:6A:0A:BF:CE-g Channel: ? Intel AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:90:4B:91:47:B4-g Channel: ? GemTek QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:A0:F8:E9:62:6D-g Channel: ? Symbol QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:11:5C:4D:E8:F0-g Channel: 4 Cisco Air2	F	F	F	F	F	F	F	F	F	P	P	F	F		15.38%
00:14:6A:07:3B:B4-g Channel: 11 Cisco QAVOFI	F	F	F	F	F	F	F	P	P	P	P	F	F		30.77%
00:14:6A:07:3B:BC-a Channel: 161 Cisco QASpectralink	F	F	F	F	F	F	F	P	P	P	P	F	F		30.77%
06:06:C9:BD:FC:3A-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F		61.54%
00:13:80:43:11:50-g Channel: 11 Cisco QA-1200-25	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:17:A4:22:D6:CB-g Channel: 10 HEWLETT PACKARD hpsetup	F	F	F	F	P	F	F	P	P	P	P	F	P		46.15%



00:19:7E:4C:F3:E9-g Channel: ? AM__Test	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:0B:6B:B0:0E:B1-g Channel: ? Wistron Neweb QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:0B:6B:B0:18:E5-g Channel: ? Wistron Neweb QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:40:96:B5:82:54-g Channel: ? Cisco QA-AirPort-jav	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:14:6A:07:3B:B3-g Channel: 11 Cisco QASpectralink	F	F	F	F	F	F	F	P	P	P	P	F	F		30.77%
00:14:6A:07:3B:BB-a Channel: 161 Cisco QAVOFI	F	F	F	F	F	F	F	P	P	P	P	F	F		30.77%
06:06:C9:CE:29:C4-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F		61.54%
00:0E:35:71:D1:05-g Channel: ? Intel hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:11:5C:4D:E9:11-g Channel: 7 Cisco AirMagnetGuest	F	F	F	F	F	F	F	P	P	P	P	F	F		30.77%
00:14:6A:07:3B:B2-g Channel: 11 Cisco QAVocera	F	F	F	F	F	F	F	F	F	P	P	F	F		15.38%
06:24:C9:B0:AE:4C-a Channel: 36 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F		61.54%



00:0C:E6:82:BA:3A-g Channel: 6 Meru meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:21:6A:32:96:B2-g Channel: ? Intel hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
00:13:02:77:23:ED-g Channel: ? Intel hpsetup	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%
06:06:C9:8C:CD:A9-g Channel: 6 meru-eng	P	P	P	P	P	F	F	F	F	P	P	P	F	61.54%
00:11:5C:4D:E9:10-g Channel: 7 Cisco Air2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:14:6A:07:3B:B1-g Channel: 11 Cisco QACisco-2	F	F	F	F	F	F	F	F	F	P	P	F	F	15.38%
00:A0:F8:E7:EE:0E-g Channel: 1 Symbol AirMagnetGuest	P	P	P	P	P	P	P	P	P	P	P	P	P	100.00%

Notes:

1) Channel specific policy violations will not be included in the Device-Specific Compliance Report.

2) For further information on the standard please visit

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml