

Cisco Unified Wireless Network Solution Positioning for the New PCI DSS Wireless Guideline

This document directly addresses the recommendations listed in the “Information Supplement: PCI DSS Wireless Guideline.” The full guideline can be found at <http://www.pcisecuritystandards.org>. This document addresses these guidelines in relation to the Cisco® Unified Wireless Network, including CAPWAP devices, the Cisco Unified Wireless LAN Controller, Mobility Services Engine (MSE), Cisco Adaptive Wireless IPS (wIPS) service, and Cisco Wireless Control System (WCS). This document does not address Cisco autonomous or standalone access points in relation to the new PCI DSS Wireless Guideline.

The descriptions and recommendations are copied verbatim from the wireless guideline. Additional information can be found in the full information supplement, which is referenced above. Cisco solutions will be highlighted in **RED** for easier reading and filtering.

Summary of Results

Table 1 provides a quick look at how the Cisco Unified Wireless Network solution supports the recommendations listed in the information supplement. “Y” = Yes, the Unified Wireless Network Solution supports this recommendation; “N” = No, the Unified Wireless Network Solution does not support this recommendation; and “N/A” = this recommendation is not applicable to the Unified Wireless Network technology.

The numbering in this document does not directly correspond to the numbering in the information supplement. For example, Section 1 in this document relates to Section 3 in the information supplement.

Table 1. Executive Summary Results

1.1.1 – Y	1.2.1.A – Y	1.2.1.B – Y	1.2.1.C – Y	1.3.1.A – Y/N (ASA 5500 or ISR)	1.3.1B – N/A
1.3.1C – N/A	2.1.1A – N/A	2.1.1.B – Y	2.1.1.C – N/A	2.1.1.D – Y	2.2.1.A – Y
2.2.1.B – Y	2.2.1.C – Y	2.2.1.D – Y	2.2.1.E – Y	2.3.1.A – Y	2.3.1.B – Y (some)
2.3.1.C – Y	2.3.1.D – Y	2.3.1.E – Y (some)	2.3.1.F – N/A	2.3.1.G – Y	2.4.1.A – Y
2.4.1.B – Y	2.4.1.C – N/A	2.4.1.D – Y	2.4.1.E – Y	2.5.1.A – Y	2.5.1.B – Y
2.6.1.A – Y	2.6.1.B – Y	2.6.1.C – Y	2.6.1.D – N/A	2.6.1.E – N/A	2.6.1.F – Y (some)
2.6.1.G – N	2.6.1.H – Y	2.6.1.I – N/A			

1. Applicable Requirements Pertaining to Wireless for All Networks

Wireless networking is a concern for all organizations that store, process, or transmit cardholder data and therefore must adhere to the PCI DSS. Even if an organization that must comply with PCI DSS does not use wireless networking as part of the Cardholder Data Environment (CDE), the organization must verify that its wireless networks have been segmented away from the CDE and that wireless networking has not been introduced into the CDE over time.

Although the PCI DSS outlines requirements for securing existing wireless technologies, there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially

dangerous rogue devices. A rogue wireless device is an unauthorized wireless device that can allow access to the CDE.

Wireless networks can be considered outside of the scope of PCI DSS if (i) no wireless network is deployed or (ii) if wireless has been deployed and segmented away from the CDE.

Regardless of whether wireless networks have been deployed, periodic monitoring is needed to keep unauthorized or rogue wireless devices from compromising the security of the CDE. Segmenting wireless networks out of PCI DSS scope requires a firewall between the wireless network and the CDE.

1.1 Maintain a Hardware Inventory

Answering the question “is a *known* WLAN deployed?” within the organization’s network depends upon the organization knowing the boundaries of the network and having an accurate networking inventory and hardware inventory.

It is strongly recommended that the organization scan all CDE locations for known WLAN devices and maintain an up-to-date inventory. Without such an inventory, the organization would not know they existed and, therefore, any that were found would have to be initially treated as rogue devices. Therefore, while not specifically mandated by PCI DSS, related documents *imply* that such an inventory should exist while authority documents outside of the PCI DSS realm mandate it

1.1.1 Summary of Recommendations

Ensure that the organization maintains an up-to-date hardware inventory so that known access points can easily be distinguished from rogue access points.

Yes. In the Cisco Unified Wireless Network, the Cisco WCS maintains a list of all wireless devices connected to the network. This can be used as the inventory list.

1.2 Wireless Scanning to Look for Rogue Access Points

The purpose of PCI DSS requirement 11.1 is to ensure that a rogue wireless device introduced into an organization’s network does not allow unmanaged and unsecured WLAN access to the CDE. The intent is to prevent an attacker from using rogue wireless devices to negatively impact the security of cardholder data.

In order to combat rogue WLANs, it is acceptable to use a wireless analyzer or a preventative control such as a wireless intrusion detection or prevention system (IDS/IPS) as defined by the PCI DSS, referenced in Table 2.

Table 2. PCI DSS 11.1

PCI DSS Requirement 11.1	Testing Procedure
Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	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. If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel. Verify the organization’s Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.

Since a rogue device can potentially show up in any CDE location, it is important that all locations that store, process, or transmit cardholder data are either scanned regularly or that a wireless IDS/IPS is implemented in those locations. Organizations must ensure that they scan all sites quarterly to comply with the standard. The organization’s responsibility is to ensure that the CDE is compliant at all times.

PCI DSS requirement 11.1 clearly specifies the use of a wireless analyzer or a wireless IDS/IPS system for scanning. Relying on wired side scanning tools (e.g. tools that scan suspicious hardware MAC addresses on switches) may identify some unauthorized wireless devices; however, they tend to have high false positive/negative detection rates. Wired network scanning tools that scan for wireless devices often miss cleverly hidden and disguised rogue wireless devices or devices that are connected to isolated network segments. Wired scanning also

fails to detect many instances of rogue wireless clients. A rogue wireless client is any device that has a wireless interface that is not intended to be present in the environment.

Wireless analyzers can range from freely available PC tools to commercial scanners and analyzers. The goal of all of these devices is to “sniff” the airwaves and “listen” for wireless devices in the area and identify them. Using this method, a technician or auditor can walk around each site and detect wireless devices. The person would then manually investigate each device to determine if it allows access to CDE and classify them as rogues or just friendly neighboring wireless device.

Although this method is technically possible for a small number of locations, it is often operationally tedious, error-prone, and costly for organizations that have several CDE locations. For large organizations, it is recommended that wireless scanning be automated with a wireless IDS/IPS system.

Although the PCI DSS standard does not directly state what the output of wireless analysis should be, it does imply that it should be created, reviewed, and used to mitigate the risk of unauthorized or rogue wireless devices. At a minimum, the list of wireless devices should clearly identify all rogue devices connected to the CDE. To comply with the intent of PCI DSS requirement 11.1, companies should immediately remediate the rogue threat in accordance with PCI DSS requirement 12.9 and rescan the environment at the earliest possible opportunity.

1.2.1 Summary of Recommendations

A. Use a wireless analyzer or a wireless IDS/IPS to detect unauthorized/rogue wireless devices that could be connected to the CDE at least quarterly at all locations. For large organizations having several CDE locations, a centrally managed wireless IDS/IPS to detect and contain unauthorized/rogue wireless devices is recommended.

Yes. The Cisco Unified Wireless Network can use the Adaptive Wireless IPS Software service (Adaptive wIPS) to detect and contain unauthorized/rogue wireless devices. The centralized Adaptive wIPS performs 24-hour scanning to immediately detect and contain unauthorized/rogue wireless devices.

B. Enable automatic alerts and containment mechanisms on the wireless IPS to eliminate rogues and unauthorized wireless connections into the CDE.

Yes. Cisco Adaptive wIPS automatically detects, classifies, alerts, and mitigates rogue access points, clients, and ad hoc connections.

C. Create an “Incident Response Plan” to physically eliminate rogue devices immediately from the CDE in accordance with PCI DSS requirement 12.9.5.

Yes. The Cisco Unified Wireless Network can locate individual rogue devices using the Cisco Wireless Control System (WCS), or locate multiple rogue devices using the Context-Aware location services in the Cisco 3300 Series Mobility Services Engine. By identifying the physical location of rogue devices, administrators can quickly physically eliminate these devices from the CDE. The Cisco Wireless Location Appliance also provides wire-side location, and Adaptive wIPS rogue switchport tracing can trace rogue devices down to a specific switchport.

1.3 Segmenting Wireless Networks

PCI DSS requires that wireless networks that do not store, process, or transmit card holder data must be isolated from the CDE using a firewall (Table 3). The intent is to prevent unauthorized users from being able to access the CDE via a wireless network deployed for purposes other than credit card transactions. The wireless firewall should perform the following general functions:

A. Completely isolate wireless network traffic from entering the CDE by filtering wireless packets based on the 802.11 protocol.

B. Perform stateful inspection of connections.

C. Monitor and log traffic allowed and denied by the firewall in accordance with PCI DSS requirement 10.

Table 3. PCI DSS 1.2.3

PCI DSS Requirement 1.2.3	Testing Procedure
Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	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.

If a firewall is being shared between wireless and other protocols/applications, the default policy for the firewall for handling inbound traffic should be to block all packets and connections into the CDE unless the traffic type and connections have been specifically permitted. This approach is more secure than another approach used often: permit all connections and traffic by default and then block specific traffic and connections.

Wireless traffic should explicitly be blocked. Organizations should consider using outbound traffic filtering as a technique for further securing their networks and reducing the likelihood of internally based attacks.

Relying on Virtual LAN (VLAN) based segmentation alone is not sufficient. For example, having the CDE on one VLAN and the WLAN on a separate VLAN does not adequately segment the WLAN and take it out of PCI DSS scope.

1.3.1 Summary of Recommendations

A. Use a stateful packet inspection firewall to block wireless traffic from entering the CDE. Augment the firewall with a wireless IDS/IPS.

Yes. Cisco recommends Cisco ASA 5500 Series Adaptive Security Appliances or Cisco Integrated Services Routers with Cisco IOS® Firewall to provide stateful firewall functionality to segment the CDE. In most organizations, wireless traffic is not the only traffic that needs to traverse the firewall. It is not recommended that all traffic flow through a wireless stateful firewall; rather, the wireless traffic should go through a high-performing, advanced stateful firewall such as the Cisco ASA 5500 Series Adaptive Security Appliance or a Cisco Integrated Services Router with Cisco IOS® Firewall.

In the Unified Wireless Network, Cisco augments the stateful firewall with the Adaptive WIPS.

B. Do not use VLAN based segmentation with MAC address filters for segmenting wireless networks.

N/A. This recommendation is not specific just to the wireless devices. Cisco supports this recommendation through both VLANs and stateful firewall to segment wireless networks from the CDE.

C. Monitor firewall logs daily and verify firewall rules at least once every six months.

N/A. Cisco provides firewall logs to a central security incident and event manager (SIEM) device such as the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS), which also collects wireless information in the network. It is the responsibility of the personnel to review the logs and firewall rules.

2 Applicable Requirements for In-Scope Wireless Networks

Wireless networks that are part of the CDE must comply with all PCI DSS requirements. This includes using a firewall (requirement 1.2.3) and making sure that additional rogue wireless devices have not been added to the CDE (requirement 11.1). In addition, PCI DSS compliance for systems that include WLANs as a part of the CDE requires extra attention to WLAN specific technologies and processes such as:

- A. Physical security of wireless devices,
- B. Changing default passwords and settings on wireless devices,
- C. Logging of wireless access and intrusion prevention,
- D. Strong wireless authentication and encryption,
- E. Use of strong cryptography and security protocols, and
- F. Development and enforcement of wireless usage policies.

2.1 Physical Security of Wireless Devices

PCI DSS promotes the need for physical security surrounding wireless devices. The focus of this requirement is on securing publicly accessible or risky devices. For example, one would not put a physical cage around every AP or chain down every handheld device, but one should secure those devices that are generally accessible to the public or at risk of being lost or compromised.

Obvious risks to physical security (other than theft) include the ability of an unauthorized person to reset the AP to factory defaults. The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the AP.

It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing.

If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel out any security settings on the device. Additionally, reset can be invoked remotely over the management interface or by using a serial console interface on the AP. These require physical access and PCI DSS requires that adequate mechanisms need to be in place to prevent unauthorized physical access to wireless devices (Table 4).

Table 4. PCI DSS 9.1.3

PCI DSS Requirement 9.1.3	Testing Procedure
Restrict physical access to wireless access points, gateways, and handheld devices.	Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.

Although the requirements do not state how to secure such devices, many ways exist to implement physical security. Options for securing wireless devices may include physically restricting access (e.g. by mounting APs high up on the ceiling) and disabling the console interface and factory reset options by using a tamper-proof chassis.

Instead of reverting to factory defaults, physically resetting an AP should result in centrally managed configurations being re-applied. Similarly, many enterprise APs are equipped with special mounting brackets that prevent ready access to the Ethernet cable.

2.1.1 Summary of Recommendations

- A. Mount APs on ceilings and walls that do not allow easy physical access.

Yes. This recommendation does not apply to technology; however, Cisco access points are easily mounted to ceilings and walls. Cisco access points are plenum rated, which gives the customer the option to place the access point in the ceiling to make physical access more difficult. Proper mounting procedures and recommendations for each model are documented in the access point installation guide.

- B. Use APs with chassis and mounting options that prevent physical access to ports and reset features. APs housed in tamper-proof chassis are recommended.

Yes. If a Cisco access point is reset, the access point looks to the WLAN controller for configuration settings, rather than resetting to factory defaults. Furthermore, Cisco lightweight access points cannot function without a WLAN controller, which the administrator has complete control over. In other words, physical access to a Cisco access point poses no risk. For customers that require tamper-proof enclosures, Cisco partners manufacture tamper-proof chassis for Cisco access points. Cisco mounting brackets block physical access to the reset button, Ethernet and console ports.

C. Secure handheld devices with strong passwords and always encrypt PSKs if cached locally.

N/A. Cisco does not manufacture handheld devices.

D. Use a wireless monitoring system that can track and locate all wireless devices and report if one or more devices are missing.

Yes. Cisco Context-Aware location services in the Mobility Services Engine track and locate wireless devices and will report if any are missing.

2.2 Changing the Default Settings of the APs

Changing default administrative passwords, encryption settings, reset function, automatic network connection functions, factory default shared keys and Simple Network Management Protocol (SNMP) access will help eliminate many of the vulnerabilities that can impact the security of the CDE through unauthorized wireless access.

Table 5. PCI DSS 2.1.1

PCI DSS Requirement 2.1.1	Testing Procedure
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.	<p>Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES):</p> <ul style="list-style-type: none"> • 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 (for example WPA/WPA2). • Other security-related wireless vendor defaults, if applicable.

Disable all unnecessary hardware, services, and applications that the AP might have shipped with. Check for the following protocols to ensure that they aren't configured unless absolutely necessary:

- A. Dynamic Host Configuration Protocol (for assigning IP addresses on the fly)
- B. HTTP SSL (for protected web pages)
- C. Wireless zero configuration service (for those APs and devices connecting to them) that run on Windows OS.

2.2.1 Summary of Recommendations

A. Enable WPA or WPA2 and make sure that default PSKs are changed. Enterprise mode is recommended.

Yes. The Cisco Unified Wireless Network supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. There is no default PSK and all PSKs must be created during configuration.

B. Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.

Yes. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

C. Do not advertise organization names in the SSID broadcast.

Yes. This is not a technology-specific requirement, but Cisco does not advertise the organization's name in the SSID broadcast. Cisco also disables SSID broadcast by default for non-guest networks.

D. Synchronize the APs' clocks to be the same as other networking equipment used by the organization.

Yes. The Cisco Unified Wireless Network does sync clocks to be the same as other networking equipment.

E. Disable all unnecessary applications, ports, and protocols.

Yes. Cisco provides an automated wireless security vulnerability scanning function in the WCS, which continuously identifies configurations, ports, and protocols that are vulnerable to exploits and threats.

2.3 Wireless Intrusion Prevention and Access Logging

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An Intrusion Detection System (IDS) is software that automates the intrusion detection process. An Intrusion Prevention System (IPS) is a system that has all the capabilities of an IDS and can also attempt to stop possible incidents.

Table 6. PCI DSS 11.4

PCI DSS Requirement 11.4	Testing Procedure
Use intrusion-detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	Verify the use of intrusion-detection systems and/or intrusion prevention systems and ensure that all traffic in the cardholder data environment is monitored. Confirm IDS and/or IPS are configured to alert personnel of suspected compromises. Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Wireless IDS/IPS provides several types of security capabilities intended to detect misconfiguration, misuse, and malicious activity. These capabilities can be grouped into three categories:

- (i) Rogue wireless device containment,
- (ii) Detection of unsafe activity or configurations,
- (iii) Selection of denial of service attacks, and wireless intrusion attempts.

Unauthorized wireless devices connected to the CDE must be detected and disabled. A wireless IPS should be able to find these rogue devices even when they are configured to not broadcast information about themselves or present in isolated network segments.

In addition to rogue containment, organizations should evaluate the automatic device classification capabilities of the wireless IDS/IPS for situations when connectivity cannot be determined. A wireless IDS/IPS should be able to observe all access points and clients, on all operational channels, and classify each device as authorized, unauthorized/rogue, or neighboring.

A wireless IDS/IPS can detect misconfigurations and unsafe activity by monitoring and analyzing wireless communications. Most can identify APs and clients that are not using the proper security controls. This includes detecting misconfigurations and the use of weak WLAN protocols.

A wireless IDS/IPS can analyze wireless traffic to look for malicious activity such as Denial of Service (DoS) and individual attacks on devices.

An IDS/IPS system can generate a lot of wireless threat information. In order for the organization to be able to use this information, the information has to be properly logged. This implies that the logs from the IDS/IPS have to be coordinated with other logging systems on the network (if there are any). In this case, the organization must ensure that at least the following logging items are coordinated correctly:

- A. The log file prefix (used to identify the device conducting the logging).
- B. The level of logging (the types of events to log).
- C. The log auto-roll setting (whether a new log file is created when the device is restarted, or the maximum log size is reached).
- D. The log maximum (log age in days).

After gathering the information within the IDS/IPS, the organization **must read and respond to the IDS/IPS reports**. If there are anomalies, they must be resolved. It is *not* enough to merely purchase and properly configure the IDS/IPS.

2.3.1 Summary of Recommendations

A. Use a centrally controlled wireless IDS/IPS to monitor for unauthorized access and detect rogues and misconfigured wireless devices.

Yes. Cisco provides the centrally controlled Adaptive WIPS to detect and mitigate rogue devices and the automated security vulnerability scanning in the WCS to identify misconfigured wireless devices.

B. Enable historical logging of wireless access that can provide granular wireless device information and store event logs and statistics for at least 90 days.

Yes. Cisco logs wireless access and granular wireless device information. It can store event logs and statistics up to the capacity of the WCS server. Length of time will depend on the volume of data. Adaptive WIPS events and forensics can be stored for multiple years on the Mobility Services Engine that Adaptive WIPS runs on.

C. Enable IPS features that automatically disable rogue wireless devices connecting to the CDE as well as accidental or malicious associations of wireless clients.

Yes. Cisco Adaptive WIPS can automatically disable rogue wireless devices connecting to the CDE as well as accidental/malicious associations of wireless clients. The client exclusion capabilities of the Cisco Unified Wireless Network can also identify and blacklist potentially malicious users.

D. Ensure the IPS signature set is regularly updated as new threats are discovered.

Yes. Cisco Adaptive WIPS provides continual updates of wireless IPS signatures.

E. Coordinate logging events with other networking devices within the organization.

Yes. Cisco Unified Wireless Network components can integrate with Cisco Security MARS, which aggregates logging events and alerts from other devices such as firewalls, wired IPSs, SNMP, NetFlow, and syslogs. Wireless LAN Controllers can send traps to multiple receivers. All wireless events may be forwarded from the WCS to any third-party event management system via SNMP. (This feature will be available in 1H10CY.)

F. Add processes and policies that will regularly read and act on the data provided by the IDS/IPS.

N/A. The Cisco WCS Management Console provides reports so that administrators can act on the data provided by Cisco Adaptive WIPS. However, it is up to the administrator to read and act on this data.

G. Maintain a current topology of all physical locations of access points.

Yes. The Cisco WCS provides a mapping tool that allows administrators to place the physical locations of the access points throughout the organization in order to map the current topology.

2.4 Strong Wireless Authentication and Encryption

PCI DSS v1.2 requires discontinuing WEP as of June 30, 2010 and moving to robust encryption and authentication such as the IEEE 802.11i standard. The Wi-Fi Alliance certifies products as WPA or WPA2 compatible for interoperability based on the 802.11i standard.

Table 7. PCI DSS 4.1.1

PCI DSS Requirement 4.1.1	Testing Procedure
<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. 	<p>For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.</p>

2.4.1 Summary of Recommendations

A. WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.

Yes. The Cisco Unified Wireless Network supports WPA and WPA2 with 802.1x authentication and AES encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

B. It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.

Yes. The Cisco Unified Wireless Network supports WPA2 Personal mode with a minimum 13-character random passphrase and AES encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

C. Pre-shared keys should be changed on a regular basis.

Cisco supports WPA-PSK and WPA2-PSK, which use pre-shared keys. Administrators will have to rotate these keys on both the infrastructure and associated devices. Thus, WPA or WPA2 Enterprise mode with 802.1x is recommended by Cisco. WCS can manage pre-shared keys on the infrastructure.

D. Centralized management systems that can control and configure distributed wireless networks are recommended.

Yes. The Cisco Unified Wireless Network is built upon centralized configuration and controller-based wireless networking with WLAN controllers, centralized WCS management, and centralized Adaptive WIPS and Context-Aware location services on the Mobility Services Engine.

E. The use of WEP in the CDE is prohibited for all deployments after June 30, 2010.

Yes. Cisco can configure, per SSID, what protocols are allowed/not allowed; provide vulnerability scanning reports to alert when WEP is in use; and highlight additional wireless security vulnerabilities that may exist in the CDE.

2.5 Use of Strong Cryptography on Transmission of Cardholder Data over Wireless

In addition to encrypting and authenticating wireless LANs using WPA2, when using wireless as a transport medium in a CDE, it is a security best practice to treat the wireless network as part of a DMZ or a public network. This means all CDE data must be encrypted as suggested in PCI DSS Requirement 4.1. Section 4.4 described Layer 2 specific wireless encryption protocols such as AES that is used within WPA2 to provide confidentiality and integrity at the wireless link layer. Higher layer encryption methods such as SSL/TLS and IPSEC and could be used to provide end-to-end cryptographic protection of card-holder data.

Table 8. PCI DSS 4.1

PCI DSS Requirement 4.1	Testing Procedure
<p>Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p>Examples of open, public networks that are in scope of the PCI DSS are:</p> <ul style="list-style-type: none"> • The Internet, • Wireless technologies, • Global System for Mobile communications (GSM), and • General Packet 	<p>Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks</p> <ul style="list-style-type: none"> • Verify that strong encryption is used during data transmission • For SSL implementations: <ul style="list-style-type: none"> ◦ Verify that the server supports the latest patched versions. ◦ Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). ◦ Verify that no cardholder data is required when HTTPS does not appear in the URL. • 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.

2.5.1 Summary of Recommendations

A. SSLv3 is mandatory for traffic that carries cardholder data.

Yes. The Cisco Unified Wireless Network defaults to the highest CipherSuite available on the network. Furthermore, fallback on less secure SSL versions (i.e., SSLv2 and SSLv1) can also be disabled, thus always forcing use of SSLv3.

B. When possible, 256-bit encryption is preferred.

Yes. The Cisco Unified Wireless Network provides 256-bit encryption and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

2.6 Development and Enforcement of Wireless Usage Policies

The PCI DSS mandates the need for acceptable usage policies and procedures, which include those for wireless devices. The importance here is that organizations understand how wireless is to be used within their environment, how it is to be secured and deployed, and how the organization will address incidents as they occur.

Table 9. PCI DSS 12.3

PCI DSS Requirement 12.3	Testing Procedure
<p>Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage, and Internet usage) to define proper use of these technologies for all employees and contractors.</p>	<p>Obtain and examine the policy for critical employee-facing technologies.</p>

2.6.1 Summary of Recommendations

A. Verify that the usage policies require explicit management approval to use wireless networks in the CDE. Any unsanctioned wireless must be removed from the CDE.

Yes. The Cisco Unified Wireless Network, with 802.1x support on the wireless side, can remove unsanctioned wireless devices from the CDE, or prevent them from accessing the CDE. If enforcing a “no wireless” environment, Adaptive WPS can be used to identify any wireless clients or access points in use and create alerts.

B. Verify that the usage policies require that wireless access is authenticated with user ID and password or other authentication item (for example, token). WPA Enterprise supports this requirement. If PSKs are used, then they must be rotated whenever employees that have access to wireless devices leave the organization. In Enterprise mode, individual user access can be enabled/disabled centrally.

Yes. Cisco can centrally enable/disable individual user access on the wireless network and enforce specific authentication and encryption policies on a per-WLAN/SSID basis. Furthermore, the WCS features automated vulnerability scanning to identify WLANs using suboptimal encryption/authentication configurations.

C. Verify that the usage policies require a list of all wireless devices and personnel authorized to use the devices.

Yes. The Cisco Unified Wireless Network uses the WCS to provide a list of all wireless devices and the personnel authorized to use those devices.

D. Verify that the usage policies require labeling of wireless devices with owner, contact information and purpose.

N/A. This is outside the technology requirements.

E. Verify that the usage policies require acceptable uses for the wireless technology. For example, if wireless devices are being used to transmit card holder data, then the same networks should not be used for guest access.

N/A. This is outside the technology requirements. However, Cisco firewalls and wireless VLANs can prevent networks from allowing cardholder data transmission, guest access, or other non-cardholder data traffic on the same network.

F. Verify that the usage policies require a list of company-approved products. For example, if a wireless AP needs to be replaced, substituting it with a non-sanctioned AP is not acceptable.

Yes. The Cisco Unified Wireless Network can only run with Cisco wireless access points; third-party access points are not supported.

G. Verify that the usage policies require automatic disconnect of sessions for wireless access after a specific period of inactivity. For example, a wireless POS terminal should automatically log out and disconnect from the CDE if left unattended.

No. Cisco does not enforce wireless automatic disconnect on the access points. This recommendation focuses more on client/POS devices, which Cisco does not manufacture.

H. Verify that the usage policies require activation of wireless-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.

Yes. Cisco provides this function via guest access capabilities built into the Unified Wireless Network, although not in the cardholder data environment.

I. Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via wireless access technologies. For example, if a wireless POS is being used, card holder data should not be stored locally on the device; it should only be encrypted and transmitted.

N/A. This recommendation refers more to wireless end devices, such as POS terminals and servers. This does not apply to the wireless access points.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CQVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)