PCI Wireless Guideline Checklist

Quick Reference Guide

Wireless networking is a concern for all organizations that store, process, or transmit cardholder data and therefore must adhere to the Payment Card Industry Data Security Standard (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.

Table 1 summarizes the Cisco® products that help organizations meet PCI DSS requirements.

PCI Wireless Requirement	Recommendations	Does Cisco Meet?	Cisco Product	Alignment	Security Beyond PCI: Optional Add-on
Maintain hardware inventory (Section 3.1, PCI DSS 9.9.1)	Scan all CDE locations for known WLAN devices and maintain up-to-date inventory in order to recognize rogue devices	☑ Yes	Cisco Wireless Control System (WCS)	Cisco WCS maintains a list of all wireless infrastructure components. It also incorporates a configuration audit capability to help ensure that devices are kept within policy.	
Scan for rogue access points (Section 3.2, PCI DSS 11.1)	Perform scans at least quarterly to prevent attacks from rogue devices that could negatively impact the CD. Wireless intrusion prevention system/intrusion detection systems (wIPS/wIDS) are acceptable for analysis and prevention. Relying on wired-network scanning tools is not recommended because these tools are error-prine and tedious to use.	☑ Yes	Cisco access points, Cisco Wireless Control System (WLC), Cisco WCS	Cisco's WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices. *Threats to network security can occur in between quarterly scans, creating the need to continuously scan and to use automatic alerts and containment mechanisms. Similarly, physical and/or port scanning on the wired network is not enough. Cisco Wireless LAN Controllers include wIPS and wIDS that find and stop rogue devices and attacks. WCS is a single point of management for WLAN devices, the mobility services engine, and mobility services.	Cisco context-aware location services in the Cisco 3300 Series Mobility Services Engine (MSE) can locate multiple rogue devices. Cisco enhanced local mode (ELM) access points offer monitor mode wIPS on local mode access points for additional protection without a separate overlay network. Cisco CleanAir technology allows the detection and location of rogue devices on nonstandard Wi-Fi channels.
Eliminate unauthorized wireless devices (Section 3.2, PCI DSS 12.9)	It is important to enable automatic alerts and containment mechanisms and create an incident- response plan to physically eliminate devices that may compromise network security.	☑ Yes	Cisco access points, WLC, WCS	Rogue devices are both detected and contained using the WLC. WCS generates an alarm when rogue access points are detected and can track a rogue down via switchport tracing. Automatic alerts take the burden off personnel so that they don't need to manually assess each device on the network and determine whether or not rogues are present.	With MSE, adaptive wireless IPS software service detects and contains unauthorized or rogue wireless devices. By identifying the physical location of rogue devices, administrators can eliminate these devices.
Segment the wireless network from other network traffic (Section 3.3, PCI DSS 1.2.3)	Any wireless network that does not store, process, or transmit card holder data must use a firewall so that it is completely isolated from the CDE. Wireless networking traffic should be separated by filtering wireless packets based on 802.11 protocol. Relying on virtual- LAN-based segmentation alone is not sufficient.	☑ Yes	Cisco ASA 5500 Series Adaptive Security Appliance or Cisco IOS® Firewall (Cisco Integrated Services Router (ISR) security image)	Cisco recommends Cisco firewalls (ASA 5500 Series Adaptive Security Appliances or Cisco Integrated Services Routers) to provide stateful functionality to segment the CDE. In most organizations, a single firewall can separate CDE for wired and wireless networks. The firewall integrates multiple, full-featured, high-performance security services, including WAN/LAN interface abilities, application-aware firewall, Secure Sockets Layer (SSL) and IPsec VPN, IPS, antivirus, antispam, antiphishing, and web filtering services.	
Maintain the physical security of wireless devices (Section 4.1, PCI DSS 9.1.3)	Restrict physical access to wireless access points, gateways, and handheld devices. Mount access points out of reach, and disable console-interface and factory-reset options with a tamper-proof chassis. Avoid pre-shared keys (PSKs) and printed passwords. Monitor to track and report on missing devices.	☑ Yes	Cisco access points, WLC, WCS	Cisco access points are easily mounted to ceilings and walls and are plenum rated, with an option to place the access point in the ceiling. Cisco mounting brackets block physical access to the reset button, Ethernet, and console ports. WCS simplifies the process of determining access point placement and access point coverage areas. WCS can enforce security via a username and password. If a Cisco access point is reset, the access point looks to the WLAN controller for configuration settings, rather than resetting to factory defaults. All access points have a Kensington Secure Lock.	Cisco context-aware location services in the MSE track and locate wireless devices and will report if any are missing.

PCI Wireless Guideline Checklist

Quick Reference Guide

PCI Wireless Requirement	Recommendations	Does Cisco Meet?	Cisco Product	Alignment	Security Beyond PCI: Optional Add-on
Change default settings (Section 4.2, PCI DSS 2.1.1)	When a wireless environment is connected to the CDE, an organization must change default settings, including (but not limited to) encryption keys, passwords, and SNMP community strings.	☑ Yes	WCS	Cisco Unified Wireless Network supports both Wi-Fi Protected Access (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. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.	
Provide intrusion detection and prevention (Section 4.3, PCI DSS 11.4)	Alert personnel to suspected compromises by keeping all intrusion detection/prevention devices up to date. Use centrally controlled wireless IDS/IPS to look for malicious activity and attacks and to disable rogues. Enable historical logging of wireless access to provide granular information for at least 90 days.	☑ Yes	WLC, WCS	Cisco Wireless Controllers have built-in IDS and IPS that analyze wireless traffic to look for and alert personnel to malicious activities and attacks. Historical data is kept on WCS for up to one year. 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. 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. It is the responsibility of the personnel to review the logs and firewall rules.	Adaptive wIPS events and forensics can be stored for many years on Cisco MSE. WCS with MSE can display location of rogue access points so that they can be physically eliminated if necessary.
Provide strong wireless authentication and encryption (Section 4.4, PCI DSS 4.1.1)	Use industry best practices to implement encryption for authentication and transmission (Wired Equivalent Privacy [WEP] is prohibited.) Centralized management of WPA or WPA2 with 802.1X authentication and AES encryption advised to control and configure distributed wireless networks. Change pre-shared keys (PSKs) regularly and use minimum of 13 character random passphrase and AES encryption.	☑ Yes	Cisco access points, WLC, WCS	Cisco supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. Cisco does not advertise the organization's name in the Service Set ID (SSID) broadcast. Cisco also disables SSID broadcast by default for nonguest networks. Cisco supports WPA2 Personal mode with a minimum 13-character random pass-phrase and Advanced Encryption Standard (AES) encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.	
Strong cryptology on wireless CD transmission (Section 4.5, PCI DSS 4.1)	Strong cryptology and security protocols are necessary to safeguard cardholder data during transmission over networks like the Internet, wireless technologies, GSM for Mobile, and General Packet Radio Service. SSLv3 is mandatory for traffic that carries CD and when possible, 256-bit encryption is preferred.	☑ Yes	Cisco access points, WLC	Offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links. 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. 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.	
Develop organizational usage policies (section 5, PCI DSS 12.3)	It is essential to have usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email usage, and Internet usage) to define proper use of these technologies for all employees and contractors.	☑ Yes	Cisco access points, WLC, WCS	WCS reports detailed inventory information for all access points, controllers, autonomous access points, and location servers in the Cisco Unified Wireless Network via an inventory report, and Role Based Access Control (RBAC) can show who has access to these devices. Cisco firewalls and wireless VLANs can prevent networks from allowing cardholder data transmission, guest access, or other noncardholder data traffic on the same network. Usage policies require activation of wireless-access technologies used by vendors only when needed by vendors, with immediate deactivation after use. Cisco provides this function via secured guest access capabilities built into the Cisco Unified Wireless Network.	