Quick Guide to Meeting PCI Wireless Requirements

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (WLAN) is part of, or connected to the cardholder data environment, the PCI DSS requirements and testing procedures for wireless environments apply and must be performed.

This guide boils down for you the key PCI requirements that need to be met, based on the use of wireless technology in PCI environments.

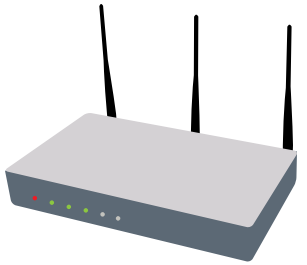
Quick PCI Overview

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.

Examples of system components include but are not limited to: firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

When wireless networks are part of the cardholder data environment

Requirement 1: Install and maintain a firewall configuration to protect cardholder data



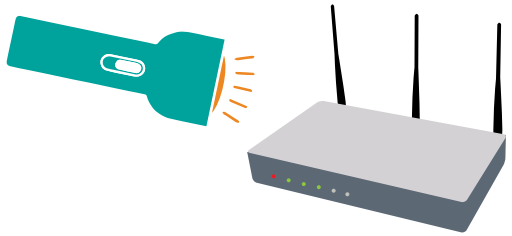
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

When wireless networks are NOT part of the cardholder data environment

Requirement 1: Install and maintain a firewall configuration to protect cardholder data



All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources.

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

General requirements regardless of location or network types

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines.

10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.)
- Wireless devices attached to a network port or network device.

11.1.c If wireless scanning is utilized, examine output from recent wireless scans to verify that:

- Authorized and unauthorized wireless access points are identified, and
- The scan is performed at least quarterly for all system components and facilities.

Continued on next page...

...General requirements continued:

11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.

11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.

12.3 Develop usage policies for critical technologies and define proper use of these technologies.
Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts. (e.g. detection of unauthorized wireless access points)

The Pwnie Express Pulse platform provides an easy-to-use platform that addresses these key PCI Security requirements across remotes sites and HQ.

"Pulse is the only solution that meets our needs. I looked at the leading Network Access Control (NAC) and WIPS/WIDS solutions, and they couldn't touch Pwnie Express when it comes to monitoring and securing our PCI wireless network and the devices that connect to it."

– One Hospitality Group Director of IT Mark Abbott

www.pwnieexpress.com

PWNIE EXPRESS