



What Is PCI DSS Compliance?

According to the American Bankers Association, it is estimated that there are 10,000 payment card transactions made every second around the world. With this kind of transaction volume and with cyber criminals constantly finding new ways to acquire sensitive cardholder data, payment card security breaches are a growing concern for many organizations. In order to protect cardholder data, the Payment Card Industry (PCI) Security Standards Council (SSC) created the Data Security Standard (DSS). PCI DSS compliance is required by all major credit card brands for any organization that processes payment cards or transfers and stores payment card data.

As organizations take advantage of wireless technology to improve operations and gain a competitive advantage, PCI DSS requires organizations to extend the same level of security from the wired network to the wireless network and provides specific guidelines as to how to protect point-of-sale data over the wireless network.

What Is Required to Achieve PCI DSS Compliance?

If you transmit point-of-sale data over the wired or wireless network, you will need to meet the requirements outlined in Table 1 to achieve PCI DSS compliance.

Table 1. PCI DSS Compliance Requirements

Req #	Requirement	Description
1	Establish firewall and router configuration Standards	Segment with a firewall between the wired and wireless network
2	Do not use vendor-supplied defaults	Provide the ability to change default passwords and settings and disable wireless transmission if connected via wired port
4	Encrypt transmission of cardholder data	Wi-Fi Protected Access (WPA) encryption. Wired Equivalent Privacy (WEP) is not acceptable when transmitting cardholder data.
5/6	Update virus software and maintain secure policies	Wireless Network Admission Control (NAC) for anti-virus and security patch enforcement
7/8	Restrict access to data and assign unique IDs	Authenticate wireless users and perform posture and profile assessment
9	Restrict physical access to cardholder data	Ensure wireless access point is hard to reach physically
10	Track and monitor access to cardholder data	Monitor wireless network and send events to monitoring and logging device
11	Regularly test security systems and policies	Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis
12	Maintain a security policy for employees	Ensure wireless network use is included in information security policy and centrally provision wireless devices for consistent, simple compliance reporting

Why Care About PCI Compliance?

Organizations that are not PCI-compliant risk more than just the significant fines imposed by credit card companies based on audits as a result of verified security breaches. According to the PCI Compliance Guide published by the PCI SSC, other ramifications that impact profitability across organizations of all sizes and market segments include:

- Card replacement costs
- Customer fear leading to a damaged brand and lost sales
- Expensive forensic audits
- Lawsuits and liability claim compensation

How to Secure the Wireless Network?

In addition to protecting the wireless transfer of cardholder information, but organizations must also secure and control physical access to the medium itself. In a supplemental document called PCI DSS Wireless Guidelines, the PCI SSC has outlined five areas that must be addressed to meet wireless requirements. Table 2 summarizes these requirements.

Table 2. PCI DSS Wireless Security Requirements

Guideline	Benefit
Maintain a hardware inventory	Quickly distinguish between authorized and rogue access points (APs)
Wireless scanning to look for rogue APs	Detect unauthorized/rogue wireless devices that could connect to the cardholder data environment (CDE)
Segment wireless networks	Block wireless traffic from entering the CDE
Physical security on wireless devices	Prevent access to ports and reset features to minimize potential "backdoor" access to cardholder data
Change default setting of the APs	Minimize the chance of unauthorized access by establish unique settings
Wireless intrusion prevention and access logging	Monitor and contain unauthorized access and detect rogue and misconfigured wireless devices
Strong wireless authentication and encryption	Leverage WPA or WPA2, 802.1x and Advanced Encryption Standard (AES) to assure only authorized devices and users can access the wireless network
Use a strong cryptography on transmission of cardholder data over wireless	Use encryption to protect cardholder data as it is transmitted through the wireless network.
Development and enforcement of wireless usage policies	Assures that internal personnel understand and abide by best practices when interacting with the wireless network.



Why Cisco Wireless?

Cisco provides a comprehensive wired and wireless solution, enabling complete end-to-end PCI DSS compliance. Specifically for wireless, Cisco provides best-in-class solutions to meet PCI DSS compliance, and also provides incremental solutions that extend security beyond PCI DSS compliance to meet the objective of truly securing cardholder data.

In addition to developing technology and solutions for achieving PCI DSS compliance, Cisco has dedicated resources to truly understand the nature of PCI DSS compliance and to provide valuable insight into PCI updates and revisions. Dedicated Cisco® personnel actively participate as members of the Worldwide PCI Council Board of Advisors in order to represent Cisco's expertise in network security, and represent our customers concerns with regard to PCI compliance.

Additionally, Cisco works with third-party quality security assessors (QSA) to help ensure that the Cisco recommended designs meet and/or exceed PCI DSS requirements. This process allows Cisco customers to deploy the recommended solution architectures with the utmost confidence that they will achieve PCI DSS compliance.

Because Cisco solutions use an architectural approach, you can reap benefits not found in single-box approach. These benefits include:

1. **Lower total cost of ownership (TCO):** The same Cisco solution that provides PCI compliance is also the solution that provides rich mobility solutions. Because Cisco uses an architectural approach, when you want to move from a wired-only to wired and wireless operational model, you can do so simply by adding a few new components to your existing PCI solution. Because there is no need to design and implement a new solution, the investment you make today will continue to add value as the business model changes and adapts.
2. **True investment protection:** PCI compliance is updated on a three-year cycle, and new requirements are added or adjusted based on each cycle. Because Cisco uses an architectural approach, you can be confident that when new standards are released, you can easily and cost-effectively maintain compliance by upgrading or updating only the solutions components impacted by new standards.
3. **Seamless wired and wireless integration:** Cisco has partnered with third-party PCI experts to help design and validate end-to-end solutions deployed across wired and wireless infrastructure to achieve PCI compliance. In contrast to wireless-only solutions that are not tested in parallel with the wired infrastructure, Cisco solutions deliver seamlessly across the network to better protect cardholder data. As an important additional benefit, you have a single support model that minimizes the need to manage multiple vendors.

Should You Think Beyond PCI Compliance?

The answer is Yes. The potential profitability of cardholder data is so great that cyber criminals continually look for new ways to acquire confidential data. Because the PCI DSS standard is updated every three years, it does not necessarily protect organizations from all potential threats. This is evident from the PCI SSC's own recommendation that merchants scan quarterly to test security systems and policies.

In addition, it's important to recognize that security threats are usually not long-term, ongoing activities, but short acquisitions of data that can easily be disguised from quarterly scans. To combat this, organizations have adopted continuous wireless intrusion prevention scanning that provides a better line of defense. To meet PCI Compliance the implementation of Cisco Access Points, Controllers and the Cisco Wireless Control System is required for wireless scanning. The addition of a firewall and Cisco Security Manager enables wireless scanning and access. However, to increase security on the wireless network, other innovative Cisco technologies have been cost-effectively added to PCI DSS solutions. These include the enhanced local mode (ELM) access points, adaptive wireless intrusion prevention system (wIPS), and Cisco CleanAir technology.

Enhanced Local Mode Access Points

ELM allows the access points to continuously scan for rogue access while providing wireless network access while at the same time adding advanced signature detection. ELM uses Cisco adaptive wIPS and the Mobility Service Engine (MSE) to recognize security threats that can avoid detection through wireless scanning or physical inspection.

Adaptive Wireless Intrusion Protection System

Adaptive wIPS employs consistent scanning with network analysis and signature-based techniques to deliver protection against rogue access points as well as many other threats. Adaptive wIPS can be implemented using access points in enhanced local mode or in access points dedicated to on-channel and off-channel scanning.

Cisco CleanAir Technology

Cisco CleanAir Technology identifies all RF interference within the wireless network, including access points running on nonstandard channels, non-Wi-Fi access points using Bluetooth or older standards, and RF layer denial-of-service (DoS) attacks that can impact wireless network security.

Learn more by visiting:

<http://www.cisco.com/go/wireless>

<http://www.cisco.com/go/wireless/securewireless>