



# PCI v1.2 Compliance for the Wireless LAN

---

---

**June 2010**

This white paper describes the PCI v1.2 requirements as they relate to wireless LANs and how Meraki can be used to build a PCI-compliant wireless network.

### **Copyright**

© 2010 Meraki, Inc. All rights reserved.

### **Trademarks**

Meraki® is a registered trademark of Meraki, Inc.



[www.meraki.com](http://www.meraki.com)

660 Alabama St.  
San Francisco, California 94110

Phone: +1 415 632 5800

Fax: +1 415 632 5899

---

## 1. The PCI Standard

The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through enhanced security measures. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

The first version of the standard, PCI DSS v1.0, went into effect in January 2005. On January 1, 2007, PCI DSS v1.1 was put in place, replacing PCI DSS v1.0 and the VISA CISP standard. PCI DSS v1.1 reflected changes in the security landscape and offered alternatives in the form of merchant “compensating controls” to make compliance more practical.

On October 1, 2008, the PCI SSC released PCI DSS v1.2. The new standard supersedes v1.1 starting January 1, 2009, and all new audits conducted after this date must adhere to the PCI DSS v1.2 specification. PCI DSS v1.2 clarifies v1.1 requirements that were previously open to interpretation. The new standard also updates requirements based on what the industry has learned about security breaches in the intervening years since v1.1 was issued.

## 2. PCI Requirements for Wireless Networks

The PCI Security Standards Council has done a good job of summarizing the PCI requirements as they relate to wireless networks (see [1], for example). The following table lists those requirements and, where applicable, describes how a Meraki system helps build a PCI compliant wireless network.

PCI Requirement	Meraki Meets	How Meraki Helps
<b>1.1.2</b> Current network diagram with all connections to cardholder data, including any wireless networks.	✓	Meraki's hosted Dashboard service has intuitive mapping and diagramming tools that can assist in creating appropriate maps.
<b>1.2.1</b> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	✓	Meraki's built-in NAT and firewall features including Identity Policy Manager can be used to restrict either inbound or outbound traffic from the wireless network
<b>1.2.3</b> 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.	✓	Meraki's built-in firewall and Identity Policy Manager can be used to effectively deny or control any wireless traffic into the local LAN or the Internet
<b>2.1.1</b> 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.	✓	Meraki supports the latest strong security standards and makes it easy to ensure they are setup correctly. Also, Meraki does not ship with default keys that need to be changed.

<p><b>4.1.1</b> 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>	✓	<p>Meraki supports the strongest encryption standards, including WPA-PSK, WPA-Enterprise, WPA2-PSK, and WPA2-Enterprise (802.11i) with AES encryption.</p>
<p><b>9.1.3</b> Restrict physical access to wireless access points, gateways, and handheld devices.</p>	✓	<p>Meraki enterprise access points feature have 3 different physical security mechanisms, including padlock and security screw, that restrict physical access. Meraki APs can also be placed in the plenum to make them more secure.</p>
<p><b>10.5.4</b> Write logs for external-facing technologies onto a log server on the internal LAN...verify that logs for external-facing technologies are offloaded or copied onto a secure centralized internal log server media.</p>	✓	<p>Meraki network logs are automatically stored in a centralized environment and backed up in geographically redundant data centers.</p>
<p><b>11.1</b> 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.</p>	✓	<p>Meraki includes IDS, also known as rogue AP detection, which reduces the need for manual scans.</p>
<p><b>12.3</b> Develop usage policies for critical employee-facing technologies (for example, remote – access technologies, wireless technologies...) to define proper use of these technologies for all employees and contractors.</p>	✓	<p>Implementer’s responsibility</p>
<p><b>12.9.3</b> Designate specific personnel to be available on a 24/7 basis to respond to alerts.</p>	✓	<p>Meraki systems provide 24 hour automated security alerts to assist in incident identification.</p>
<p><b>12.9.5</b> Include alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems.</p>	✓	<p>Meraki’s wireless intrusion detection system generates automatic alerts to warn of potential security threats.</p>

Additional detail on the PCI requirements can be found in [2].

---

### 3. Network Segmentation (VLANs) and PCI Compliance

PCI audits can be expensive and time-consuming, especially when the audit scope includes your entire network infrastructure. PCI DSS security requirements apply to all system components, where “system components” are defined as “any network component, server, or application that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access point, network appliances, and other security appliances. In other words, anything that sensitive cardholder data “touches” is subject to compliance requirements and auditing.

One way that the scope of a PCI audit can be reduced is through network segmentation. Network segmentation, or isolation of the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a means of reducing the scope and cost of a PCI DSS assessment as well as a means of reducing general risk to the organization.

One way to segment your network is by using virtual LANs , or VLANs. If your wireless network is not being used to transmit or store sensitive cardholder data, then the use of VLANs on your network can effectively segment the wireless network from the cardholder data environment and potentially remove it from the scope of a PCI audit. Meraki supports VLAN tagging to enable effective use of VLAN segmentation across your wired and wireless infrastructure.

If the wireless network is being used to transmit or store cardholder data, then the use of VLANs will not remove the wireless network from the audit scope. However, using VLANs to separate guest and other types of insecure traffic from sensitive cardholder data traffic is still a recommended best practice, and can be done with Meraki wireless networks. Each SSID can be mapped to a unique VLAN to effectively segment sensitive traffic from other types of traffic.

---

## 4. Summary

The PCI DSS v1.2 standard describes clear requirements for building compliant wireless LANs.

Meraki's secure wireless solutions offer a simple, cost-effective means of achieving PCI compliance. Meraki's integrated mapping, logging, and rogue AP detection tools eliminate the need to build a solution from component parts. In addition, centralized control of geographically distributed networks makes it easy to implement the same PCI-compliant architecture across large numbers of retail locations.

You can learn more about Meraki solutions for retail at <http://www.meraki.com>.

---

## 5. References

- [1] PCI DSS v1.2 Wireless Guideline,  
[https://www.pcisecuritystandards.org/pdfs/PCI\\_DSS\\_Wireless\\_Guidelines.pdf](https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf)
- [2] PCI DSS v1.2,  
[https://www.pcisecuritystandards.org/pdfs/pr\\_080930\\_PCIDSSv1-2.pdf](https://www.pcisecuritystandards.org/pdfs/pr_080930_PCIDSSv1-2.pdf)