PCI Compliance

All organizations that accept credit or debit cards for customer purchases must proactively protect sensitive customer account data. The PCI Security Standards Council Data Security Standard (PCI DSS) is designed to mitigate the security risks for payment accounts. DSS is a multi-faceted security strategy that includes requirements for security management, policies, procedures, network architecture, and software design. From a wireless LAN perspective, retailers and other enterprises subject to PCI DSS must protect their networks from attacks from unauthorized wireless access points and clients – even if they don't have a wireless LAN implemented themselves. Failure to comply with the PCI DSS standard could result in expensive fines – not to mention significant reputation damage from a well-publicized security breach.

Aruba's secure mobility solutions offer a cost-effective means of achieving PCI compliance. By providing an integrated solution, and eliminating the need to purchase and integrate multiple disparate network technologies, Aruba simplifies the task of securing a wireless network. Aruba also offers a range of solutions intended to fit varying needs for security controls on existing or legacy wireless networks, preventing the need for a wholesale upgrade.
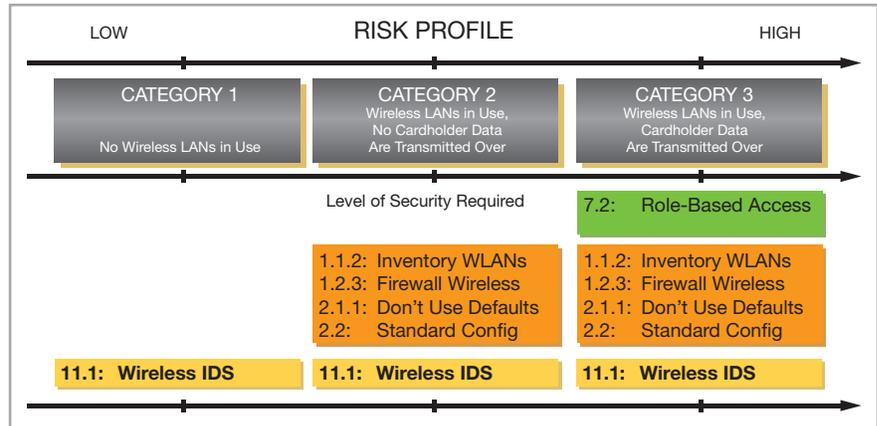
- **Significant capital and operational cost savings:** Built-in security capabilities address every wireless LAN-specific PCI requirement (and many wired LAN requirements).

- **Easy to integrate:** Fits on top of your existing networks and thereby eliminates the need to redesign or replace legacy network infrastructure. Aruba's solutions extend the same high security paradigm to remote locations and stores, providing one common model for the entire enterprise.

- **Protects existing investments:** Securely segments legacy WEP-only devices to move them outside the scope of PCI compliance, thereby avoiding costly device upgrades.

Aruba Benefits

- Low TCO with built-in security for PCI compliance

- Protect legacy wired and wireless networks with an overlay architecture

- Prevent security breaches in WEP-only networks by using identity-based security

- Easy migration to next-gen wireless LANs with multi-purpose platform

- Designed to scale for large number of remote retail stores

PCI Requirements for Securing Wireless LANs

PCI DSS includes 12 major steps for securing payment account information along with testing methodologies to ensure that these requirements are met. Wireless LAN security is a core component of these requirements. The PCI requirements specific to wireless LANs have been sorted into three levels of implementation in the illustration. Each category has a different risk profile, and a distinct level of mandatory security controls.

RISK PROFILE

LOW   HIGH

CATEGORY 1	CATEGORY 2	CATEGORY 3
No Wireless LANs in Use	Wireless LANs in Use, No Cardholder Data Are Transmitted Over	Wireless LANs in Use, Cardholder Data Are Transmitted Over

Level of Security Required

		7.2: Role-Based Access
	1.1.2: Inventory WLANs 1.2.3: Firewall Wireless 2.1.1: Don't Use Defaults 2.2: Standard Config	1.1.2: Inventory WLANs 1.2.3: Firewall Wireless 2.1.1: Don't Use Defaults 2.2: Standard Config
11.1: Wireless IDS	11.1: Wireless IDS	11.1: Wireless IDS

What Can Aruba Do?

Aruba Networks is a participating organization within the PCI Security Standards Council and supplies secure wireless LANs that are used by numerous leading merchants worldwide to comply with PCI standards and prevent network breaches. Aruba offers three levels of wireless LAN security to attain PCI compliance and beyond:

LEVEL 1: PCI MONITORING

The PCI monitoring option entails installing AirWave Wireless Management Suite™ from Aruba Networks. AirWave is designed to inventory, monitor and manage multi-vendor wireless networks, and represents the most cost-effective approach to addressing applications in which legacy wireless networks are already in place - no hardware or software is required at any remote location.

AirWave Wireless Management

- Server at HQ monitors all locations
- No dedicated sensor hardware required
- Monitors for and reports rogue APs

LEVEL 2: WIRELESS IDS

AirWave's PCI monitoring capabilities outlined in level 1 above are enhanced when used in conjunction with Wireless IDS (WIDS), while greater RF granularity is obtained by using dedicated sensors. By utilizing sensors in all remote locations, WIDS compares wired and wireless traffic, identifying and locating any rogue devices, attacks originating from outside the building, and most importantly, automatically blocks rogue devices and attacks.

Both the level 1 and level 2 solution options enables merchants to outfit existing networks without replacing or re-architecting existing wired and wireless networks.

AirWave Wireless Management

Aruba Mobility Controller

Sensor

- Server and controller at HQ
- Sensors in stores scan RF
- No change to existing LAN or WLAN
- Monitors for rogues, attacks & reports
- Prevents rogues & attacks

LEVEL 3: ARUBA WIRELESS LAN WITH IDS AND ROLE-BASED ACCESS CONTROL FOR LEGACY WEP DEVICES

The wireless LAN with IDS and role-based access control option integrates the functions of a centralized wireless LAN, built-in stateful firewall, built-in wireless IDS, and AirWave monitoring. Aruba Controllers in the data center and remote locations are managed centrally through the Airwave Management Platform, which aggregates all wireless network information and provides PCI compliance reports.

The integrated Aruba WLAN provides all of the security controls necessary to meet wireless LAN PCI requirements, offers security controls for some PCI wired LAN requirements, and includes security controls that go beyond PCI requirements to help prevent breaches. Competing solutions require 3x - 4x the amount of hardware and software to provide comparable functionality.

The level 3 solution is ideal for merchants that need to replace existing, legacy wireless LANs in order to comply with security, management and application requirements.

AirWave Wireless Management

Aruba Mobility Controller

Aruba Hybrid Access Points

- Server and controller at HQ
- Sensors become hybrid APs
- APs added as necessary for coverage
- Stateful firewall segmentation
- Monitors for rogues, reports on attacks
- Protects legacy (WEP-only) client devices