



The Payment Card Industry (PCI) Data Security Standard (DSS) is designed to help ensure the security of cardholder data and information—at the point of sale (POS), in transit, and at rest. The standards for achieving PCI compliance are somewhat broad, but all retailers are required to evaluate their current networks, policies, and processes. Cisco® has developed a set of architectures in a lab environment with PCI requirements in mind. Cisco invited PCI auditors to evaluate these architectures, and the auditors found that the technology, if properly deployed and maintained, could help retailers achieve PCI compliance.

### Cisco Recommended Architectures

The Cisco PCI Solution for Retail includes recommended network architectures and a portfolio of products that can be customized for your specific store footprints and application needs. These suggested network architectures and accompanying product information are contained in the Cisco PCI Solution for Retail Design Guide, available from your Cisco account team. Cisco also works with a wide range of vendors who can provide solutions for antivirus, POS software, wireless POS, scan, audit, remediation services, and best practices.

### PCI DSS Primary Requirements

The PCI DSS outlines 12 requirements that retailers must meet for achieving compliance. Cisco Intelligent Retail Networks use Cisco routing, switching, security, wireless, and management products to build integrated, collaborative, and adaptive solutions that can help a retailer address many of the 12 PCI requirements. Table 1 includes many elements that are used to create a Cisco PCI Solution for Retail.

Table 1: PCI Requirements Addressed by Cisco PCI Solution for Retail

Solution Feature	Solution Provides
<b>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</b>	
ISR Router	Network security (firewall segmentation/filtering), stateful filtering
CiscoWorks (LMS), CSM	Configuration management/secure configurations
<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</b>	
ISRs, switches, wireless devices, WCS, ACS, CiscoWorks (LMS), CSA, CSM	Vendor defaults changed
WCS/wireless controllers	Wireless security (WPA/WPA2, SSID broadcast disabled)
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks [LMS])	Best practice security parameters enabled
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Non-console encrypted administrative access
<b>Requirement 3: Protect stored cardholder data.</b>	
PCI consultants or Cisco partners can help you identify specific solutions for meeting this requirement	
<b>Requirement 4: Encrypt transmission of cardholder data across open, public networks.</b>	
Wireless controllers	WPA wireless security
<b>Requirement 5: Use and regularly update anti-virus software or programs.</b>	
CSA	Anti-virus protection, malware/spyware protection, alerting
<b>Requirement 6: Develop and maintain secure systems and applications.</b>	
CiscoWorks (LMS), CSM (Workflow mode)	Change control
<b>Requirement 7: Restrict access to cardholder data by business need-to-know.</b>	
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Least-privilege, role-based access



Table 1: PCI Requirements Satisfied by Cisco PCI Solution for Retail (continued)

Solution Feature	Solution Provides
<b>Requirement 8: Assign a unique ID to each person with computer access.</b>	
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Unique user IDs, authenticated access, encrypted passwords, no group/shared IDs/passwords
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS)	Password strength requirements
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS)	Account lockout requirements
<b>Requirement 9: Restrict physical access to cardholder data.</b>	
PCI consultants or Cisco partners can help you identify specific solutions for meeting this requirement	
<b>Requirement 10: Track and monitor all access to network resources and cardholder data.</b>	
ISRs, switches, wireless devices, WCS, ACS, CiscoWorks (LMS) CSA	Audit trails, time synchronization
<b>Requirement 11: Regularly test security systems and processes.</b>	
Wireless controllers	Rogue wireless AP/device detection
ISRs (sensor), CSM (policy, signature updates)	Network IDS
CSA	Host-based IDS
CSA	File integrity
<b>Requirement 12: Maintain a policy that addresses information security.</b>	
PCI consultants or Cisco partners can help you identify specific solutions for meeting this requirement	

For detailed notes on each solution feature and the audit findings, strengths, and weaknesses, see Chapter 3, “Solution Components—Cisco Products and PCI.” Specific implementation and configuration details are in Chapter 4, “Implementation and Configuring the Solution.” Finally, for a complete audit report by Cybertrust on this specific lab, see Appendix E, “Report on Compliance.”

### Key of Acronyms

- ISR – Integrated Services Routers
- CSM – Cisco Security Manager
- WCS – Wireless Control Server
- ACS – Access Control Server
- Cisco Works (LMS) – Cisco Works LAN Management Solution
- CSA – Cisco Security Agent
- CS-MARS – Cisco Secure Monitoring, Analysis and Remediation System
- WPA – Wi-Fi Protected Access
- IDS – Intrusion Detection System

### Learn More Today

Cisco retail solutions facilitate retailers’ ability to achieve their compliance goals. To learn how a Cisco PCI Solution for Retail can help meet your organization’s specific requirements, please contact your local Cisco account manager and request the **Cisco PCI Solution for Retail Design Guide**. The Design Guide provides you with more information about the wide range of Cisco products and services that can help you address PCI DSS requirements. For additional information about Cisco solutions for retail, please visit: [www.cisco.com/go/retail](http://www.cisco.com/go/retail).