Cisco PCI Wireless Security Compliance Supplemental Document: Catalyst 9800

Contents

Introduction

Every year, network attacks become more widespread, more intelligent, and more difficult to detect. Given the public nature of retailers, entry points into the network go beyond employee laptops, desktops, and smartphones to include public Wi-Fi and public-facing e-commerce servers. As a result, retail networks have two primary challenges. The first is dealing with the complexity of managing many remote locations. The second is being able to provide security protection that mirrors the same threats as those facing large enterprise networks.

Many of today's security incidents are blended attacks that use multiple techniques at different layers to try to infiltrate the network. These attacks can bypass outdated firewalls that lack the power to inspect all traffic, including large files and HTTPS encrypted traffic.

In businesses that accept credit card payments, maintaining compliance with PCI standards is essential. The Payment Card Industry Data Security Standard (PCI DSS) has six high-level goals, including building and maintaining a secure network, regularly monitoring and testing networks, and implementing strong access control measures. These goals drive specific requirements to ensure that credit card data, including cardholders' personal information, is protected and secured. Maintaining PCI compliance can help your business avoid costly penalties but should not be viewed as a complete network security solution. Rather, it is an important waypoint along your journey to make your network as secure as possible.

Cisco and PCI DSS compliance

Since 2007, Cisco and Verizon have partnered to offer PCI compliance guidance. The resulting Cisco® Compliance Solution for PCI was developed to implement guidance in specific Cisco laboratory configurations that undergo the Verizon Qualified Security Assessor (QSA) assessment. With the release of PCI DSS 3.0, 3.1, and 3.2, there are questions that Cisco customers naturally ask.

- What are the significant changes from version 2.0 to 3.2?
- How do they affect the existing Cisco Compliance Solution for PCI?

In this supplemental document you will learn:

- How PCI DSS 3.2 affects the scoping, vendor equipment assessment, and enterprise architecture of existing Cisco Compliance Solution for PCI implementations
- The significant changes between PCI DSS 2.0 and 3.2 pertaining to wireless deployments

Cisco Compliance Solution for PCI

The Cisco Compliance Solution for PCI provides enterprise guidance and component-level configurations:

- **Enterprise architecture:** The solution uses a reference architecture to validate compliance guidance. The reference architecture consists of branch offices of different sizes, WANs, data center, and internet edge technology. It details the security and respective compliance controls as credit card transactions occur at the branch location and flow throughout the enterprise, where they exit to the acquiring banks.

  Assessment: The architecture sections of the Cisco Compliance Solution for PCI are still valid. Nothing in the standard update has affected the guidance provided here.

- **Components:** The solution uses a standardized metric for evaluating a component's native ability to support PCI. This metric is known as the capability scorecard. It summarizes the relevant sections of the PCI DSS for an in-scope device.

  Assessment: The capability scorecards of the Cisco Compliance Solution for PCI are still valid. Nothing in the standard update has affected the guidance provided here.

General changes to the PCI DSS

One of the biggest areas of confusion continues to be the definition of the PCI scope. The PCI 3.0 to 3.2 standards include wording that clarifies PCI scoping and segmentation to include systems that:

- Provide security services (for example, authentication servers)
- Facilitate segmentation (for example, internal firewalls)
- Affect the security of the cardholder data environment (for example, name resolution and web redirection servers)

The standard also uses the term "isolation" for the first time, as part of the segmentation definition. The PCI 3.0 to 3.2 standards clarify "out-of-scope systems" to mean those systems that, if compromised, cannot affect the security of the cardholder data environment. Requirement 11.3 has wording that is designed to increase the testing of the cardholder data environment perimeter. It specifies that penetration testing is needed along the internal perimeter as well as along the external perimeter, to verify that there is no access to sensitive information.

Noteworthy 3.2 changes by requirement

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

Requirement 1.1.3: Broken out from the network diagram requirement; a new requirement specifically requires maintenance of a data flow diagram that shows all cardholder data flows across systems and networks (effective immediately).

Requirement 1.1.6: Simple Network Management Protocol (SNMP) versions 1 and 2 added to list of "insecure protocols" (effective immediately).

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security requirements.

Requirement 2.1: Clarifies that changing vendor defaults applies to all passwords, including system and application credentials, and that unnecessary default accounts are removed or disabled (effective immediately).

Requirements 2.2.2 and 2.2.3: Make system configuration standards more prescriptive and explicit by breaking out "necessary" services and "secure" services (effective immediately).

Requirement 2.4: New requirement to maintain current inventory of all PCI system components to develop configuration standards (effective immediately).

Requirement 3: Protect stored data. No major changes.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.

Requirement 4.1: Bluetooth, CDMA, and satellite communications added to examples of "open public networks" (effective immediately).

Requirement 4.1: Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (for example, internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure that wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission. (Where SSL/early TLS is used, the requirements in PCI DSS Appendix A2 must be completed.)

Secure Sockets Layer (SSL) and early Transport Layer Security (TLS) should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included:

- New implementations must not use SSL or early TLS as a security control.
- After June 30, 2018, all entities must have stopped use of SSL/early TLS as a security control and use only secure versions of the protocol (an allowance for certain point-of-sale [POS] and point-of-interaction [POI] terminals is described in the last bullet below).
- Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2018.

Requirement 5: Use and regularly update antivirus software.

Requirement 5.1.2: Calls for evaluation of evolving malware threats for systems not “commonly affected by malware.”

Requirement 6: Develop and maintain secure systems and applications.

Requirement 6.5.x: New requirement for coding practices to document the way that Primary Account Number (PAN) and Sensitive Authentication Data (SAD) is handled in memory (effective July 1, 2015).

Requirement 6.5.10: New requirement for coding practices to protect against broken authentication and session management (effective July 1, 2015).

Requirement 7: Restrict access to data by business need to know. No major changes.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 8.3: Clarifies that two-factor authentication applies to users, administrators, and all third parties, including vendor access for support and maintenance (effective immediately).

Requirement 8.5.1: Mandates that service providers must use different credentials to access different customer environments (effective July 1, 2015).

Requirement 8.6: Secure all individual nonconsole administrative access and all remote access to the cardholder data environment using multifactor authentication. This requires the use of at least two of the three authentication methods described in 8.2 for authentication. Using one factor twice (for example, using two separate passwords) is not considered multifactor authentication. This requirement applies to administrative personnel with nonconsole access to the cardholder data environment from within the entity's network, and to all remote network access (including for users, administrators, and third parties) originating from outside the entity's network. (Note: The requirement for multifactor authentication for nonconsole administrative access from within the entity's network is a best practice until January 31, 2018, after which it becomes a requirement.)

Requirement 9: Restrict physical access to cardholder data.

Requirement 9.3: New procedures to verify that physical access for terminated employees has been revoked (effective immediately).

Requirement 9.9.x: New requirement to protect POS devices that capture payment card data from tampering or unauthorized modification or substitution; requirement includes a list of devices, personnel training, device inspection, etc. (effective July 1, 2015).

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 10.2.x: Enhanced logging requirements, including use of and changes, additions, or deletions to administrative privileges, and stopping or pausing the audit logging system (effective immediately).

Requirement 10.6.2: Update or clarification stating that logs for all "noncritical" and "nonsecurity" assets must be reviewed "periodically" for malicious activity (effective immediately).

Requirement 11: Regularly test security systems and processes.

Requirement 11.1.1: New requirement for an inventory of all authorized wireless access points and accompanying business justification (effective immediately).

Requirement 11.2: Adds guidance that multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all vulnerabilities have been addressed (effective immediately).

Requirement 11.3: Increases specificity for pen test methodology, inclusion of testing segmentation controls, and requirement to retest to validate remediation (effective July 1, 2015).

Requirement 12: Maintain a policy that addresses information security.

Requirement 12.2.b: New requirement that risk assessments must be performed after significant changes to the environment (effective immediately).

Requirement 12.8.x: New requirement for maintaining a "responsibilities matrix" that details PCI requirements in scope for service providers (effective immediately).

Requirement 12.9: New requirement for service providers to acknowledge in writing to the customer that they will maintain all applicable PCI DSS requirements (effective July 1, 2015).

PCI DSS 3.2 wireless security requirements

Cisco wireless technologies provide connectivity for mobile clients within the branch. They can secure connectivity for traditional business functions, such as guest access or inventory control, without increasing risk. Innovative customer experience services such as mobile POS are equally secure. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues. Industry-leading performance is available with Cisco Aironet® and Cisco Catalyst® access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to specific business needs and topologies. Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations, and management. They extend the Cisco Software-Defined Access (SD-Access) network policy and security from the wired network to the wireless edge.

Primary PCI function

The primary PCI function of Cisco Unified Wireless is secure connectivity of wireless clients (4.1, 4.2) and rogue detection (1.1).

Design considerations

Rogue detection for wireless technology in the branch is required at a minimum of once per quarter, whether or not the organization has wireless deployed. A hacker might infiltrate a branch and install a rogue wireless device (for example, an access point, wireless-enabled printer, or radio-enabled USB stick). This would allow a hacker remote access into the branch (from the parking lot, for example) that is hard to detect. The PCI DSS offers several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic. The PCI DSS states that wireless technology is an untrusted network connection. Wireless technology in the branch requires firewall and intrusion detection services to segment and protect the cardholder data environment. Stateful firewalls must be configured to limit traffic to and from the wireless environment (all enabled services, protocols, and ports must have documented justification for business purposes). All other access must be denied. When including POS clients in the wireless network, strong wireless encryption technology needs to be implemented. Caution: Wireless clients must be protected from each other as well. For example, when using hand-held scanners and mobile POS, the scanners need to be on separate SSIDs and networks from the POS, and protected with firewall and intrusion detection services that are restricted to justified business access.

Cisco recommends using the Unified Wireless (controller-based) architecture for enterprise wireless deployments because of the Cisco ongoing wireless strategy. The autonomous Cisco IOS® access points are not being enhanced. Future security and user enhancements will be developed on the Unified and SD-Access controller-based architectures.

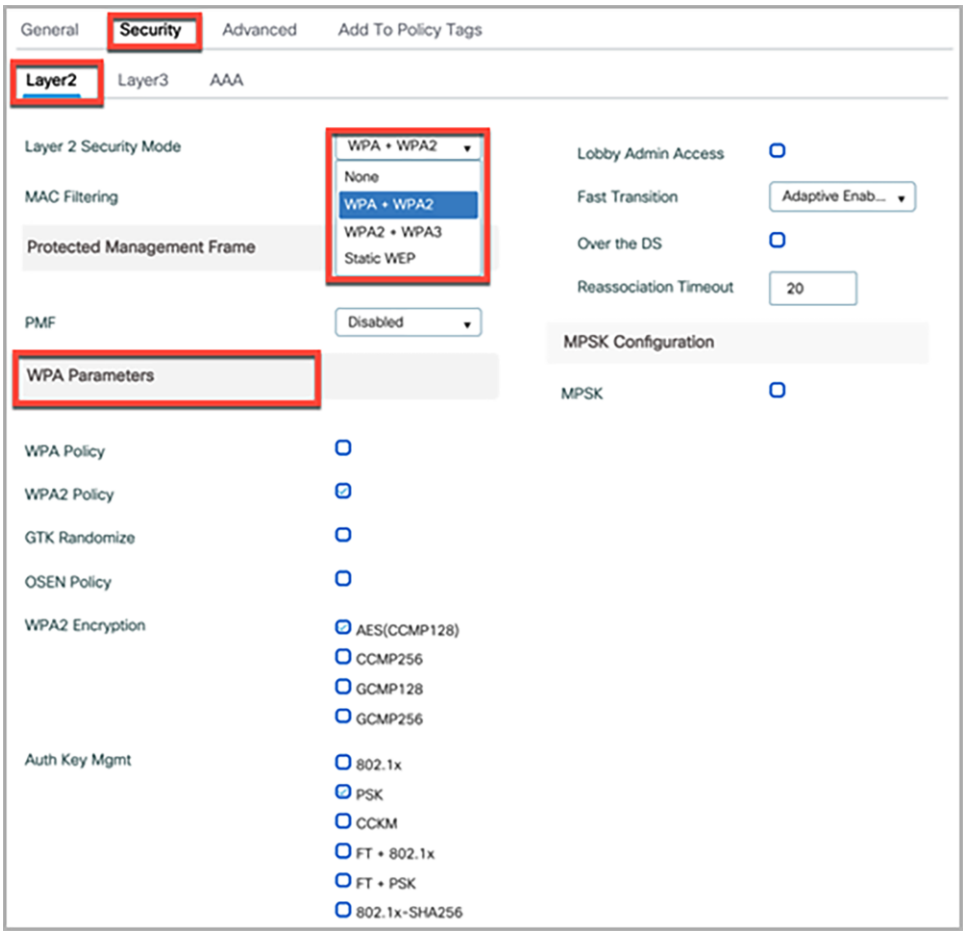
PCI assessment detail—PCI sub-requirements satisfied

Whenever possible, a screen shot highlighting the appropriate Cisco Wireless Control System functionality is provided.

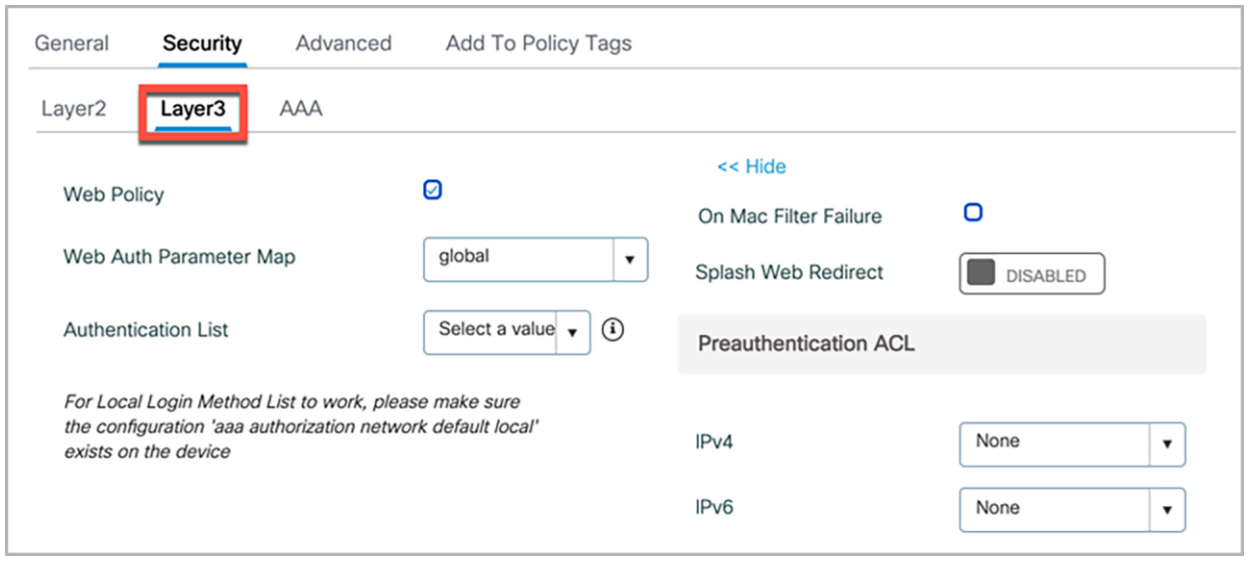
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- PCI 2.1.1: 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. The Cisco Unified Wireless Network supports both Wi-Fi Protected Access versions 2 (WPA2) and 3 (WPA3),* providing automated vulnerability scanning in the wireless controller to identify WLANs using suboptimal encryption. There is no default Pre-Shared Key (PSK), and all PSKs or Identity PSKs must be created during configuration. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

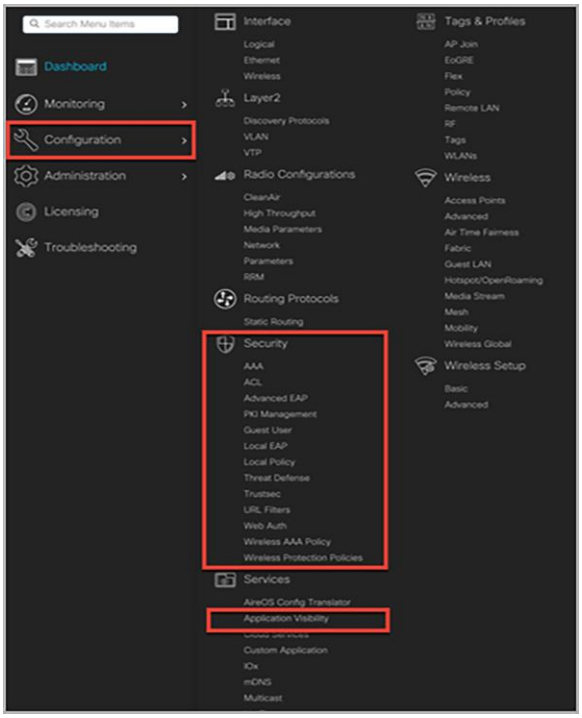
Below are screen shots of the WLAN security Layer2 and Layer3 configurations.



*Supported on 802.11ac Wave 2 access points and Catalyst 802.11ax access points.

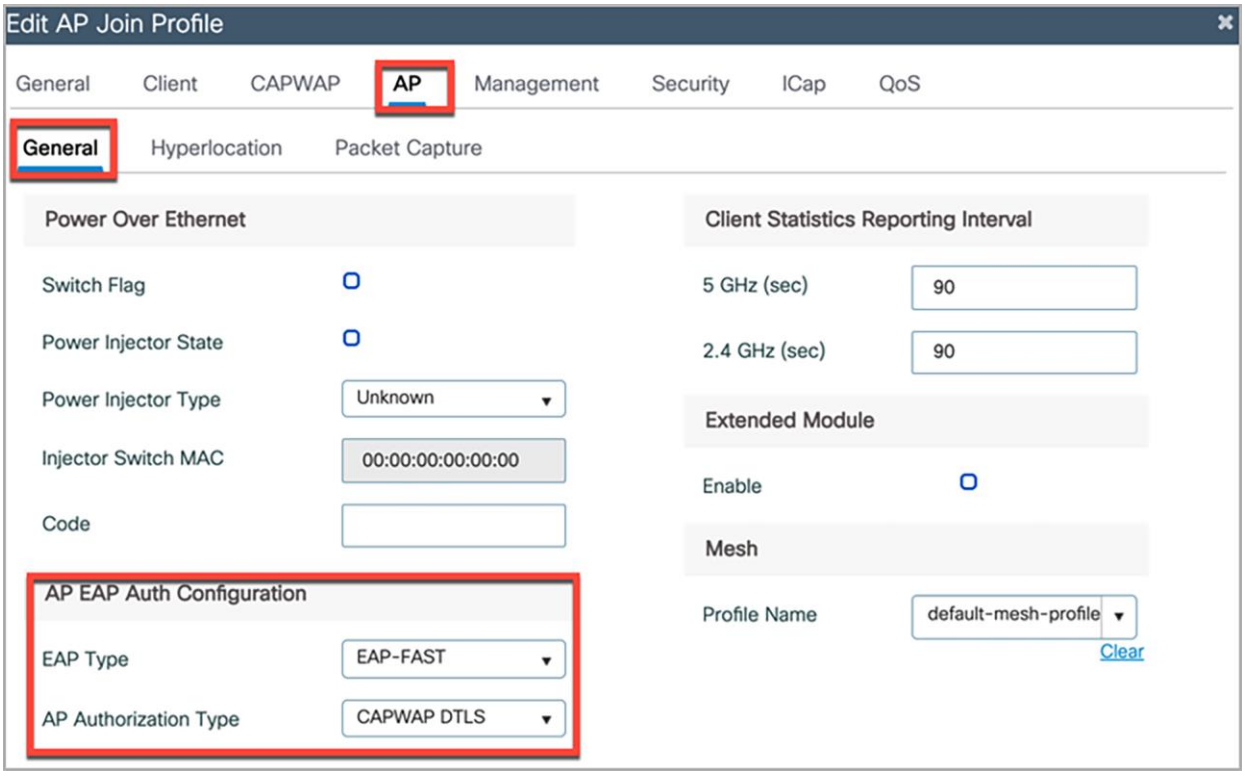


The screen shot below from the Cisco Catalyst 9800 Series Wireless Controller Security Configuration screen shows the comprehensive list of security features, which meets and exceeds the PCI DSS security compliance requirements.



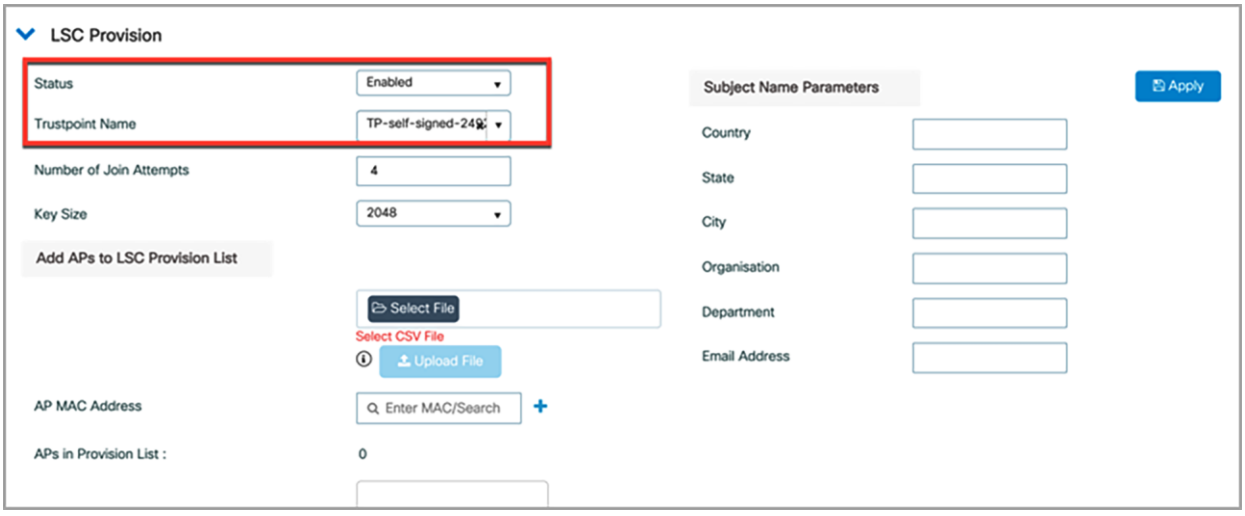
To enhance the security of the Cisco Aironet and Catalyst access points, the access point supplicant authentication methods have been added to the wireless controller. An access point supplicant works in conjunction with the switch port 802.1X authentication support. Now there is an option on the controller to enable an access point 802.1X supplicant with one of the Extensible Authentication Protocol (EAP) authentication methods — EAP-TLS, Protected EAP (EAP-PEAP), or EAP Flexible Authentication via Secure Tunneling (EAP-FAST) — globally or individually per access point. When EAP-TLS or EAP-PEAP is selected, the TLS outer tunnel between controller and access point is created with either a manufacturer installed certificate (MIC) or Locally Significant Certificate (LSC).

The new EAP-FAST authentication supplicant is supported on Wave 1 access points. The EAP-FAST, EAP-TLS, and EAP-PEAP authentication methods are supported on Wave 2 access points (Aironet 1800, 2800, 3800, and 4800 Series) and Catalyst 9100 access points.



Control and Provisioning of Wireless Access Points (CAPWAP) Datagram TLS (DTLS) LSC support on the access point is used for provisioning and downloading the certificate onto the access point.

The following screen shot shows access point provisioning with LSC.



Requirement 4: Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

Requirement 4.1: Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks. SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/ early TLS, the following provisions are included:

- New implementations must not use SSL or early TLS as a security control.
- All service providers must provide a secure service offering by June 30, 2016.
- After June 30, 2018, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet below).
- Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2018.

Note: TLSv1.2 is strongly encouraged in order to meet PCI DSS for safeguarding payment data.

The access point DTLS cipher suites supported on the Catalyst 9800 Series wireless controllers are shown in the tables below.

Access point DTLS ciphers

Configuration	Configuration options	Supported releases and notes
(config)#ap dtls-cipher?	AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384	**16.10 to 17.4** **Note:** AES128-SHA is restricted in WLAN CC mode.
(config)#ap dtls-cipher?	ECDHE-RSA-AES128-GCM-SHA256	**17.3.x and 17.4**

Configuration	Configuration options	Supported releases and notes
(config)#ap dtls-ciphersuite priority <> cipher <>	AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256	**17.5.1 onward** **Note:** AES128-SHA is restricted in WLAN CC mode.

Default cipher suites

Ciphers	Supported release and notes
AES128-SHA	**16.10 to 17.4** Applicable to non-FIPS and FIPS modes.
DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384	**16.10 to 17.3** Applicable to WLAN CC mode.
ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 AES128-SHA	**17.5.1 onward** Applicable to non-FIPS and FIPS modes.
DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 **ECDHE-RSA-AES128-GCM-SHA256**	**17.3.1 onward** Applicable to WLAN CC mode.

AP DTLS version

Config options	Supported versions
(config)#ap dtls-version? dtls_1_0 Configure DTLS 1.0 dtls_1_2 Configure DTLS 1.2	16.10 onward (from day 1)

Default DTLS version on WLC	Supported labels
DTLSv1.0 DTLSv1.0 and DTLSv1.2	16.10 to 17.2 17.3 onward

Mobility DTLS version

- Not configurable. Hard-coded to “DTLSv1.0 and DTLSv1.2.”

Mobility DTLS cipher

- Not configurable.
- Hard-coded to AES128-SHA from 16.10 to 17.4.
- Following hard-coded list from 17.5 onward.

  ECDHE-RSA-AES128-GCM-SHA256

  AES256-GCM-SHA384

  AES128-SHA

IP HTTP version

(config)#ip http tls-version?

TLSv1.0 Set TLSv1.0 version Only

TLSv1.1 Set TLSv1.1 version Only

TLSv1.2 Set TLSv1.2 version Only

Default: TLSv1.1. and TLSv1.2.

IP HTTP cipher

(config)#ip http secure-ciphersuite?

Note: Use extreme caution when applying the TLSv1.2 cipher if you have older or non-Wave 2 access points in your network that don't support that cipher. The access points that don't support TLSv1.2 will go down and cause network coverage issues.

Additional resources

PCI Data Security Standard version 3.2

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1525790995255

Cisco PCI DSS Design and Implementation Guide

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/Compliance_DIG/Compliance_DIG.pdf

Cisco SAFE SSL/TLS Vulnerability Response

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone/ssl-tls-vulnerability-response.pdf

PCI Security Standards Council

https://www.pcisecuritystandards.org/document_library

Cisco Catalyst 9800 Series LSC Configuration Guides

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/locally-significant-certificates.html#concept_FC84F350446D4D76A965400D13DA122A

Configure Simple Certificate Enrollment Protocol (SCEP) for LSC Provisioning on Catalyst 9800 Series WLC

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-management/215557-configure-scep-for-locally-significant-c.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C96-744764-00 05/21