Cisco PCI DSS 3.2 Wireless Security Compliance Supplemental Document

Revised: May 21, 2018

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 ecommerce 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 attacks are blended attacks which 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 These attacks can bypass outdated firewalls that lack the power to inspect all traffic, including large files and HTTPS encrypted traffic.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 business that accepts credit card payments, maintaining compliance with PCI standards is essential. 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 ensuring 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 as 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 Payment Card Industry (PCI) compliance guidance. The resulting Cisco® Compliance Solution for PCI was developed to implement guidance in specific Cisco laboratory configurations that undergo Verizon Qualified Security Assessor (QSA) assessment. With the release of PCI Data Security Standard (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 reference architecture to validate compliance guidance. The reference architecture consists of multiple-size branch offices, WANs, the 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 components' 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 PCI scope definition.

The PCI 3.0-3.2 standards includes 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 or web redirection servers)

The standard also uses the term "isolation" for the first time, as part of the segmentation definition. The PCI 3.0-3.2 standards clarified "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: Clarified 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 (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure 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.)

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
- 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 30th June, 2018.

Requirement 5: Use and regularly update anti-virus 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: Clarified 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 non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity's network. (Note: The requirement for multi-factor authentication for non-console administrative access from within the entity's network is a best practice until 31 January 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 point of sale (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 "non-critical" and "non-security" 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: Added 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: Increased 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 point-of-sale 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 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 SDA 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 a quarter, whether or not the organization has wireless deployed. A hacker might infiltrate a branch and install a rogue wireless device (for example, 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 point-of-sale 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 SDA controller-based architectures.

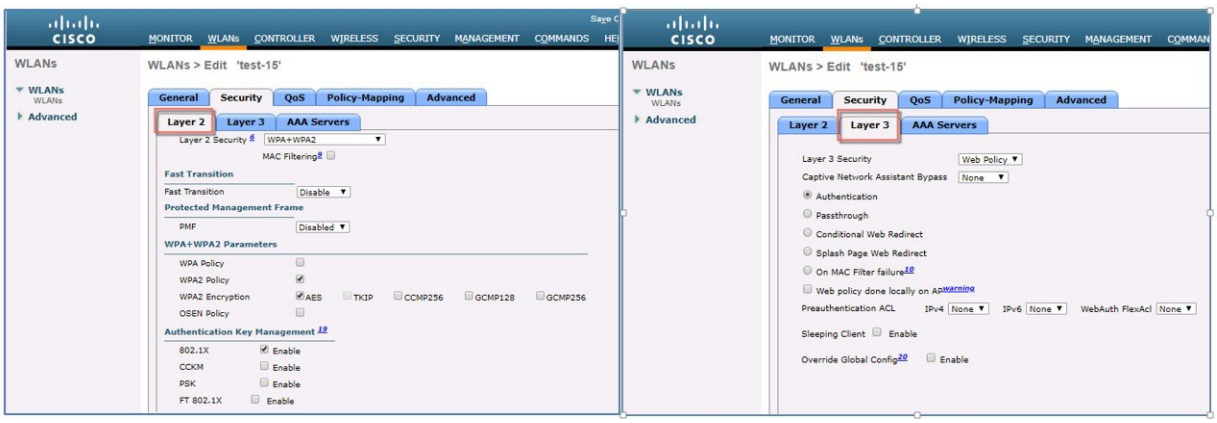
PCI Assessment Detail—PCI Sub-Requirements Satisfied

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

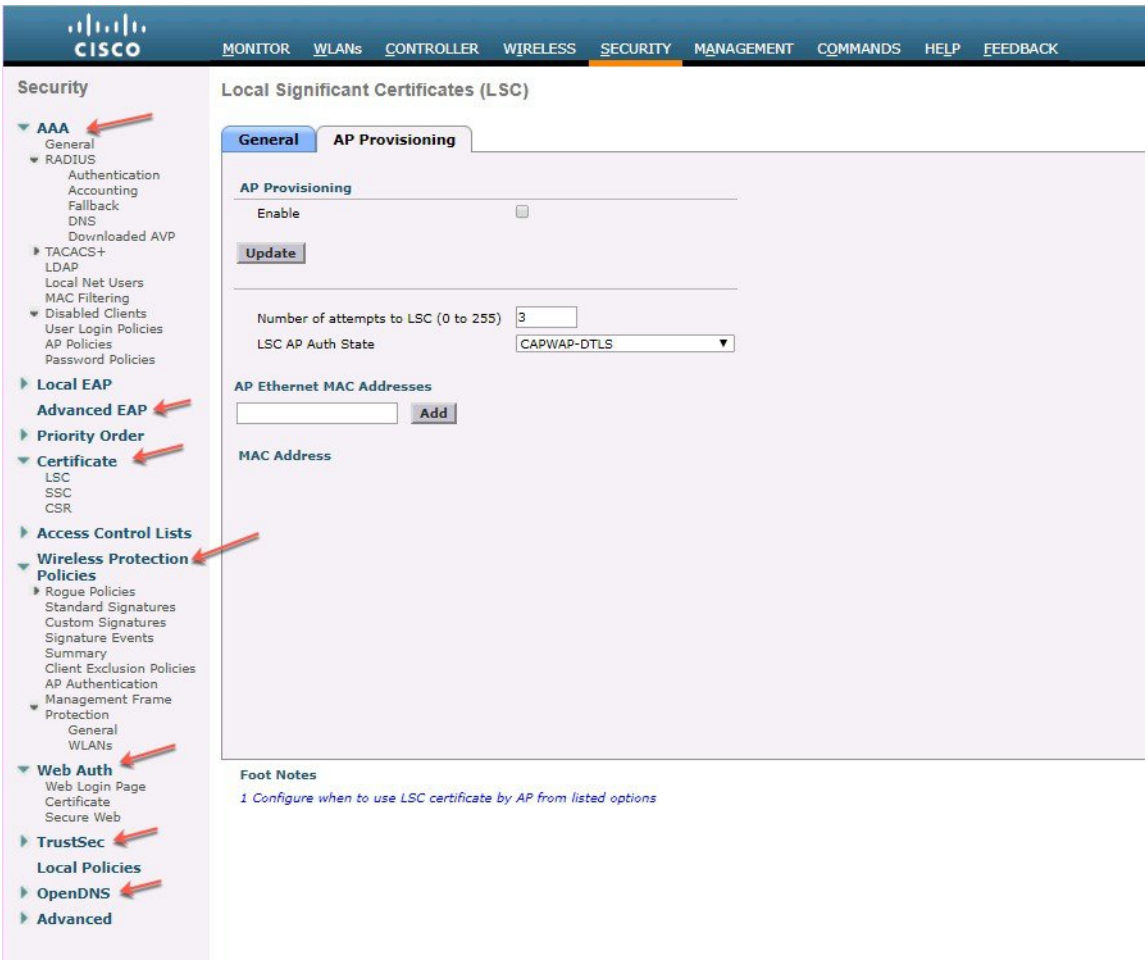
Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- 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 (WPA) and WPA2 and provides automated vulnerability scanning in the WLC to identify WLANs using suboptimal encryption. There is no default PSK, and all PSKs or Identity PSK must be created during configuration. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

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



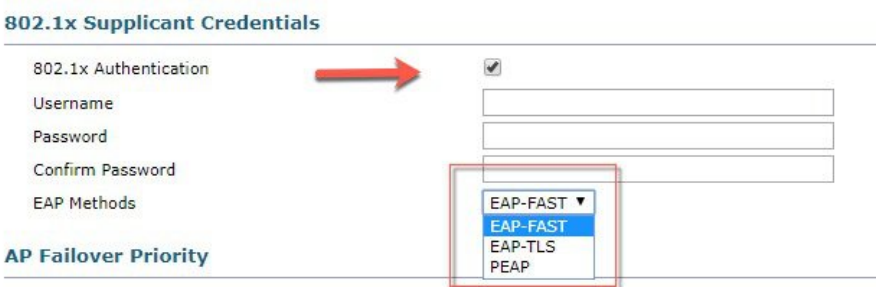
The screen shot below from the Cisco Wireless Controller Security Configuration screen shows the comprehensive list of security features that meets and exceeds the PCI DSS security compliance requirements.



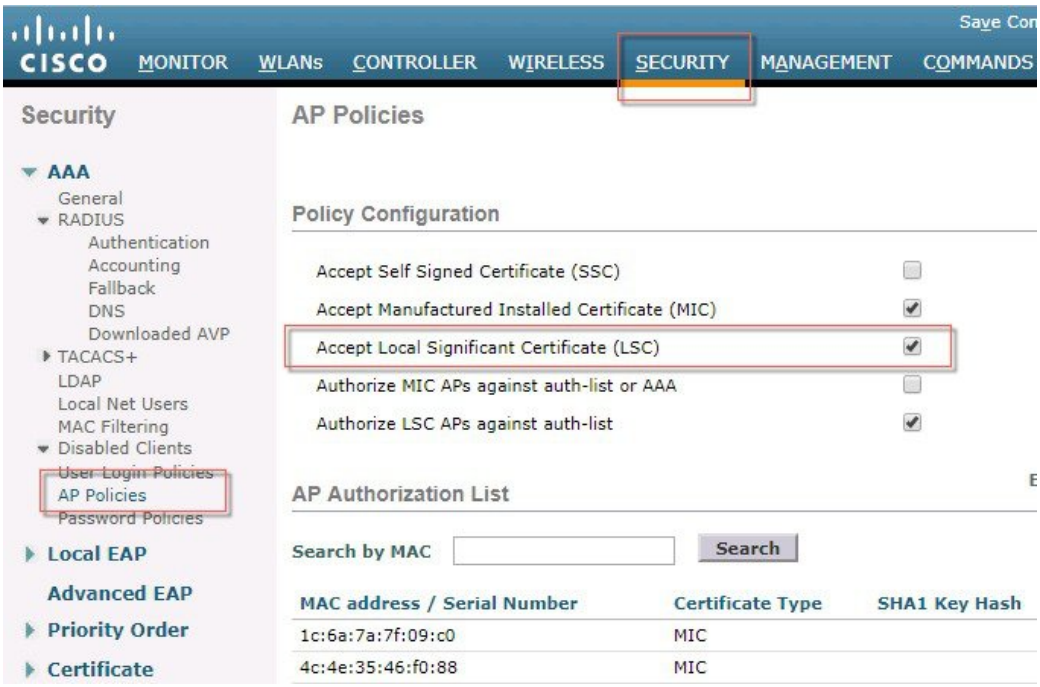
To enhance security of the Cisco Aironet APs, in release 8.7 and above new AP supplicant authentication methods have been added. AP supplicant works in conjunction with the switch port 802.1x authentication support. Now there is an option on the controller to enable AP 802.1x supplicant with one of the EAP authentication methods - EAP-TLS, EAP-PEAP or EAP-FAST globally or individually per AP. When EAP-TLS or EAP-PEAP method selected the TLS outer tunnel between Controller and AP is created with either MIC or LSC certificates. The new EAP-FAST authentication supplicant is supported on Wave-1 APs.

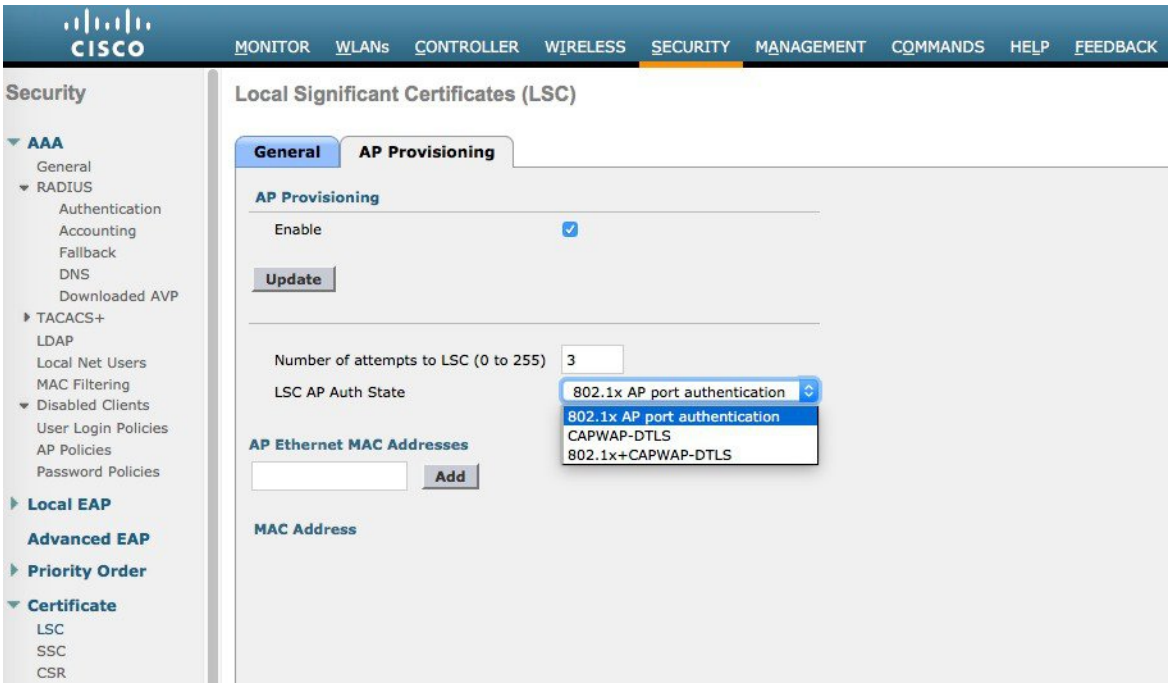
EAP-FAST/TLS/PEAP authentication methods are supported on Wave-2 APs (1800, 2800, 3800 and 4800 series).

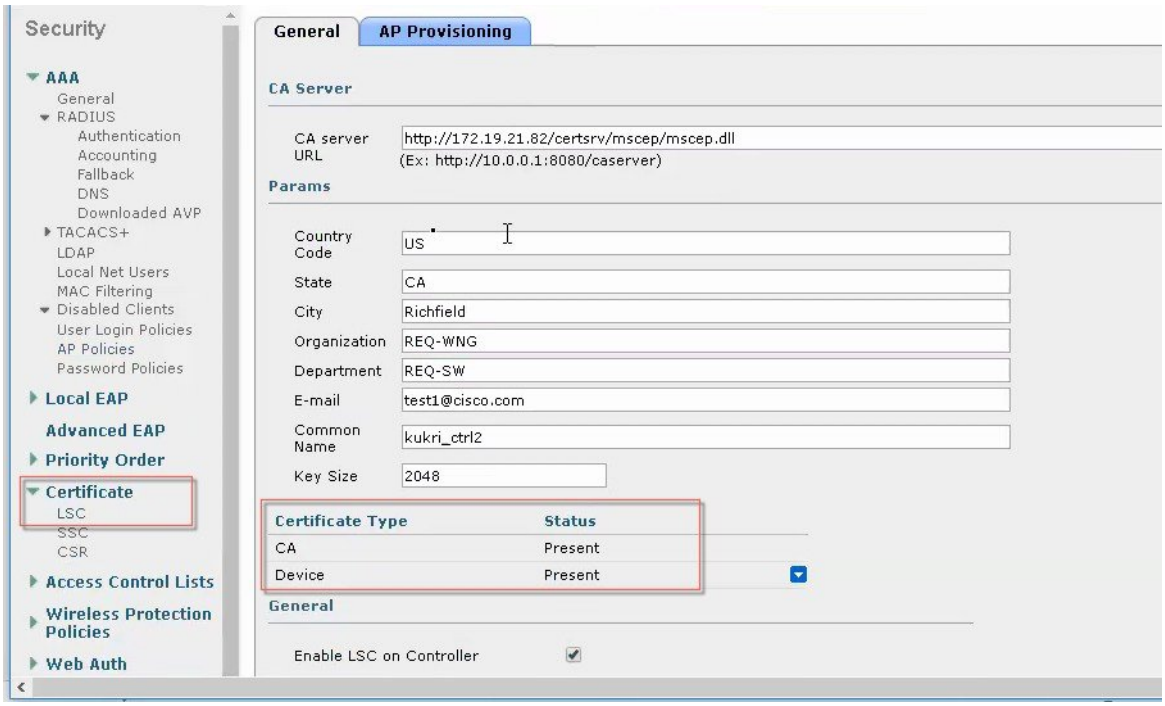
CAPWAP DTLS LSC support on the AP is used for provisioning and downloading the certificate on to the AP. In release 8.7 Flex, Local, Mesh mode for RAPs are supported.



AP provisioning with LSC screen shots is shown below:


Save Con
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
AP Policies
Policy Configuration
Accept Self Signed Certificate (SSC)
Accept Manufactured Installed Certificate (MIC)
Accept Local Significant Certificate (LSC)
Authorize MIC APs against auth-list or AAA
Authorize LSC APs against auth-list
AP Authorization List
Search by MAC
Search
MAC address / Serial Number
Certificate Type
SHA1 Key Hash
1c:6a:7a:7f:09:c0
MIC
4c:4e:35:46:f0:88
MIC


CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
LSC
SSC
CSR
Local Significant Certificates (LSC)
General
AP Provisioning
AP Provisioning
Enable
Update
Number of attempts to LSC (0 to 255)
3
LSC AP Auth State
802.1x AP port authentication
802.1x AP port authentication
CAPWAP-DTLS
802.1x+CAPWAP-DTLS
AP Ethernet MAC Addresses
Add
MAC Address



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 30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Cisco Unified Wireless Networks supports the following Security Ciphers for WebAuth and Web Management as shown below with High cipher option as TLS v1.2.

```
(5520-MA1) >config network secureweb cipher-option ?

high            Configure whether or not to use TLSv1.2 for web admin and web auth.
rc4-preference  Configure RC4 cipher suite preference for SSL/TLS 1.0 based web administration and web authentication.
sslv2           Enable or disable SSLv2 for both web administration and web authentication.
```

The AP DTLS Ciphers suites supported as shown below are:

```
(5520-MA1) >config ap dtls-cipher-suite ?

ECDHE-ECDSA-AES128-GCM-SHA256        Select ECDHE-ECDSA-AES128-GCM-SHA256 cipher
ECDHE-ECDSA-AES256-GCM-SHA384        Select ECDHE-ECDSA-AES256-GCM-SHA384 cipher
RSA-AES128-GCM-SHA256        Select RSA-AES128-GCM-SHA256 cipher
RSA-AES128-SHA        Select RSA-AES128-SHA cipher
RSA-AES256-GCM-SHA384        Select RSA-AES256-GCM-SHA384 cipher
RSA-AES256-SHA        Select RSA-AES256-SHA cipher
RSA-AES256-SHA256     Select RSA-AES256-SHA256 cipher
```

TLS 1.2 SHA2 family (non-AEAD)

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)

Note Use extreme caution when applying the TLS 1.2 cipher and you have older or non-Wave-2 APs in your network that don't support that cipher. The APs that don't support TLS 1.2 will go down and cause network coverage issues.

AP DTLS version to be used can be configured on the controller as DTLS ver 1.0 or 1.2 or both.

```
(Cisco Controller) >config ap dtls-version ?

dtls1.0             Select DTLS1.0 version
dtls1.2             Select DTLS1.2 version
dtls_all            Select all DTLS versions for backward compatibility

(Cisco Controller) >config ap dtls-version
```

Note Use extreme caution when applying the DTLS 1.2 protocol and you have older or non-Wave-2 APs in your network that don't support that protocol. The IOS based APs and Wave-1 APs would go down and cause network interruptions.

Table below summarizes what Authentication Methods and also TLS versions supported by the IOS and COS Wave-2 based APs. It also shows the CAPWAP TLS version supported by the IOS and COS based APs.

SW Version	IOS AP - Port Auth		IOS -AP - CAPWAP	COS AP - Port Auth		COS-AP CAPWAP
8.3	EAP FAST	TLS 1.0	TLS 1.0	No support		TLS 1.0/1.2
8.5	EAP FAST	TLS 1.0	TLS 1.0	No support		TLS 1.0/1.2
8.6	EAP FAST	TLS 1.0	TLS 1.0	EAP FAST	TLS 1.0	TLS 1.0/1.2
8.7	EAP FAST	TLS 1.0	TLS 1.0	EAP-FAST, EAP-TLS, PEAP	TLS 1.0	TLS 1.0/1.2
8.8	EAP FAST	TLS 1.0	TLS 1.0	EAP-FAST, EAP-TLS, PEAP	TLS 1.2	TLS 1.0/1.2

Figure 1:

		5508,2504,8510	5520,3504,8540,vwlc
COS AP	UI(when we use HTTS)	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	Local-EAP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	WPA2-EAP(ccmp)	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	LDAP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	webauth	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	NMSP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	local Auth on flex	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	.1x Supplicant	TLS1.0- 8.0, 8.2, 8.3,8.5.,8.6,8.7 TLS1.2 –8.8	TLS1.0- 8.0, 8.2, 8.3,8.5.,8.6,8.7 TLS1.2 –8.8
	CAPWAP	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8
	Mesh	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8

		5508,2504,8510	5520,3504,8540,vwlc
IOS AP	UI(when we use HTTS)	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	Local-EAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	WPA2-EAP(ccmp)	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	LDAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	webauth	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	NMSP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	local Auth on flex	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	.1x Supplicant	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	CAPWAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8

Additional References:

PCI Data Security Standard ver 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 Wireless Deployment Guides

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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