



Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2)

**FIPS 140-2 Non Proprietary Security Policy  
Level 1 Validation**

**Version 0.6**

**November 25, 2015**

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
1.1	PURPOSE.....	3
1.2	MODELS .....	3
1.3	MODULE VALIDATION LEVEL .....	3
1.4	REFERENCES.....	4
1.5	TERMINOLOGY .....	4
1.6	DOCUMENT ORGANIZATION .....	4
<b>2</b>	<b>CISCO SYSTEMS 2504, 7500, 8510 WIRELESS LAN CONTROLLERS AND CISCO CATALYST 6807-XL SWITCH WITH WIRELESS SERVICES MODULE-2 (WISM2)...</b>	<b>6</b>
2.1	CRYPTOGRAPHIC MODULE PHYSICAL CHARACTERISTICS .....	6
2.2	MODULE INTERFACES.....	6
2.3	ROLES, SERVICES AND AUTHENTICATION .....	11
2.4	SERVICES AVAILABLE IN A NON-FIPS MODE OF OPERATION .....	14
2.5	UNAUTHENTICATED SERVICES .....	14
2.6	CRYPTOGRAPHIC ALGORITHMS .....	14
2.7	CRYPTOGRAPHIC KEY MANAGEMENT .....	16
2.8	SELF-TESTS .....	22
<b>3</b>	<b>SECURE OPERATION .....</b>	<b>23</b>

# 1 Introduction

## 1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2), Firmware 8.0 with SNMP Stack v15.3, OPENSLL-0.9.8g-8.0.0, QUICKSEC-2.0-8.0 and FP-CRYPTO-7.0.0; referred to in this document as controllers or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

## 1.2 Models

- Cisco 2504 Wireless Controller (HW: 2504)
- Cisco 7500 Wireless Controller (HW: 7500)
- Cisco 8510 Wireless Controller (HW: 8510)
- Cisco Catalyst 6807-XL (HW: 6807-XL) with Wireless Services Module-2 (WiSM2) (HW: WiSM2)

In addition, to ensure Cisco Catalyst 6807-XL with WiSM2 function properly, one of the following Supervisor blades is required in FIPS mode:

- VS-S2T-10G (HW: VS-S2T-10G)
- VS-S2T-10G-XL (HW: VS-S2T-10G-XL)
- VS-S720-10G-3C (HW: VS- S720-10G-3C)
- VS-S720-10G-3CXL (HW: VS- S720-10G-3CXL)

Please notice that if any substitutions or modifications to the particular hardware versions listed above in any way would void the validation of the subject module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/groups/STM/index.html>.

## 1.3 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1

5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	<b>Overall module validation level</b>	<b>1</b>

**Table 1 Module Validation Level**

## 1.4 References

This document deals only with operations and capabilities of the Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2), in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems Security. Please refer to the following website:

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product\\_data\\_sheet\\_0900aecd802930c5.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet_0900aecd802930c5.html)

<http://www.cisco.com/en/US/products/ps6120/index.html>

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at [www.cisco.com](http://www.cisco.com).

The NIST Validated Modules website (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>) contains contact information for answers to technical or sales-related questions for the module.

## 1.5 Terminology

In this document, the Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2), are referred to as controllers, WLC, or the modules.

## 1.6 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2) and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

## **2 Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2)**

The Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2) (herein referred to as the module) are designed for maximum 802.11n performance and offers scalability for medium to large-scale enterprise and Government wireless deployments. The module supports Control and Provisioning of Wireless Access Points (CAPWAP) and Wi-Fi Protected Access 2 (WPA2) security. CAPWAP uses DTLS to provide a secure link over which CAPWAP control messages are sent and supports data DTLS to provide a secure link for CAPWAP data traffic. DTLS is essentially TLS, but over datagram (UDP) transport. WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i standard.

The module automatically detects, authorizes and configures access points, setting them up to comply with the centralized security policies of the wireless LAN. In a wireless network operating in this mode, WPA2 protects all wireless communications between the wireless client and other trusted networked devices on the wired network with AES-CCMP encryption. CAPWAP protects all control and bridging traffic between trusted network access points and the module with DTLS encryption.

Optional CAPWAP data DTLS is also supported by the module. The module supports HTTPS using TLS, CAPWAP, WPA2 (802.11i), MFP, RADIUS KeyWrap (using AES key wrapping), IPSec, Local-EAP, EAP-FAST, TACACS+, and SNMP. HTTPS using TLS uses 2048 bit modulus RSA keys to wrap 128/256 bit AES symmetric keys, and RADIUS KeyWrap uses 128 bit AES symmetric keys.

### **2.1 Cryptographic Module Physical Characteristics**

Each module is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case.

### **2.2 Module Interfaces**

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following tables:

Router Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>Two 10 Gigabit Ethernet interfaces</li> <li>SFP-10G-SR</li> <li>SFP-10G-LR</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>Two 10 Gigabit Ethernet interfaces</li> <li>SFP-10G-SR</li> <li>SFP-10G-LR</li> </ul>	Data Output Interface
<ul style="list-style-type: none"> <li>Two 10 Gigabit Ethernet interfaces</li> <li>SFP-10G-SR</li> <li>SFP-10G-LR</li> </ul>	Control Input Interface
<ul style="list-style-type: none"> <li>LEDs, mini-USB</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>Power Supply</li> </ul>	Power Interface

**Table 2 Cisco 7500 and 8510 Wireless LAN Controllers Physical Interface/Logical Interface Mapping**

Note: Small Form-Factor Pluggable (SFP) listed in table 2 above is only referred to Cisco SFP

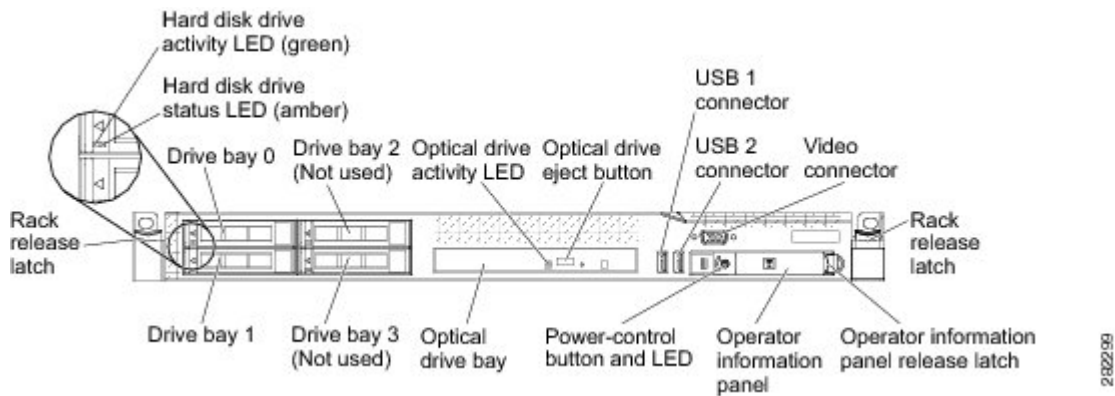
Router Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>Four 1 Gbps Ethernet (RJ-45)</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>Four 1 Gbps Ethernet (RJ-45)</li> </ul>	Data Output Interface
<ul style="list-style-type: none"> <li>Four 1 Gbps Ethernet (RJ-45)</li> </ul>	Control Input Interface
<ul style="list-style-type: none"> <li>LEDs</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>Power Supply</li> </ul>	Power Interface

**Table 3 Cisco 2504 Wireless LAN Controller Physical Interface/Logical Interface Mapping**

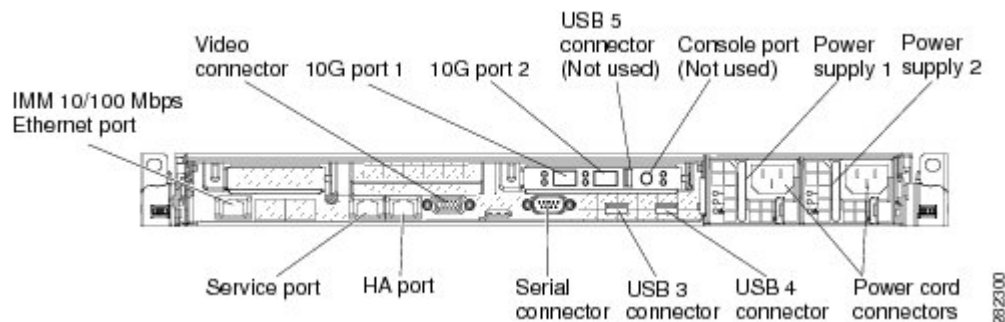
Router Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>One 10/100/1000 Ethernet port (Supervisor blade)</li> <li>Two Gigabit Ethernet ports (Supervisor blade)</li> <li>Three Console ports (two are on Supervisor blade, and one is on the WiSM2)</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>One 10/100/1000 Ethernet port (Supervisor blade)</li> <li>Two Gigabit Ethernet ports (Supervisor blade)</li> <li>Three Console ports (two are on Supervisor blade, and one is on the WiSM2)</li> </ul>	Data Output Interface

Router Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>• One 10/100/1000 Ethernet port (Supervisor blade)</li> <li>• Two Gigabit Ethernet ports (Supervisor blade)</li> <li>• Three Console ports (two are on Supervisor blade, and one is on the WiSM2)</li> </ul>	Control Input Interface
<ul style="list-style-type: none"> <li>• One 10/100/1000 Ethernet port (Supervisor blade)</li> <li>• Two Gigabit Ethernet ports (Supervisor blade)</li> <li>• Three Console ports (two are on Supervisor blade, and one is on the WiSM2)</li> <li>• LEDs</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>• Power Supply</li> </ul>	Power Interface

**Table 4 Cisco Catalyst 6807-XL Switch with WiSM2 Physical Interface/Logical Interface Mapping**



**Figure 1 – Cisco 8510 Wireless LAN Controller Front Panel**



**Figure 2 – Cisco 8510 Wireless LAN Controller Rear Panel**



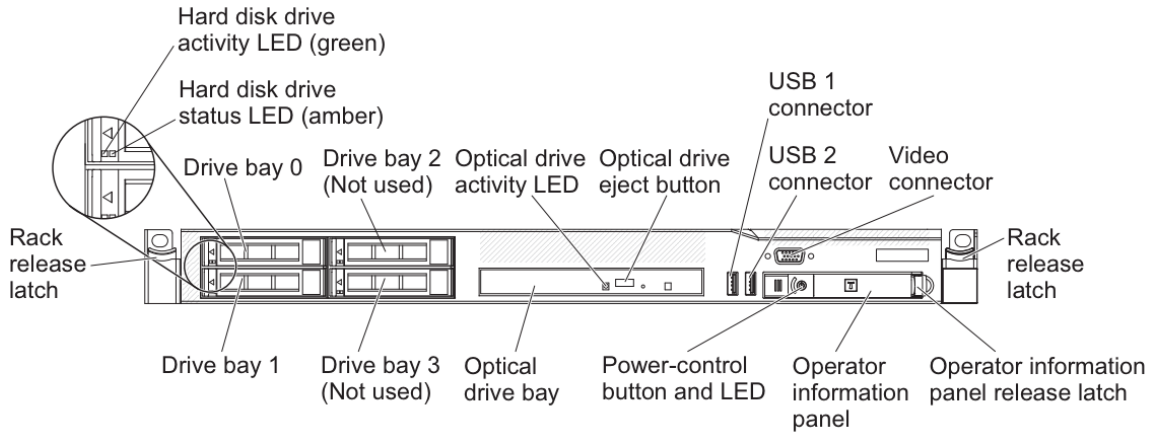


Figure 3 – Cisco 7500 Wireless LAN Controller Front Panel

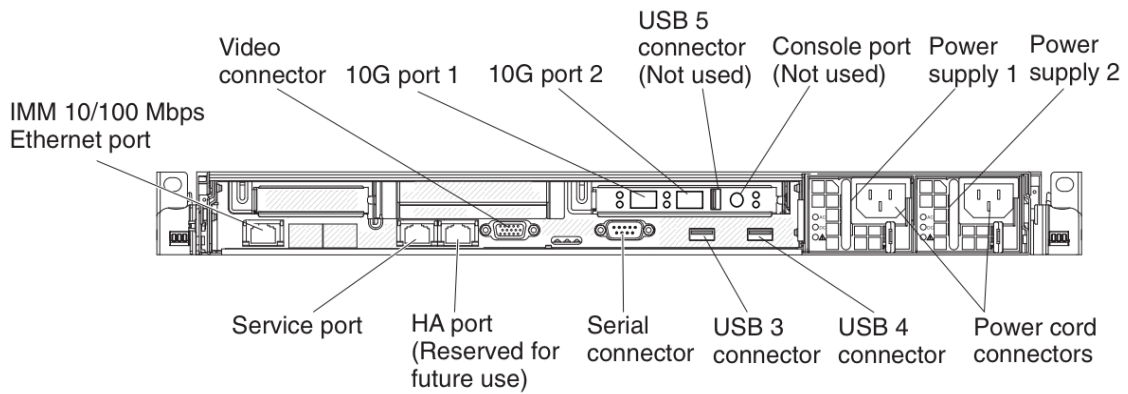


Figure 4 – Cisco 7500 Wireless LAN Controller Rear Panel

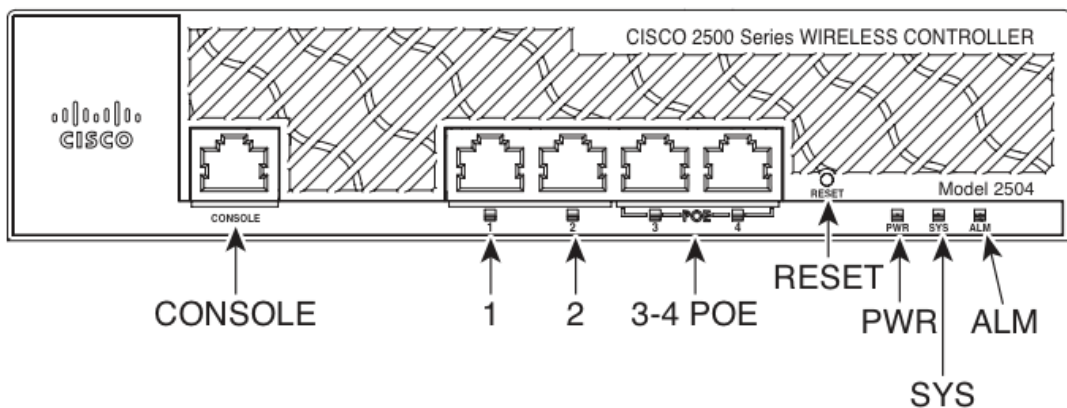


Figure 5 – Cisco 2504 Wireless LAN Controller Front Panel

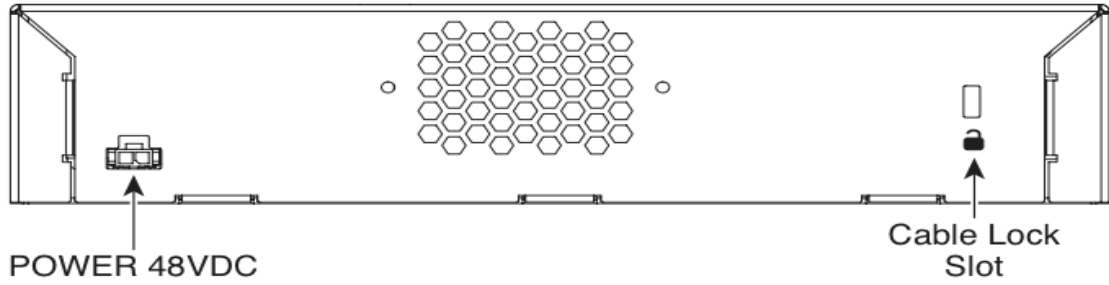


Figure 6 – Cisco 2504 Wireless LAN Controller Back Panel

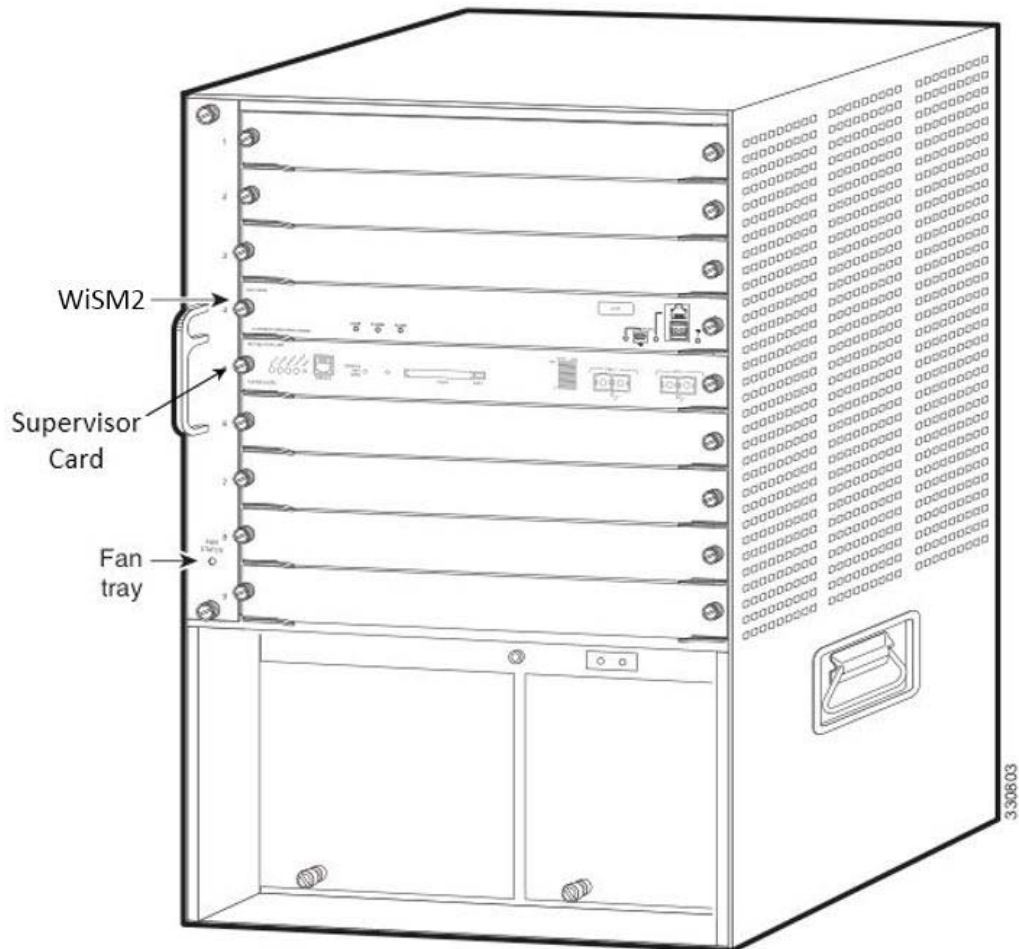


Figure 7 – Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2)

## 2.3 Roles, Services and Authentication

The module supports role-based authentication. There are four roles in the module that the operators may assume in the FIPS mode:

- AP Role—This role is filled by an access point associated with the controller.
- Client Role—This role is filled by a wireless client associated with the controller.
- User Role—This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with read-only privileges.
- Crypto Officer (CO) Role—This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module. The product documentation refers to this role as a management user with read-write privileges.

The Module does not support a Maintenance Role.

### User Services

The services available to the User role consist of the following:

Services	Description	Keys & CSPs Access (please see table 9 below for CSP Details)
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A
TACACS+	User & CO authentication to the module using TACACS+.	N/A (No keys are accessible)
IPSec	Secure communications between controller and RADIUS	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IPSec session encryption key, IPSec session authentication key – w, d
RADIUS Key Wrap	Establishment and subsequent receive 802.11i PMK from the RADIUS server.	RADIUS AES KeyWrap KEK, RADIUS KeyWrap MACK – w, d

**Table 5 - User Services (r = read, w = write, d = delete)**

### Crypto Officer Services

The Crypto Officer services consist of the following:

Services	Description	Keys & CSPs Access (please see table 9 below for CSP Details)
----------	-------------	---

Self Test and Initialization	Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A (No keys are accessible)
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A (No keys are accessible)
TACACS+	User & CO authentication to the module using TACACS+.	TACACS+ authentication secret, TACACS+ authorization secret, TACACS+ accounting secret – r, w, d
IPSec	Secure communications between controller and RADIUS	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IPSec session encryption key, IPSec session authentication key – w, d ISAKMP preshared – r, w, d
Zeroization	Zeroize CSPs and cryptographic keys by calling 'switchconfig key-zeroize controller' command or cycling power to zeroize all cryptographic keys stored in SDRAM. The CSPs (password, secret, cscoCCDefaultMfgCaCert, engineID) stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed
Module Configuration	Selection of non-cryptographic configuration settings	N/A (No keys are accessible)
SNMPv3	Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password – r, w, d SNMP session key – w, d
HTTPS/TLS	<ul style="list-style-type: none"> <li>Establishment and subsequent data transfer of a TLS session for use between the module and the CO.</li> <li>Protection of syslog messages</li> </ul>	TLS pre-master secret, encryption key, integrity key – w, d
DTLS Data Encrypt	Enabling optional DTLS data path encryption for Office Extended AP's	DTLS Master Secret, encryption keys, DTLS Session Integrity Keys – w, d
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11i PMK from the RADIUS server.	RADIUS Server Shared Secret, RADIUS AES KeyWrap KEK, RADIUS KeyWrap MACK – w, d

**Table 6 - Crypto Officer Services (r = read, w = write, d = delete)**

## AP and Client Services

The AP and Client services consist of the following:

Services	Description	Keys & CSPs Access (please see table 9 below for CSP Details)
MFP (AP Role)	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.	Infrastructure MFP MIC Key -d
Local EAP Authenticator (Client Role)	Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller.	N/A (No keys are accessible)
802.11i (AP Role)	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point	802.11i Pairwise Master Key (PMK), 802.11i Key Confirmation Key (KCK), 802.11i Key Encryption Key

		(KEK), 802.11i Pairwise Transient Key (PTK), 802.11i Group Temporal Key (GTK) – w, d
RADIUS Key Wrap (AP and Client Role)	Establishment and subsequent receipt of 802.11i PMK from the RADIUS server.	RADIUS AES KeyWrap KEK, RADIUS KeyWrap MACK – w, d

**Table 7 – AP and Client Services (r = read, w = write, d = delete)**

### **CO Authentication**

The module prompts the operator for CO role authentication via CLI. If the password is validated against the CO role’s password in memory, the CO role is authenticated and allowed entry to execute services that were designed for CO role.

CO passwords must be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be  $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251, 596, 800$ ). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

### **User Authentication**

The module prompts the operator for User role authentication via CLI. If the password is validated against the User role’s password in memory, the User role is authenticated and allowed entry to execute services that were designed for User role.

User role passwords must be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be  $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251, 596, 800$ ). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

### **AP Authentication**

The module performs mutual authentication with an access point through the CAPWAP protocol, using an RSA key pair with 1024 bits or 2048 bits modulus, which has an equivalent symmetric key strength of 80 bits or 112 bits. Assuming the low end of that range, an attacker would have a 1 in  $2^{80}$  chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a

successful random key guess in one minute, an attacker would have to be capable of approximately  $1.8 \times 10^{21}$  attempts per minute, which far exceeds the operational capabilities of the modules to support.

### **Client Authentication**

The module performs mutual authentication with a wireless client through EAP-TLS or EAP-FAST protocols. EAP-FAST is based on EAP-TLS and uses EAP-TLS key pair and certificates. The RSA key pair for the EAP-TLS credentials has modulus size of 1024 bits or 2048 bits, thus providing between 80 bits or 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in  $2^{80}$  chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately  $1.8 \times 10^{21}$  attempts per minute, which far exceeds the operational capabilities of the modules to support.

Please notice that the RSA used in either AP role or Client role (RSA 1024 bits or 2048 bits) authentication above only performs RSA signature verification. More information can be obtained in section 2.6 in this document.

## 2.4 Services Available in a Non-FIPS Mode of Operation

- SSHv1 with RC4 and HMAC-MD5
- SNMP v1 and v2
- IPSec/IKE with Diffie-Hellman 768-bit/1024-bit modulus and Triple-DES

## 2.5 Unauthenticated Services

An unauthenticated operator may observe the System Status by viewing the LEDs on the module, which show network activity and overall operational status. A solid green LED indicates normal operation and the successful completion of self-tests. The module does not support a bypass capability in the approved mode of operations.

## 2.6 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

### **Approved Cryptographic Algorithms**

The module supports the following FIPS 140-2 approved algorithm implementations, whose names are SNMP (FW: SNMP Stack v15.3), OSSL (FW: OPENSLL-0.9.8g-8.0.0), QuickSec (FW: QUICKSEC-2.0-8.0) and 5508 CN56xx Datapath (HW: CN56XX; FW: FP-CRYPTO-7.0.0).

	SNMP	OSSL	QuickSec	5508 CN56xx
--	------	------	----------	-------------

<b>P/N or Version</b>	FW: SNMP Stack v15.3	FW: OPENSSL- 0.9.8g-8.0.0	FW: QUICKSEC-2.0- 8.0	Datapath HW: P/N CN56XX FW: FP- CRYPTO-7.0.0
AES-CBC	N/A	#2894	#2895	#1348
AES-CFB	#2906	N/A	N/A	N/A
AES-ECB	N/A	#2894	N/A	N/A
SHA-1	N/A	#2437	#2438	#1230
SHA-256	N/A	#2437	N/A	N/A
HMAC SHA-1	#1840	#1830	#1831	#787
DRBG	N/A	#526	N/A	N/A
RSA	N/A	#1524	N/A	N/A
CVL (SP800- 135)	N/A	#322	N/A	N/A
KBKDF (SP800- 108)	N/A	#31	N/A	N/A

**Table 8 - Approved Cryptographic Algorithms**

Note:

- RSA Cert. #1524 only supports RSA Signature Verification in this module.
- CVL Cert. #322 supports the KDF (key derivation function) used in each of IKEv1, TLS and SNMPv3 protocols.
- IKEv1, TLS and SNMPv3 protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.

### **Non-Approved Cryptographic Algorithms but Allowed in FIPS mode**

The module supports the following non-approved, but allowed cryptographic algorithms:

- AES (Cert. #2894, key wrapping; key establishment methodology provides 128 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- MD5 (MD5 is allowed in DTLS v1.0)
- NDRNG

### **Non-Approved Cryptographic Algorithms**

- Diffie-Hellman (less than 112 bits of encryption strength)
- HMAC-MD5
- RC4
- Triple-DES (non-compliant)

## 2.7 Cryptographic Key Management

Cryptographic keys are stored in plaintext form, in flash for long-term storage and in SDRAM for active keys. The AES key wrap KEK, AES key wrap MACK keys, and the Pre shared key (PSK) are input by the CO in plaintext over a local console connection. The PMK is input from the RADIUS server encrypted with the AES key wrap protocol or via IPsec. RSA public keys are output in plaintext in the form of X.509 certificates. The CAPWAP session key is output wrapped with the AP's RSA key, and the MFP MIC key and 802.11i PTK, 802.11i GTK are output encrypted with the CAPWAP session key. Asymmetric key establishment (RSA key transport) is used in the creation of session keys during EAP-TLS and EAP-FAST. Any keys not explicitly mentioned are not input or output.

Tables 5-7 list the access to the keys by service. Table 9 lists the secret and private cryptographic keys and CSPs used by the module. Please note that the CSPs below are stored in plaintext in both SDRAM and Flash.

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
<b>General Keys/CSPs</b>					
DRBG entropy input	SP 800-90 CTR_DRBG	HW based entropy source output used to construct seed	256-bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DRBG seed	SP 800-90 CTR_DRBG	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	384 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DRBG V	SP 800-90 CTR_DRBG	Internal V value used as part of SP 800-90a CTR_DRBG.	128 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DRBG Key	SP 800-90 CTR_DRBG	This is the 256-bit DRBG key used for SP 800-90a CTR_DRBG.	256 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
ciscoCCDefaultMfgCaCert	rsa-pkcs1-sha2	Verification certificate, used with CAPWAP to validate the certificate that authenticates the access point generated/installed at manufacturing.	2048	Flash	Overwrite with new certificate
Diffie-Hellman public key	Diffie-Hellman (Group 14)	The public key used in Diffie-Hellman (DH) Exchange.	2048 bits	SDRAM	'switchconfig key-zeroize controller' command or



Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
					Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	The private key used in Diffie-Hellman (DH) Exchange.	224 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	2048 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
RADIUS Server Shared Secret	Shared secret	This is the shared secret between the RADIUS server and Controller. Entered by the Crypto Officer in plaintext form and stored in plaintext form.	22 bytes	Flash	Overwrite with new secret
RADIUSOverIPSecEncryptionKey	AES-128/256	AES-128/AES-256 encryption/decryption key, used in IPSec tunnel between module and RADIUS to encrypt/decrypt EAP keys.	128-256 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
RADIUSOverIPSecIntegrityKey	HMAC	Integrity/authentication key, used in IPSec tunnel between module and RADIUS.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
User password	Password	Identity based authentication data for user.	Variable (8+ characters)	Flash	Overwrite with new password
Enable secret	Password	Identity based authentication data for CO.	Variable (8+ characters)	Flash	Overwrite with new secret
TACACS+ authentication secret	Shared secret	This is the authentication shared secret between the TACACS+ server and Controller. Entered by the Crypto Officer in plaintext form and stored in plaintext form.	64 bytes	Flash	Overwrite with new secret
TACACS+ authorization secret	Shared secret	This is the authorization shared secret between the TACACS+ server and Controller. Entered by the Crypto Officer in plaintext form and stored in plaintext form.	64 bytes	Flash	Overwrite with new secret

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
TACACS+ accounting secret	Shared secret	This is the accounting shared secret used for authentication between the TACACS+ server and Controller. Entered by the Crypto Officer in plaintext form and stored in plaintext form.	64 bytes	Flash	Overwrite with new secret
<b>IKE/IPSEC</b>					
skeyid	HMAC-SHA-1	It was derived by using 'ISAKMP pre-shared' and other non-secret values through the key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKE v1.	160-bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
skeyid_d	HMAC-SHA-1	It was derived by using skeyid, Diffie-Hellman shared secret and other non-secret values through key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKE v1.	160-bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
IKE session encryption key	AES	The IKE session (IKE Phase I) encrypt key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv1). Used for IKE payload protection.	256-bit AES	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
IKE session authentication key	HMAC-SHA-1	The IKE session (IKE Phase I) authentication key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv1). Used for IKEv1/IKEv2 payload integrity verification.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
ISAKMP pre-shared	Shared secret	This shared secret was manually entered by CO for IKE pre-shared key based authentication	8 chars	Flash	Overwrite with new secret

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
		mechanism.			
IPSec authentication key	HMAC-SHA1	The IPSec (IKE Phase II) authentication key is derived via using the KDF defined in SP800-135 KDF (IKEv1). Used to authenticate the IPSec peer.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
IPSec encryption key	AES	The IPSec (IKE phase II) encryption key is derived via a key derivation function defined in SP800-135 KDF (IKEv1).Used to Secure IPSec traffics.	256-bit AES	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
<b>DTLS</b>					
DTLS Pre-Master Secret	Shared Secret	Generated by approved DRBG for Used to derive the DTLS Encryption/Decryption Key and DTLS Integrity Key.	48 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to derive the DTLS Encryption/Decryption Key and DTLS Integrity Key.	48 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DTLS Encryption/Decryption Key (CAPWAP session keys)	AES-CBC	Session Keys used to encrypt/decrypt CAPWAP control messages.	128-256 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
DTLS Integrity Key	HMAC-SHA1	This key is used for integrity checks on CAPWAP control messages.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
<b>SNMPv3</b>					
snmpEngineID	Shared secret	Unique string to identify the SNMP engine.	32-bits	Flash	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	32 bytes	Flash	Overwrite with new password

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
SNMPv3 session key	AES-CFB	Encrypts SNMPv3 traffics.	128-bit	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
<b>HTTPS/TLS</b>					
HTTPS TLS Pre-Master secret	Shared secret	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	48 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
HTTPS TLS Encryption Key	AES-CBC	AES key used to encrypt TLS data.	128 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
HTTPS TLS Integrity Key	HMAC-SHA1	HMAC-SHA-1 key used for HTTPS integrity protection.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
TLS Pre-Master Secret	Shared secret	Shared secret used to generate new TLS session keys for syslog.	48 byte	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
TLS Encryption Key	AES-CBC	Symmetric AES key for encrypting syslog messages over TLS.	128 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
TLS Integrity Key	HMAC-SHA1	Used for TLS integrity protection of syslog messages.	160 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
Infrastructure MFP MIC Key	AES-CMAC	This key is generated in the module by calling FIPS approved DRBG and then is transported to the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CMAC function to sign management frames when infrastructure MFP is enabled.	128 bits	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
<b>802.11i</b>					
802.11i Pre-Shared Key (PSK)	Shared secret	This is the shared secret used for 802.11i client authentication.	63 bytes	Flash	Overwrite with new secret.

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
802.11i Pairwise Master Key (PMK)	HMAC-SHA-1	The PMK is transferred to the module, protected by RADIUS AES KeyWrap key. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	32 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
802.11i Key Confirmation Key (KCK)	HMAC-SHA1	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.	16 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
802.11i Key Encryption Key (KEK)	AES Key Wrap	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.	16 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
802.11i Pairwise Transient Key (PTK)	AES-CCM	The PTK is the 802.11i session key for unicast communications. This key is generated in the module by calling FIPS approved DRBG and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11i unicast communications service.	16/32 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
802.11i Group Temporal Key (GTK)	AES-CCM	The GTK is the 802.11i session key for broadcast communications. This key is generated in the module by calling FIPS approved DRBG and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11i broadcast communications service.	16/32 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle
RADIUS AES KeyWrap KEK	AES-ECB	This key is used by the RADIUS Keyrap service to protect the PMK for the 802.11i protocol.	16 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle

Key/CSP Name	Generation/Algorithm	Description	Key Size	Storage	Zeroization
RADIUS KeyWrap MACK	HMAC-SHA1	The MAC key used by the RADIUS Keywrap service to authenticate RADIUS traffics.	16 bytes	SDRAM	'switchconfig key-zeroize controller' command or Power cycle

**Table 9 - Cryptographic Keys and CSPs**

Note: The KDF infrastructure used in DTLS v1.0 is identical to the one used in TLS v1.0/1.1, which was certified by CVL Cert. #322.

## 2.8 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly.

Power On Self-Tests Performed:

- SNMP algorithm implementation
  - AES encryption KAT
  - AES decryption KAT
  - HMAC SHA-1 KAT
- OSSL algorithm implementation
  - AES encryption KAT
  - AES decryption KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - HMAC SHA-1 KAT
  - SP 800-90 DRBG KAT
  - RSA (verify) KAT
  - Firmware Integrity Test RSA with SHA-256
- QuickSec algorithm implementation
  - AES encryption KAT
  - AES decryption KAT
  - SHA-1 KAT
  - HMAC SHA-1 KAT
- 5508 CN56xx Datapath algorithm implementation
  - AES encryption KAT
  - AES decryption KAT

- SHA-1 KAT
- HMAC SHA-1 KAT

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before a role can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure.

Conditional Tests Performed:

- Continuous Random Number Generator Test for the FIPS-approved DRBG
- Continuous Random Number Generator Test for the non-approved NDRNG

### 3 Secure Operation

The module was validated with firmware version 8.0 with SNMP Stack v15.3, OPENSLL-0.9.8g-8.0.0, QUICKSEC-2.0-8.0 and FP-CRYPTO-7.0.0 (This is the only allowable image for FIPS-approved mode of operation). Follow the instructions provided below to place the module in FIPS-approved mode. Operating the module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

#### 1. Enable FIPS Mode of Operations

The following CLI command places the controller in FIPS mode of operations, enabling all necessary self-tests and algorithm restrictions:

```
> config switchconfig fips-prerequisite enable
```

#### 2. Configure HTTPS Certificate

The following command configures the controller to use the manufacture-installed Cisco device certificate for the HTTPS server. It must be executed after enabling FIPS mode of operations:

```
> config certificate use-device-certificate webadmin
```

#### 3. Configure Authentication Data

All users shall have a password containing 8 or more characters, including numbers and letters. A crypto officer can use the following CLI command to set user passwords:

```
>config mgmtuser password username password
```

Note that this and all subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document. It is the Crypto Officer's responsibility to securely deliver the password over to User.

#### 4. Configure Communications with RADIUS

Communications between the controller and RADIUS may be configured for RADIUS KeyWrap or IPsec.

#### 5. RADIUS KeyWrap and MACK Keys

The following CLI commands configure the RADIUS shared secret and AES-key wrap KEK and MACK:

```
> config radius auth add index ip-address port hex secret
```

```
> config radius auth keywrap add hex kek mack index
```

```
> config radius auth keywrap enable
```

#### 6. IPsec/IKE

Optionally, the controller may be configured to communicate with RADIUS via IPsec. Refer to the document at the following link for additional instructions:

[http://www.cisco.com/en/US/products/ps6366/products\\_tech\\_note09186a0080a829b8.shtml](http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080a829b8.shtml)

In addition, please be aware that AES is the only allowed symmetric algorithm used in IPsec/IKE encryption/decryption operations in FIPS mode.

#### 7. Configure Pre-shared Keys for 802.11i

802.11i Pre-shared key (PSK) is an optional mode permitted by this security policy. Generation of pre-shared keys is outside the scope of this security policy, but they should be entered as 64 hexadecimal values (256 bits) by the following command syntax:

```
> config wlan security wpa akm psk enable index
```

```
> config wlan security wpa akm psk set-key hex key index
```

Refer to Cisco Wireless LAN Controller Configuration Guide for additional instructions.

#### 8. Configure Ciphersuites for 802.11i

The following CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:



- > config wlan create index *profile\_name ssid*
- > config wlan radius\_server auth add *index radius-server-index*
- > config wlan enable *index*

## 9. Configure SNMPv3

Only SNMPv3 with HMAC-SHA-1 is permitted by this security policy. The user passwords shall be selected to be 8 or more characters, including numbers and letters. This has been tested and is FIPS compliant.

The following CLI commands enable SNMPv3 with HMAC-SHA1:

- > config snmp version v1 disable
- > config snmp version v2c disable
- > config snmp version v3 enable
- > config snmp v3user create *username <ro|rw> hmacsha aes128 authkey encryptkey*

## 10. Configure TACACS+ secret

The crypto officer may configure the module to use TACACS+ for authentication, authorization and accounting. Configuring the module to use TACACS+ is optional. If the module is configured to use TACACS+, the Crypto-Officer must define TACACS+ shared secret keys that are at least 8 characters long. The following CLI command configures TACACS+ for authentication (auth), authorization (athr) and accounting (acct):

```
>config tacacs <auth|athr|acct> add index ip port <ascii|hex> secret
```

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

## 11. Configure MFP –Management Frame Protection (Optional)

Infrastructure MFP (Management Frame Protection) enables one access point to validate a neighboring Access Point's management frames. The following CLI command is used to enable infrastructure MFP:

```
>config wps mfp infrastructure enable
```

802.11w also called PMF (Protected Management Frames) is a standards based form of MFP used to encrypt and sign management frames between the AP and the client. The following CLI command is used to enable client 802.11w:

>config wlan security pmf required <WLAN ID>

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

## 12. Configure Data DTLS (optional)

The crypto officer may configure the module to use CAPWAP data encryption. CAPWAP data packets encapsulate forwarded wireless frames. Configuring the module to use CAPWAP data encryption is optional.

The following CLI commands enable DTLS data encryption for access points on the controller:

To enable or disable data encryption for all access points or a specific access point, enter this command:

a. >config ap link-encryption {enable | disable} {all | *Cisco\_AP*}

When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter

b. >Y

To save your changes, enter this command:

c. >save config

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

## 13. Configure Data DTLS with Office Extend Access Points (optional)

The crypto officer may configure the module to use CAPWAP data encryption with Office Extend Access Points (AP models 1131, 1142, and 3502i). CAPWAP data encryption with Office Extend APs secures communications from a controller to a remote access points using CAPWAP data encryption. The following CLI commands enable CAPWAP data encryption with Office Extend APs:

To enable hybrid-REAP on the access point, enter this command:

a. >config ap mode flexconnect *Cisco\_AP*

To configure one or more controllers for the access point, enter one or all of these commands:

b. >config ap primary-base *controller\_name Cisco\_AP controller\_ip\_address*

- c. `>config ap secondary-base controller_name Cisco_AP controller_ip_address`
- d. `>config ap tertiary-base controller_name Cisco_AP controller_ip_address`

To enable the OfficeExtend mode for this access point, enter this command:

- e. `>config flexconnectoffice-extend {enable | disable} Cisco_AP` To save your changes, enter this command:
- f. `>save config`

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

#### 14. Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

- a. `>save config`
- b. `>reset system`