FIPS 140-2 Security Policy for Cisco 5508 Wireless LAN Controller

May 24, 2013
Policy Version 3.4

This document details the Security Policy for the module. This Security Policy may be freely distributed.

Contents

This security policy contains these sections:

- Overview, page 2
- Physical Security Policy, page 4
- Secure Configuration, page 5
- Roles, Services, and Authentication, page 10
- Cryptographic Key Management, page 13
- Disallowed Security Functions, page 20
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 21

Cisco Systems, Inc.
www.cisco.com

Overview

The Cisco 5508 Wireless LAN Controller (herein referred to as the module) is 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. Figure 1 shows the entire module.

Figure 1 Entire Module

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 bit AES symmetric keys, and RADIUS KeyWrap uses 128 bit AES keys as key encrypting keys to wrap AES keys of up to 128 bits. It is a multiple-chip standalone cryptographic module.

Table 1 Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2

Security Requirements Section	Level
Design Assurance	3
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module includes all hardware and firmware. The evaluated platform consists of model number CT5508, with firmware version 7.0.240.0, hardware revision B0, and opacity baffle version A0.

In the FIPS mode of operations, the module supports the following cryptographic algorithm implementations:

- AES (AES Cert. #2330, key wrapping; key establishment methodology provides 128 bits of encryption strength)
- AES-CBC and ECB (firmware) (Cert. #2330)
- AES-ECB and CCM (firmware) (Cert. #1347)
- AES-CBC (hardware/firmware) (Cert. #1348)
- SHA-1 (firmware) (Certs. #1228 and #2014)
- SHA-1 (hardware/firmware) (Cert. #1230)
- SHA-256 (firmware) (Cert. #2014)
- HMAC SHA-1 (firmware) (Certs. #785 and #786)
- HMAC SHA-1 (hardware/firmware) (Cert. #787)
- ANSI X9.31 Random Number Generator (hardware/firmware) (Cert. #742)
- RSA signature verification (firmware) (Certs. #653 and #654)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- TDES (firmware) (Cert. #935)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (used to seed the Approved RNGs)
- SP800-90 Block Cipher DRBG (firmware) (DRBG Cert. #289; uses AES with 256 bits of encryption strength)

The module is interoperable with all FIPS 140-2 validated wireless LAN clients that support the ratified IEEE 802.11i standard.

Physical Security Policy

The Crypto Officer is responsible for the installation of the FIPS opacity shield and the placement and maintenance of the tamper evident labels.

Installing the FIPS Opacity Shield

Installation requires the 5508 FIPS kit (AIR-CT5508FIPSKIT=) which includes the FIPS opacity shield and FIPS Tamper Evident Labels, and the 5508 controller rack mounting brackets that were shipped with the controller. For additional information refer to the Cisco document at this URL: http://www.cisco.com/en/US/docs/wireless/controller/5500/install/guide/ctrl5500.html#wp63805

Follow these steps to install the opacity shield:

Step 1 Align the FIPS shield to the front of the controller unit, aligning screw holes to existing mount holes on left and right sides of controller.

Step 2 Attach one of the front brackets to the controller using three M4 screws. The screws will go through the front mount bracket, then through the FIPS shield, and thread into the side of the controller.

Follow the same steps to attach the second bracket to the opposite side.

Note Only three of the four holes on each bracket are used (top, left, and right).

Step 3 Put tamper-evident labels over the bottom panel.

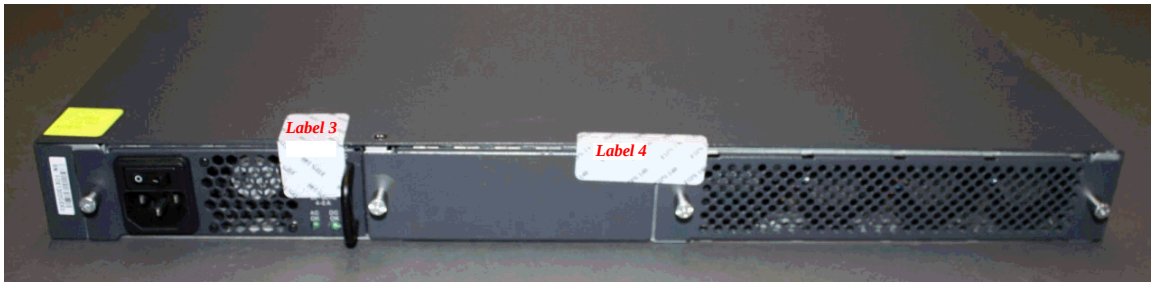
Step 4 Attach the opacity shield over the front face.

Step 5 Place one seal each over the left and right side mounting brackets, for a total of two (2) labels (see Figure 2). These protect the front opacity shield from removal. The two (2) seals on the rear protect any components from being removed without tamper evidence (see Figure 3). All four seals protect against the removal or prying open of the top cover to expose the module's interior.

Note If replacement of the tamper evident labels is deemed necessary, please reference FIPS kit AIRLAP-FIPSKIT=, version B0.

Figure 2 Placement of Tamper-evident Labels on Mounting Brackets

Figure 3 Placement of Tamper-evident Labels (Rear View)



Secure Configuration

Configuration of the module shall be performed only over a local link via the console connection.

Only the 7.0.240.0 Cisco Unified Wireless Network controller software version may be loaded on the WLAN controllers for distribution to access points.

Follow these steps to prepare the secure configuration for the module:

1. Enable FIPS Mode of Operations
2. Disable Boot Break
3. Configure HTTPS Certificate
4. Configure Authentication Data
5. Configure Communications with RADIUS
6. Configure Pre-shared Keys for 802.11i

7. Configure Ciphersuites for 802.11i
8. Configure SNMP
9. Configure TACACS+ secret
10. Configure MFP (Management Frame Protection)
11. Configure Local EAP
12. Configure EAP-FAST
13. Configure EAP-TLS
14. Configure Data DTLS (optional)
15. Configure Data DTLS with Office Extend Access Points (optional)
16. Save and Reboot

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
```

After completing the steps, saving the configuration and rebooting, the Controller stays in FIPS mode unless the FIPS mode is explicitly disabled. The non-approved cryptographic algorithms do not get used in FIPS mode unless they are explicitly configured.

To view the current mode of operation, the following CLI command needs to be used:

```
> show switchconfig
```

If the controller is in FIPS mode, the following will be displayed:

```
FIPS prerequisite features..................... Enabled
```

In FIPS mode, an SP800-90 DRBG and an ANSI X9.31 PRNG are used to generate random numbers on the Controller. In non-FIPS mode, a FIPS 186-2 based PRNG is used in place of the SP800-90 DRBG; the ANSI X9.31 PRNG also gets used in non-FIPS mode.

Disable Boot Break

The following CLI command prevents breaking out of the boot process. It must be executed after enabling FIPS mode of operations.

```
> config switchconfig boot-break disable
```

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
```

In non-FIPS mode, a self-signed certificate may be used for the HTTPS server.

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.

In non-FIPS mode, the password must contain 3 or more characters.

Configure Communications with RADIUS

Communications between the controller and RADIUS in FIPS mode may be configured for RADIUS KeyWrap or IPSec. In non-FIPS mode, this is optional.

RADIUS KeyWrap and MACK Keys

The following CLI commands configure the RADIUS 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
```

IPSec

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

If IPSec is used in FIPS mode, the message authentication protocol needs to be configured as HMAC-SHA1 and the encryption needs to be configured as 3DES. When used in non-FIPS mode, HMAC-MD5 is also an option for message authentication; the encryption may be AES or DES or none.

Configure Pre-shared Keys for 802.11i

WPA2 Pre-shared key (WPA2-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 set-key hex key index
> config wlan security wpa akm psk enable index
```

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

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
```

Configure SNMP

Non-security related remote monitoring and management of the Controller can be done via SNMP. No CSPs are entered or output via SNMP. 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.

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 [none|des] authkey encryptkey
```

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.

Configure MFP (Management Frame Protection)

Infrastructure MFP enables one access point to validate a neighboring Access Point's management frames. Configuring the module to use MFP is optional. The following CLI command is used to enable infrastructure MFP:

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

Client MFP is used to encrypt and sign management frames between the AP and the client. The following CLI command is used to enable client MFP:

```
> config wlan mfp client enable index required
```

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

Configure Local EAP

The module can be optionally configured in FIPS and non-FIPS modes as a local EAP authentication server to authenticate wireless clients. EAP-TLS and EAP-FAST are supported and permitted by this security policy.

Refer to the Cisco Wireless LAN Controller Configuration Guide for instructions on configuring Local EAP server to authenticate wireless clients without a RADIUS server.

Configure EAP-FAST

EAP-FAST is an Extensible Authentication protocol and can be used as an authentication method between the Controller and the wireless client. When a RADIUS server is used to authenticate clients, no extra EAP-FAST configuration is required.

When the Controller is configured as an EAP-FAST authentication server, the following CLI command is used by the crypto officer to enter a new EAP-FAST server key, where hex-key can be up to 32 hex digits or 16 bytes.

```
> config local-auth method fast server-key hex-key
```

Refer to the Cisco Wireless LAN Controller Configuration Guide for instructions on configuring Local EAP server with EAP-FAST as the authentication method for the wireless clients.

Configure EAP-TLS

EAP-TLS is an Extensible Authentication protocol and can be used as an authentication method between the Controller and the wireless client. When a RADIUS server is used to authenticate clients, no extra EAP-TLS configuration is required.

When the Controller is configured as an EAP-TLS authentication server, it requires configuration based on certificates issued from a PKI. Refer to the Cisco EAP-TLS Deployment Guide for Wireless LAN Networks configuration instructions to use EAP-TLS as the authentication method for the wireless clients.

Click this URL for an example configuration:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080851b42.shtml

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:

Step 1 To enable or disable data encryption for all access points or a specific access point, enter this command:

```
> config ap link-encryption {enable | disable} {all | Cisco_AP}
```

Step 2 When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter

```
> Y
```

Step 3 To save your changes, enter this command:

```
> save config
```

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

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:

Step 1 To enable hybrid-REAP on the access point, enter this command:

> **config ap mode h-reap** *Cisco_AP*

Step 2 To configure one or more controllers for the access point, enter one or all of these commands:

> **config ap primary-base** *controller_name Cisco_AP controller_ip_address*

> **config ap secondary-base** *controller_name Cisco_AP controller_ip_address*

> **config ap tertiary-base** *controller_name Cisco_AP controller_ip_address*

Step 3 To enable the OfficeExtend mode for this access point, enter this command:

> **config hreap office-extend** {**enable** | **disable**} *Cisco_AP*

Step 4 To save your changes, enter this command:

> **save config**

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

Save and Reboot

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

```
> save config
> reset system
```

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

The module supports these four roles:

- 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.

Services

The services provided are summarized in Table 2.

Table 2 Module Services

Service	Role	Purpose
Self Test and Initialization	CO	Cryptographic algorithm tests, firmware integrity tests, module initialization.
Firmware Update	CO	Upgrade firmware to new release version.
System Status	User or CO	The LEDs show the network activity and overall operational status and the command line status commands output system status.
Key Management	CO	Key and parameter entry, key output, key zeroization.
Module Configuration	CO	Selection of non-cryptographic configuration settings.
SNMPv3	CO	Non security related monitoring by the CO using SNMPv3.
TACACS+	User or CO	User & CO authentication to the module using TACACS+.
IPSec	User or CO	Secure communications between controller and RADIUS
CAPWAP	AP	Establishment and subsequent data transfer of a CAPWAP session for use between the module and an access point.[1]
MFP	AP	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.
TLS	CO	Establishment and subsequent data transfer of a TLS session for use between the module and the CO.
Local EAP Authenticator	Client	Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller.
802.11i	AP	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point.
RADIUS KeyWrap	Any	Establishment and subsequent receive 802.11i PMK from the RADIUS server.

Table 2 Module Services (continued)

Service	Role	Purpose
DTLS data encrypt	CO	Enabling optional DTLS data path encryption for Office Extend APs.[2]
TLS for syslog messages	CO	Establishment of TLS tunnel for the protection of syslog messages.

1. CAPWAP uses RSA key wrapping which provides 112 bits of effective symmetric key strength.
2. For further DTLS data configuration information, see the *Cisco Wireless LAN Controller Configuration Guide.*

The module does not support a bypass capability in the approved mode of operations.

User and CO Authentication

When a user first connects to the module via console port, the module prompts the user to enter a username and password. The user is authenticated based on the password provided. Once the user has been authenticated, the module provides services to that user based on whether they have read-only privileges (the user role) or read-write privileges (the CO role). The "*" characters are used to mask user password when the users authenticate. If the incorrect password is entered, the module will re-prompt the user to login again. After the module power cycles, a user must reauthenticate.

The module supports password based local authentication for access via the CLI or HTTPS, as well as remote authentication using RADIUS and TACACS+. The module also supports remote access via SNMPv3. All SNMP traffic to and from the module is considered unprotected. RADIUS, TACACS+ and SNMPv3 may be used in the FIPS mode.

The security policy stipulates that all user passwords must be 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

AP Authentication

The module performs mutual authentication with an access point through the CAPWAP protocol, using an RSA key pair with 2048-bit modulus, which has an equivalent symmetric key strength of 112 bits. An attacker would have a 1 in 2^{112} 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 $5.2x10^{28}$ attempts per minute, which far exceeds the operational capabilities of the module 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 bit to 2048 bit, thus providing between 80 bits and 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 1.8×10^{21} attempts per minute, which far exceeds the operational capabilities of the modules to support.

Ports and Interfaces

The module has the following physical ports and interfaces:

- 8 1000BaseT, 1000Base-SX and 1000Base-LH transceiver slots (data input, data output, status output, control input)
- LED indicators (status output)
- Console Port: RS232 (DB-9 male/RJ-45), mini-USB (control input, status output)
- Power Supply 1, Power Supply 2 (power input)
- Service Port: 10/100/1000 Mbps Ethernet (RJ45), not used in FIPS mode.
- Utility Port: 10/100/1000 Mbps Ethernet (RJ45), not used in FIPS mode.

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 MAC keys, and the Pre shared key (PSK) are input by the CO in plaintext over a local console connection. The PMK and NSK are 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. PAC key is output wrapped with the Client's RSA 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.

Table 3 lists the secret and private cryptographic keys and CSPs used by the module. Table 4 lists the public keys used by the module. Table 5 lists the access to the keys by service.

Table 3 Secret and Private Cryptographic Keys and CSPs

Name	CSP Type	Storage	Description
cscoDefaultIdCert	RSA	Flash	2048 bit RSA private key for the controller
DRBG Seed Material	SP800-90 DRBG	SDRAM	Seed material for the DRBG. Generated in hardware on the Cavium RNG.
DTLS Pre-Master Secret	Shared secret	SDRAM	Shared secret generated by approved RNG for generating the DTLS encryption key.
DTLS Encryption Key (CAPWAP Session Key)	AES-CBC	SDRAM	Session key used to encrypt and decrypt CAPWAP control messages.
DTLS Integrity Key	HMAC- SHA-1	SDRAM	Session key used for integrity checks on CAPWAP control messages.
DTLS Master Key	Shared Secret	SDRAM	Used to create the DTLS Encryption and Integrity Keys

Table 3 Secret and Private Cryptographic Keys and CSPs (continued)

Name	CSP Type	Storage	Description
802.11i Temporal Key (TK)	AES-CCM	SDRAM	AES-CCM key used in 802.11i broadcast communications
ANSI X9.31 PRNG Seed Key	NDRNG	SDRAM	Seed key for the PRNG
ANSI X9.31 PRNG Encryption Key	NDRNG	SDRAM	AES-128 Encryption key for the PRNG
AAA Shared Secret	Shared secret	Flash	Used to derive IPSec encryption keys and IPSec HMAC keys.
RADIUSOverIPSec EncryptionKey	TDES	SDRAM	TDES encryption/decryption key, used in IPSec tunnel between module and RADIUS to encrypt/decrypt EAP keys.
RADIUSOverIPSec IntegrityKey	HMAC	SDRAM	Integrity/authentication key, used in IPSec tunnel between module and RADIUS.
User Password	Shared secret	Flash	Identity-based authentication data for a user.
SNMPv3 Password	Shared secret	Flash	This secret is used to derive HMAC-SHA1 key for SNMPv3 authentication.
TACACS+ authentication secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate the Crypto-Officer's authentication requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant and the Crypto-Officer must ensure a strong user password.
TACACS+ authorization secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate the Crypto-Officers' operation's authorization requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant.
TACACS+ accounting secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate accounting requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant.
bsnOldDefaultIdCert	RSA	Flash	1536-bit RSA private key used to authenticate to the access point, generated during the manufacturing process.

Table 3 Secret and Private Cryptographic Keys and CSPs (continued)

Name	CSP Type	Storage	Description
VendorDeviceCert	RSA	Flash	Certificate to authenticate controller to EAP clients during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method.
HTTPS TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.
HTTPS TLS Encryption Key	AES-CBC	SDRAM	AES key used to encrypt HTTPS data.
HTTPS TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for HTTPS integrity protection.
Infrastructure MFP MIC Key	AES-CMAC	Flash	This 128-bit AES key is generated in the controller using approved SP800-90 DRBG. This key is sent to the AP encrypted with the DTLS encryption key. This key is used by the AP to sign management frames when infrastructure MFP is enabled.
Pre-Shared Key (PSK)	AES-CCM	Flash	The 802.11i pre shared key (PSK). This key is optionally used as a PMK.
802.11i Pairwise Master Key (PMK)	Shared secret	SDRAM	The PMK is a secret shared between an 802.11 supplicant and authenticator, and is used to establish the other 802.11i keys.
802.11i Key Confirmation Key (KCK)	HMAC- SHA-1	SDRAM	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.
802.11i Key Encryption Key (KEK)	AES-KeyWrap	SDRAM	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.
802.11i Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The PTK, also known as the CCMP key, is the 802.11i session key for unicast communications.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications.
RADIUS AES KeyWrap KEK	AES-KeyWrap	Flash	The key encrypting key used by the AES Key Wrap algorithm to protect the PMK for the 802.11i protocol.
RADIUS AES KeyWrap MACK	AES-KeyWrap	Flash	The MAC key used by the AES Key Wrap algorithm to authenticate RADIUS conversation.
EAP-TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new EAP-TLS session keys can be created.

Table 3 Secret and Private Cryptographic Keys and CSPs (continued)

Name	CSP Type	Storage	Description
EAP-TLS Encryption Key	AES-CBC	SDRAM	AES key used to encrypt EAP-TLS session data.
EAP-TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for EAP-TLS integrity protection.
EAP-TLS Peer Encryption Key	Shared secret	SDRAM	This 32-byte key is master session key of the EAP-TLS authentication algorithm. It is the PMK for 802.11i.
EAP-FAST Server Key	AES-CCM	Flash	EAP-FAST server master key to generate client protected access credential (PAC).
EAP-FAST PAC-Key	Shared secret	SDRAM	Shared secret between the local EAP authenticator and the wireless client. For EAP-FAST authentication. It is created by PRNG and is used to derive EAP-FAST tunnel master secret.
EAP-FAST tunnel master secret	Shared Secret	SDRAM	This is the master secret for EAP-FAST. It is used to derive EAP-FAST Encryption key, EAP-FAST Integrity key, EAP-FAST Session Key Seed.
EAP-FAST Encryption Key	AES-CBC	SDRAM	Encryption Key for EAP-FAST tunnel.
EAP-FAST Integrity Key	HMAC-SHA-1	SDRAM	Integrity Key for EAP-FAST tunnel.
EAP-FAST Session-Key Seed	Shared Secret	SDRAM	This secret is used to derive the EAP-FAST master session key by mixing with the EAP-FAST Inner Method Session Key.
EAP-FAST Inner Method Session Key	Shared Secret	SDRAM	This 32-byte key is the session key generated by the EAP handshake inside the EAP-FAST tunnel.
EAP-FAST Master Session Key	Shared Secret	SDRAM	This 64-byte key is the session key generated by the EAP-FAST authentication method. It is then used as PMK for 802.11i.
TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret used to generate new TLS session keys for syslog.
TLS Encryption Key	AES-CBC key	SDRAM	Symmetric AES key for encrypting syslog messages over TLS.
TLS Integrity Key	HMAC-SHA-1 key	SDRAM	Used for TLS integrity protection of syslog messages.

Table 4 Public Keys

Name	Algorithm	Storage	Description and Zeroization
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used for CAPWAP authentication.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, used to validate the controller's firmware image.
bsnDefaultCaCert	RSA	Flash	Verification certificate, used for CAPWAP authentication.
bsnDefaultBuildCert	RSA	Flash	Verification certificate, used to validate the controller's firmware image.
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, used with CAPWAP to validate the certificate that authenticates the access point.
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the access point.
cscoDefaultDevCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the access point.
bsnOldDefaultIdCert	RSA	Flash	Authentication certificate, used to authenticate to the access point.
bsnSslWebadminCert	RSA	Flash	Server certificate used for HTTPS-TLS.
VendorCACert	RSA	Flash	Certificate to validate wireless clients certificates during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method.

Table 5 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes DRBG seed
System Status	• None
Firmware Update	• Upgrade firmware to new release version
Key Management	• Read/Write PSK, AAA Shared Secret, PSK, RADIUS AES KeyWrap KEK, RADIUS AES KeyWrap MACK, EAP-FAST Server Key • Destroy all keys (with Key Zeroization command)

Table 5 Key/CSP Access by Service (continued)

Service	Key Access
Module Configuration	• Modify user passwords • Modify TACACS+ shared secret
SNMPv3	• Authenticate using SNMPv3 user password
TACACS+	• Authenticate, authorize and accounting using TACACS+ shared secrets
IPSec	• Use AAA Shared Secret, RADIUSOverIPSecEncryptionKey, and RADIUSOverIPSecIntegrityKey
CAPWAP	• Verify with cscoDefaultNewRootCaCert and cscoDefaultMfgCaCert • Sign with cscoDefaultIdCert Private Key • Read (and transmit) cscoDefaultIdCert Certificate • Establish and then encrypt/decrypt with CAPWAP Session Key
MFP	• Derive Infrastructure MFP MIC key from DRBG and distribute to connected APs
HTTPS (TLS)	• Sign with bsnSslWebadminCert Private Key • Read (and transmit) bsnSslWebadminCert Public Key • Establish TLS Pre-Master Key • Establish and then perform cryptographic operations with TLS Encryption Key and TLS Integrity Key
Local EAP Authenticator (EAP-TLS)	• Sign with VendorDeviceCert Private Key • Read (and transmit) VendorCACert • Establish EAP-TLS tunnel Pre-master secret • Derives EAP-TLS Master secret and tunnel encryption & integrity keys • Derives EAP-TLS peer encryption Key

Table 5 Key/CSP Access by Service (continued)

Service	Key Access
Local EAP Authenticator (EAP-FAST)	In-band PAC Provisioning without certificates: • Establish EAP-TLS pre-master secret using anonymous Diffie Hellman key exchange • Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys • Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client In-band PAC Provisioning with certificates: • Sign with VendorDeviceCert Private Key • Read (and transmit) VendorCACert • Read and verify Client certificate • Establish EAP-TLS pre-master secret using authenticated Diffie Hellman key exchange • Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys • Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client EAP-FAST Tunnel Establishment: • Read EAP-Fast Server Key • Decrypt client PAC to recover client EAP-FAST PAC-Key • Derive EAP-FAST Master secret and tunnel encryption/integrity keys and EAP-FAST Session-Key Seed. Authentication: • Derive EAP-FAST Inner Method Session Key according to the inner EAP algorithm • Derive EAP-FAST Master Session Key using the Session-Key Seed and Inner Method Session Key(s).
802.11i	• Compute 802.11i KCK, 802.11i KEK and 802.11i PTK from 802.11i PMK or 802.11i PSK • Generate 802.11i GTK • Encrypt/decrypt using 802.11i KEK • Authenticate data using 802.11i KCK
DTLS data encrypt	• Use DTLS Master Secret to derive DTLS Encryption Key and DTLS Integrity Key • Use DTLS Encryption Key and DTLS Integrity Key

Table 5 Key/CSP Access by Service (continued)

Service	Key Access
RADIUS	• Decrypt 802.11i PMK using KeyWrap KEK • Authenticate data using KeyWrap MACK
TLS for syslog messages	• Establish TLS tunnel Pre-Master Secret • Derives TLS Encryption Key and TLS Integrity Key

Key Zeroization

To switch the controller from either FIPS Approved mode to Non-FIPS Approved mode, or from Non-FIPS Approved mode to FIPS Approved mode, the CO shall zeroize the module, thus zeroizing all keys in the module, by entering this CLI command from a PC connected to the console port:

```
> config switchconfig key-zeroize controller
```

After this step, power cycle the module and hold down the escape key to initiate a memory test that will clear any residual keys from the RAM.

Disallowed Security Functions

These cryptographic algorithms are not approved and may not be used in FIPS mode of operations:

- RC4
- MD5
- HMAC MD5 (permitted for use in the TLS/DTLS PRF)
- AES-CTR (non-compliant)
- CCKM
- Diffie-Hellman (non-compliant; less than 80 bits of encryption strength)
- FIPS 186-2 RNG (Cert. #741) (No security claimed)

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of AES-CBC, AES-ECB, AES-CCM, SHA-1, HMAC SHA-1, RNG, TDES, EAP-FAST KDF, and RSA algorithms
- Continuous random number generator test for Approved and non-Approved RNGs
- Firmware update test using RSA

Self Tests are performed automatically when power is applied to the module. Self Tests may be run on-demand at any time by cycling power to the module.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at this URL:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2010-2013 Cisco Systems, Inc. All rights reserved.