FIPS 140-2 Security Policy for Cisco Catalyst 3750G Integrated Wireless LAN Controller

May 3, 2011
Version 2.3

Contents

This security policy contains these sections:

- Overview, page 2
- Physical Security, page 3
- Secure Configuration, page 5
- Roles, Services, and Authentication, page 9
- Ports and Interfaces, page 10
- Cryptographic Key Management, page 11
- Disallowed Security Functions, page 18
- Self Tests, page 18
- Mitigation of Attacks, page 19
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 19

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco Catalyst 3750G Integrated Wireless LAN Controllers support support 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. DTLS is essentially TLS over datagram (UDP) transport. WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i standard.

It 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 data 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.

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 1536 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, compliant with all requirements of FIPS 140-2 Level 2 and Level 3 requirements for Design Assurance.

Cisco Catalyst 3750G Integrated Wireless LAN controller consists of a 3750 Catalyst switch and a 4402 Wireless Controller. The cryptographic boundary of the module includes all hardware and firmware. The 3750 Catalyst switch hardware and firmware is excluded from the FIPS requirements as it does not perform any security relevant services and hence does not affect the overall security of the module.

The evaluated platform consists of model number WS-C3750G, and hardware Version ID is M0. The 3750G FIPS Kit (P/N 69-1707-01) includes the opacity shield, screws, a cap for the mode button and tamper evident seals. The 4402 controller in the module runs CAPWAP version 7.0.98.0, 7.0.98.213 or 7.0.116.0 firmware. In the FIPS mode of operations, the module supports the following cryptographic algorithm implementations:

- AES (AES Cert. #1344, key wrapping; key establishment methodology provides 128 bits of encryption strength)
- AES-CBC (firmware)
- AES-ECB (firmware)
- AES-CCM (firmware)
- SHA-1 (firmware)
- HMAC SHA-1 (firmware)
- FIPS 186-2 Random Number Generator (firmware)
- RSA (key wrapping; key establishment methodology provides 96 bits of encryption strength)
- RSA signature generation and verification (firmware)
- TDES (firmware)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (used to seed the Approved RNG)

The module is interoperable with all FIPS 140-2 validated wireless LAN clients that support the ratified IEEE 802.11i standard. This security policy is non-proprietary and may be freely shared.

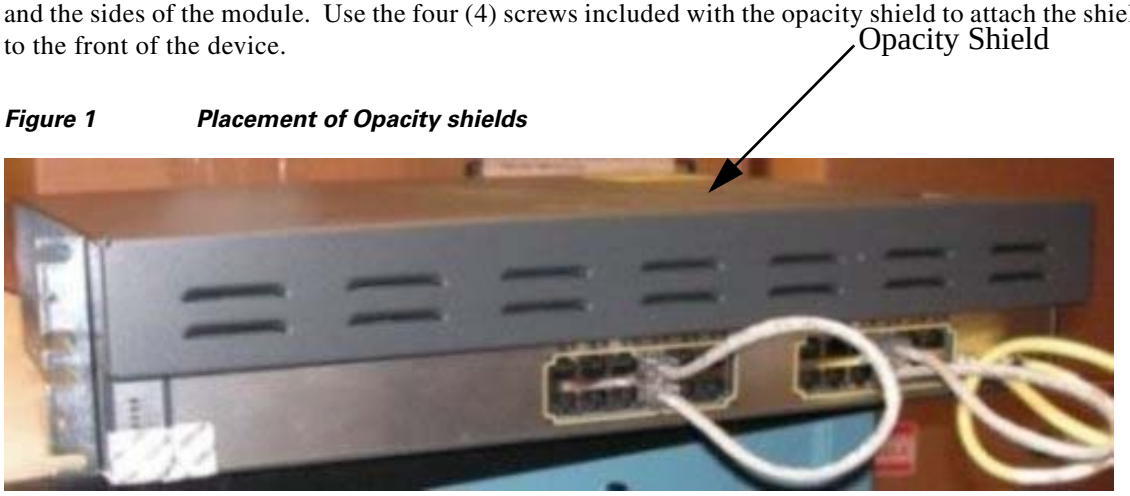
This document details the security policy for the module.

Physical Security

Note To operate in FIPS Approved mode the physical security devices shall be installed as indicated.

The Crypto Officer is responsible for the application and maintenance of the physical security mechanisms in order to remain in a FIPS-approved mode of operation. One (1) opacity shield must be placed on the front side of the module as shown in Figure 1 to cover the ventilation holes on the front and the sides of the module. Use the four (4) screws included with the opacity shield to attach the shield to the front of the device.

Figure 1 Placement of Opacity shields



One (1) cap must be placed on the mode button in order to prevent it from being pressed. Figure 2 shows the placement of the cap.

Figure 2 Placement of cap on the mode button

Put one (1) tamper evident label over the cap of the mode button, one (1) over the serial port of the switch, one (1) over the service port, three (3) over the stack ports, a total of four (4) over each of the opacity baffle screws, two (2) on the right side at the opacity shield and removable cover, and two (2) on the left side at the opacity shield and removable cover as shown in Figures 3 through 6.

Figure 3 Placement of Tamper evident label on the cap of the mode button

Figure 4 Placement of Tamper evident labels over the serial port, service port, and stack ports

Figure 5 Placement of Tamper evident labels over the opacity shield and the removable cover

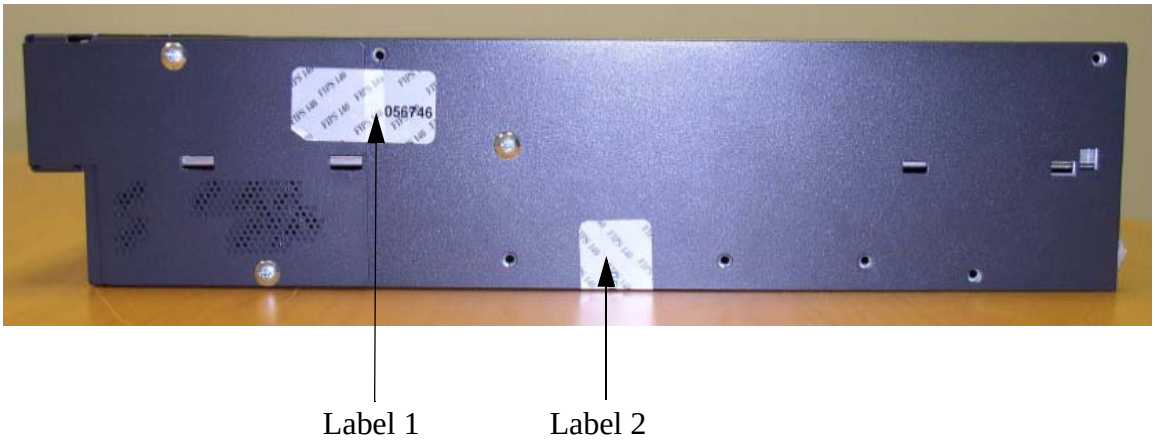
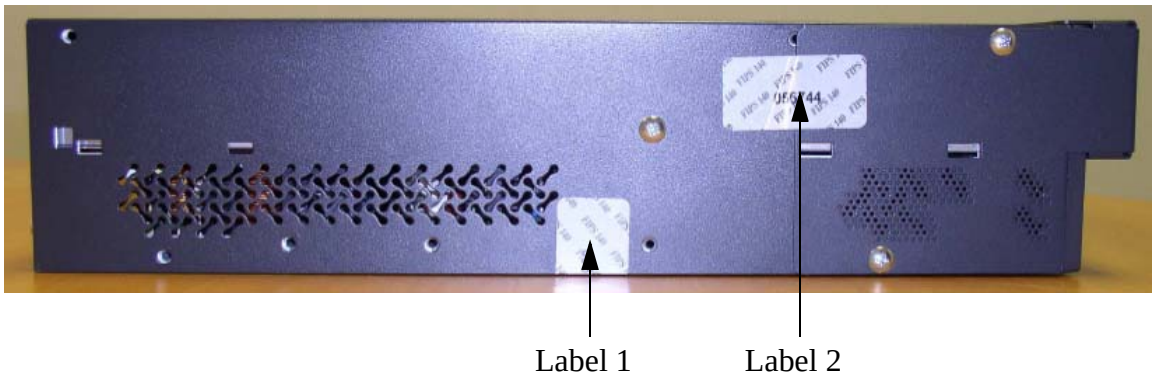


Figure 6 Placement of Tamper evident labels over the opacity shield and the removable cover



Secure Configuration

The configuration of the controller in the module is performed over a local link through the local console access of CLI of the controller. The Crypto Officer must ensure that the PC that is used for the console connection is a stand-alone or non-networked PC. After the first three steps below, remote access through HTTPS may be used for subsequent configuration. For connecting using HTTPS, the Crypto Officer shall configure their web browsers so that only TLS v1.0 is used. The HTTPS client must be configured to use AES_128_CBC_SHA based cipher suites.

Only the CAPWAP version 7.0.98.0, 7.0.98.213 or 7.0.116.0 may be loaded on the wireless LAN controller within the module 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 for the Controller
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. Save and Reboot

Enable FIPS Mode of Operations

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

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

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 in the module 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
```

Configure Authentication Data for the Controller

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

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

All subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document.

Configure Communications with RADIUS

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

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

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 the should be entered as 64 hexadecimal values (256 bits) using 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 the controller configuration guide for further 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 module can be done 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 accouting (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 controller in the module can be optionally configured as a local EAP authentication server to authenticate wireless clients. Both 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.

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
```

For further instructions on configuring Local EAP server with EAP-FAST or EAP-TLS as the authentication method for the wireless clients, refer to the instructions at:

http://www.cisco.com/en/US/tech/tk722/tk720/technologies_configuration_example09186a00807bf3c8.shtml and

http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a00807917a6.shtml

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. 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

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 roles:

- AP Role—This role is filled by an access point associated with the controller in the module.
- Client Role—This role is filled by a wireless client associated with the controller in the module.
- 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.
- Controller 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 1.

Table 1 Module Services

Service	Role	Purpose
Self Test and Initialization	Any role except AP and Client role	Cryptographic algorithm tests, firmware integrity tests, module initialization.
System Status	Any role except AP and Client role	The LEDs show the network activity and overall operational status, and the command-line status commands output system status.
Key Management	Controller CO	Key and parameter entry, key output, key zeroization.
Module Configuration	Controller CO	Selection of non-cryptographic configuration settings.
SNMPv3	Controller CO	Non security-related monitoring by the CO using SNMPv3.

Table 1 Module Services (continued)

Service	Role	Purpose
TACACS+	Controller CO, Controller User	User and CO Authentication to the module using TACACS+
IPSec	Controller CO, Controller User	Secure communication between the controller and RADIUS.
CAPWAP	AP	Establishment and subsequent data transfer of an CAPWAP session for use between the module and an AP[1].
MFP	AP	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.
TLS	Controller 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 in the module.
802.11i	AP	Establishment and subsequent data transfer of an 802.11i context for use between the client and the access point.
RADIUS KeyWrap	Controller CO, Controller User	Establishment and subsequent receive 802.11i PMK from the RADIUS server.

1. CAPWAP uses RSA key wrapping which provides 96 bits of effective key strength.

An unauthenticated operator may observe the System Status by viewing the LEDs on the module which show network activity and overall operational status. The module does not support a bypass capability in the approved mode of operations.

The only services available to an unauthenticated user are Self Test and Initialization (by power cycling the unit) and viewing System Status (by observing the LEDs).

Ports and Interfaces

The module has the following physical ports and interfaces:

- 24 10/100/1000 Ethernet ports
- Controller console serial port
- Two Small Form-factor Pluggable (SFP) interfaces
- Power port/ RPS connector
- LEDs: The module has 8 LEDs: PoE LED, Stack LED, Speed LED, Duplex LED, Status LED, Master LED, RPS LED and System LED on the front panel that indicates the status of the various ports and overall operational status of the module. The status of the controller within the module is displayed by the status LED of the 3750 switch.

The ports protected by tamper-evident seals are not available in FIPS mode.

User and CO Authentication

When a Controller user first connects to the controller in the module through the console ports, the module prompts the user to enter a username and password. The Controller user is authenticated based on the password provided. Once this user has been authenticated, the module provides services to that user based on whether they have read-only privileges (the Controller user role) or read-write privileges (the Controller 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 re-authenticate.

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 non-crypto related remote access via the SNMPv3. RADIUS, TACACS+ and SNMPv3 may be used in the FIPS mode.

The security policy stipulates that all user passwords must contain 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords (for a character set of 36). 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 1536 bit modulus, which has an equivalent symmetric key strength of 96 bits. An attacker would have a 1 in 2^{96} 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 $7.9x10^{23}$ 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.

Cryptographic Key Management

Cryptographic keys are stored in plaintext form, in flash for long-term storage and in SDRAM (for active keys) of the controller in the module. 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 or in encrypted form when sent over the TLS session. 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 DTLS (CAPWAP) pre-master 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 DTLS (CAPWAP) encryption 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 2 lists the secret and private cryptographic keys and CSPs used by the module. Table 3 lists the public keys used by the module. Table 4 lists the access to the keys by service.

Table 2 Secret and Private Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description
PRNG seed key	FIPS 186-2	Flash	This is the seed key for the PRNG. It is statically stored in the code.
PRNG seed	FIPS 186-2	SDRAM	This is the seed for the PRNG. It is generated using an un-approved RNG based on the controller's /dev/urandom device.
Controller User Password	Shared secret	Flash	Identity based authentication data for a user.
SNMPv3 user 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 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
bsnDefaultIdCert	RSA	Flash	1536-bit RSA private key, not used in FIPS mode.
bsnSslWebadminCert	RSA	Flash	1536-bit RSA private key used for HTTPS-TLS, generated during the manufacturing process.
bsnSslWebauthCert	RSA	Flash	1024-bit RSA private key, not used in FIPS mode.
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.
Pre-shared key (PSK)	AES-CCM	Flash	The 802.11i preshared key (PSK). This key is optionally used as a PMK.
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	128-bit AES key used to encrypt HTTPS session data.
HTTPS TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for HTTPS integrity protection.
DTLS Pre-Master Secret	Shared secret	SDRAM	Shared secret generated by an AP and entered wrapped by the AP's RSA key. Used to derive the DTLS Master Secret.
DTLS Master Secret	Shared secret	SDRAM	Used to create the DTLS Encryption and Integrity Keys
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.
AAA Shared Secret	TDES	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.
Infrastructure MFP MIC Key	AES-CMAC	Flash	This 128-bit AES key is generated in the controller using FIPS 186-2 approved RNG. This key is sent to the AP encrypted with the DTLS Encryption Key. This key is used by AP to sign management frames when infrastructure MFP is enabled.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
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 Temporal Key (TK)	AES-CCM	SDRAM	AES-CCM key used in 802.11i 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.
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.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
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.

Table 3 Public Keys

Name	Algorithm	Storage	Description
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.

Table 3 Public Keys (continued)

Name	Algorithm	Storage	Description
cscoDefaultR3CaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations.
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 client certificates during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method.

Table 4 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG seed
System Status	• None
Key Management	• Read/Write AAA Shared Secret, PSK, RADIUS AES KeyWrap KEK, RADIUS AES KeyWrap MACK, EAP-FAST Server Key • Destroy all keys (with Key Zeroization command)
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, RadiusOverIPSecIntegrityKey
CAPWAP	• Verify with cscoDefaultNewRootCaCert and cscoDefaultMfgCaCert • Sign with bsnOldDefaultIdCert Private Key • Read (and transmit) bsnOldDefaultCert Certificate • Establish and then encrypt/decrypt with CAPWAP Session Key
MFP	• Derive Infrastructure MFP MIC key from PRNG and distribute to connected access points
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

Table 4 Key/CSP Access by Service (continued)

Service	Key Access
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
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)

Table 4 Key/CSP Access by Service (continued)

Service	Key Access
802.11i	• Compute 802.11i KCK, 802.11i KEK, 80211.i TK, 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
RADIUS	• Decrypt 802.11i PMK using KeyWrap KEK • Authenticate data using KeyWrap MACK

Key Establishment

The module uses RSA key wrapping which provides 96 bits of effective key strength to establish 128-bit AES keys for DTLS. Keys are output from the module encrypted with the DTLS Encryption Key.

Key Zeroization

All keys in the module can be zeroized 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 **Escape** to initiate a memory test that clears 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 (MD5 is allowed for use in DTLS)
- HMAC MD5
- AES-CTR (non-compliant)
- CCKM

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of 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

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.

Mitigation of Attacks

The module provides mitigation against the following attacks:

- Protection against wireless denial of service attacks due to forged 802.11 management frames. When wireless clients and wireless infrastructure are enabled with MFP (Management Frame Protection) the system is protected against DoS attacks from exploited 802.11 management frames.
- Protection against rogue or unauthorized APs in joining the trusted network. The Cisco APs and Controllers support mutual authentication via x.509 certificates that are installed from the factory.
- Protection against MiTM attacks against AP control traffic. All control and bridging traffic between Controllers and APs is protected with AES-CCM encryption.

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:

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