



FIPS 140-2 Security Policy for Cisco Catalyst 6506, 6506-E, 6509, and 6509-E Switches with Wireless Services Modules-2 (WiSM-2) (Firmware Release 7.0.240.0)

Jan 08, 2014
Version 1.5

Contents

This security policy contains these sections:

- [Overview, page 2](#)
- [Secure Configuration, page 6](#)
- [Roles, Services, and Authentication, page 12](#)
- [Ports and Interfaces, page 14](#)
- [Cryptographic Key Management, page 15](#)
- [Disallowed Cryptographic Functions, page 23](#)
- [Self Tests, page 23](#)
- [Installing the Opacity Shield on Catalyst 6506, 6506-E, 6509 and 6509-E Switches, page 24](#)
- [Physical Security, page 27](#)
- [Mitigation of Attacks, page 34](#)
- [Obtaining Documentation and Submitting a Service Request, page 34](#)



Overview

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches together with the Wireless Services Module 2 (WiSM2) provide unparalleled security, mobility, redundancy, and ease of use for mission-critical wireless LANs (WLANs). The WiSM2 works in conjunction with Cisco Aironet® Series lightweight access points operating in CAPWAP mode to deliver a secure and unified wireless solution that supports data, voice, and video applications.

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches are multi-chip, standalone cryptographic modules containing a WiSM2 Module to perform the cryptographic operations and a supervisor blade to manage overall chassis configuration.

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
Design Assurance	3
Mitigation of Other Attacks	N/A

The WiSM2 module in conjunction with Cisco Aironet Series Access Points 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. The WiSM2 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-CCM encryption. CAPWAP protects all control and bridging traffic between trusted network access points and the module with DTLS encryption. In the FIPS mode of operation, the WiSM2 supports WPA2 (802.11i), HTTPS using TLS, CAPWAP, MFP, RADIUS KeyWrap (using AES Key wrapping), IPSec, Local-EAP, EAP-FAST, TACACS+ and SNMP, and uses the following approved 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)
- SP800-90 Block Cipher DRBG (firmware) (DRBG Cert. #289, uses AES with 256 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)

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.

This document details the security policy for the Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules (WiSM2s). This security policy may be freely distributed.

The tested platform consists of the following:

- Chassis Hardware Version
 - Catalyst 6506 switch
 - Catalyst 6506-E switch
 - Catalyst 6509 switch
 - Catalyst 6509-E switch
- Backplane Hardware Version
 - WS-C6506-E
 - WS-C6509-E
 - WS-C6506
 - WS-C6509
- WiSM2-specific FIPS Kit WS-SVCWISM2FIPKIT=
- Chassis-level FIPS Kit (includes chassis-level opacity shield and tamper labels)
 - P/N 800-27009 (Catalyst 6506 and Catalyst 6506-E switch chassis)
 - P/N 800-26335 (Catalyst 6509 and Catalyst 6509-E switch chassis)
- Supervisor Blade Hardware Version
 - WS-SUP720-3BXL
 - WS-SUP720-3B

- VS-S720-10G-3C or VS-S720-10G-3CXL
- Supervisor Blade Firmware Version
 - Cisco IOS Release 12.2.33SXJ
 - Cisco IOS Release 12.2.33SXJ1
 - Cisco IOS Release 12.2.33SXJ2
- WiSM2 Module Hardware Version
 - WS-SVC-WISM2-K9=
 - WS-SVC-WISM2-5-K9
 - WS-SVC-WISM2-5-K9=
 - WS-SVC-WISM2-3-K9
 - WS-SVC-WISM2-3-K9=
 - WS-SVC-WISM2-1-K9
 - WS-SVC-WISM2-1-K9=
- WiSM2 Module Firmware Version 7.0.240.0

This security policy describes how the listed Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with WiSM2 Modules meet the security requirements of FIPS 140-2, and describes how to operate the hardware devices in a secure FIPS 140-2 mode. The addition of any component not addressed by this FIPS 140-2 validation and not included in the boundary definition is considered out of scope and may affect the correct operation of the module. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the listed Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules (WiSM2s). This Security Policy document is non-proprietary and can be freely distributed.

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 this URL:

<http://csrc.nist.gov/cryptval/>

Cisco Catalyst 6506, 6506-E, 6509, and 6509-E Switches with WiSM2 Cryptographic Modules

The cryptographic boundary is defined as encompassing the following:

- The entire outer enclosure of the chassis
- One WiSM2 Module
- One Supervisor Blade (either SUP720-3B, SUP720-3BXL, VS-S720-10G-3C, or VS-S720-10G-3CXL)
- Opacity shield
- Slot covers

[Figure 1](#) and [Figure 2](#) below show the cryptographic boundary as the dark border around the module.

The chassis requires that a special opacity shield be installed over the intake-side air vents to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications. The tamper-evident seals and opacity

shield included in the FIPS Kit shall be installed for the module to operate in a FIPS Approved mode of operation. Detailed installation instructions for the opacity shield and the application of the tamper evident seals are provided in this publication.

Figure 1 *Cryptographic Boundary on Catalyst 6506 and Catalyst 6506E Switches*

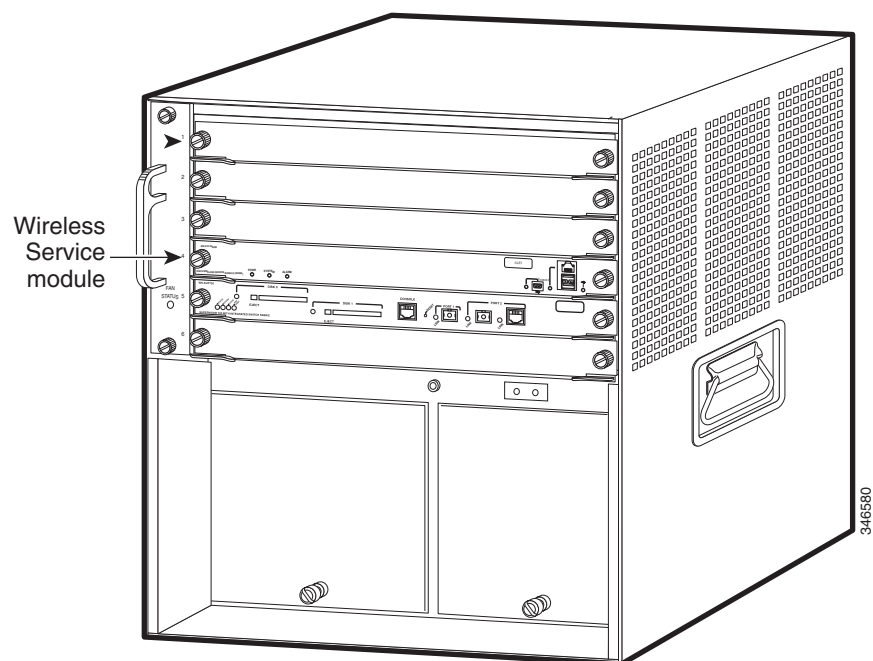
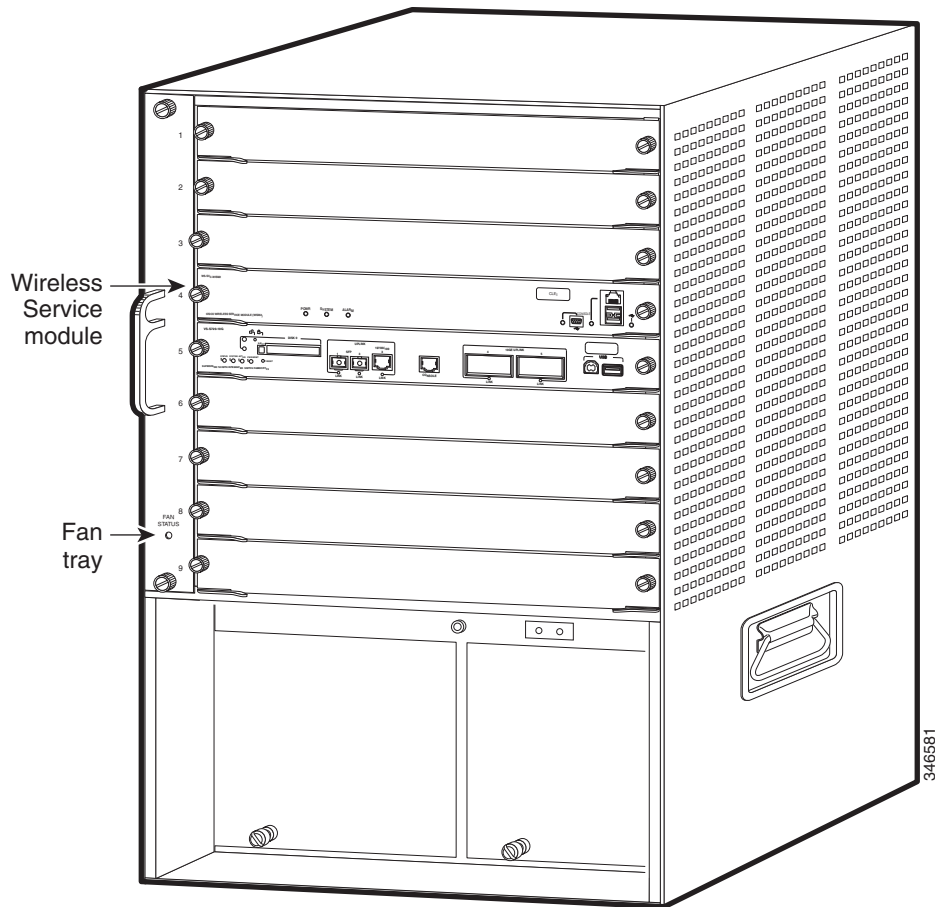


Figure 2 *Cryptographic Boundary on Catalyst 6509 and Catalyst 6509E Switches*



Secure Configuration

The initial configuration of the Supervisor card is accomplished by creating a VLAN that defines the connection between the Supervisor card and the WiSM2 card and by creating authentication data as explained in the Configure Supervisor Authentication Data section.

The initial configuration of the WiSM2 is performed through the local access of CLI of the Supervisor and by initiating a session from the supervisor CLI to each of the controllers in the WiSM2. The rest of the configuration shall be performed over a local link through the console connection of each of the controllers in the WiSM2. 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 7.0.240.0 CAPWAP firmware releases may be contained on the wireless LAN controllers for distribution to access points.

Configure Supervisor Authentication Data

The Supervisor crypto officer (this role is defined in the Roles, Services and Authentication section) must create the enable password for the supervisor crypto officer role. The password must be at least eight characters (all digits, all lower and uppercase letters, and all special characters except '?' are accepted) and is entered when the crypto officer first engages the **enable** command. The crypto officer enters the following syntax at the # prompt:

```
# enable secret password
```

The crypto officer must always assign passwords (of at least eight characters) to users. Enter this command to set user passwords:

```
# username name password password
```

Follow these steps on each WiSM2 controller to securely configure 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 initiates the steps for placing the controller in FIPS approved mode of operations, and enabling all necessary algorithm restrictions. All necessary self-tests are carried out in both FIPS and non-FIPS modes.

```
> 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 three 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 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 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 Controllers 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 in FIPS and non-FIPS modes. 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 in FIPS and non-FIPS modes. 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. 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 the 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:

1. `save config`
2. `reset system`

# Roles, Services, and Authentication

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

## Roles

The module supports these six roles:

- AP Role—This role is filled by an access point associated with the controller in the WiSM2.
- Client Role—This role is filled by a wireless client associated with the controller in the WiSM2.
- 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 Crypto Officer must maintain security and control at all times of any unused tamper-evident labels. The product documentation refers to this role as a management user with read-write privileges.
- Supervisor Crypto Officer (CO) Role—This role performs the initial WiSM2 configuration by initiating a session to the WiSM2 through the local access of the switch (Supervisor) CLI. The Supervisor CO can zeroize the user passwords stored in the supervisor blade.
- Supervisor User Role—This role can perform basic supervisor user services and can view the status of the WiSM2 configuration from the Supervisor CLI by issuing the show commands.

The module does not support a maintenance role.

## Services

The services provided are summarized in [Table 2](#).

**Table 2**      **Module Services**

| Service                                    | Role                               | Purpose                                                                                                                       |
|--------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Firmware Update                            | CO                                 | Upgrade firmware to new release version.                                                                                      |
| 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                             | CO                                 | Key and parameter entry, key zeroization.                                                                                     |
| Module Configuration                       | CO, Supervisor CO                  | Selection of non-cryptographic configuration settings.                                                                        |
| Supervisor Authentication data Zeroization | Supervisor CO                      | Supervisor User passwords zeroization.                                                                                        |
| SNMPv3                                     | CO                                 | Non security-related monitoring by the CO using SNMPv3.                                                                       |
| TACACS+                                    | CO, User                           | User and CO Authentication to the module using TACACS+                                                                        |
| IPSec                                      | CO, User                           | Secure communication between the controller and RADIUS.                                                                       |
| CAPWAP                                     | AP                                 | Establishment and subsequent data transfer of a CAPWAP session for use between the module and an AP <sup>1</sup> .            |
| 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.                            |
| DTLS Data Encryption                       | CO                                 | Enabling optional DTLS data path encryption for Office Extend APs                                                             |
| Local EAP Authenticator                    | Client                             | Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller in the WiSM2.                 |
| 802.11i                                    | AP                                 | Establishment and subsequent data transfer of an 802.11i context for use between the client and the access point.             |
| RADIUS KeyWrap                             | CO, User                           | Establishment and subsequent receive 802.11i PMK from the RADIUS server.                                                      |
| TLS for syslog messages                    | CO                                 | Establishment of TLS tunnel for the protection of syslog messages                                                             |

**Table 2**      **Module Services (continued)**

| Service | Role | Purpose                                 |
|---------|------|-----------------------------------------|
| SSH     | CO   | Remote administration of the controller |
| Telnet  | CO   | Remote administration of the controller |

1. CAPWAP uses RSA key wrapping which provides 112 bits of effective symmetric key strength.

These services are not FIPS compliant:

- TACACS+
- SNMPv3
- SSH
- Telnet

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

After applying the tamper-evident labels, the Cisco Catalyst series switch modules have the following physical ports and interfaces available:

- WISM2:
  - USB CONSOLE port
  - RJ-45 CONSOLE port
  - Status LEDs
- WS-SUP720-3B:
  - CONSOLE port
  - Disk, Link, and Status LEDs
- VS-S720-10G-3C:
  - CONSOLE port
  - Disk, Link, and Status LEDs

## Supervisor User and Supervisor CO Authentication

When a Supervisor User tries to connect to the CLI of the Supervisor via the Console port, the module prompts the Supervisor User to enter a password. The Supervisor User is authenticated based on the password provided. Once the user has been authenticated, the module provides a basic set of services to that user.

The Supervisor Crypto Officer must first assume the Supervisor User role and then enter the "enable" command. The Supervisor CO will be prompted to enter another password in order to receive additional services that are reserved for the Supervisor Crypto Officer. The Supervisor CO will be authenticated if a correct password is provided to the module.

## User and CO Authentication

When a user first connects to the controllers in the WiSM2 module through the console ports, 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 based on whether they have read-only privileges (the User role) or read-write privileges (the CO role).

The "\*" characters are used to mask the password when the users authenticate. If the incorrect password is entered, the module will re-prompt the user to login.

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 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 be 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

Each controller of the WiSM2 module in the Cisco Catalyst series switch 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  $5.2 \times 10^{28}$  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  $1.8 \times 10^{21}$  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 controllers in the WiSM2 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 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.

Dynamically generated keys are not shared between modes.

The module uses RSA key wrapping with 2048 bit modulus and provides 112 bits of encryption strength in key establishment.

**Table 3** Secret and Private Cryptographic Keys and CSPs

| Name                          | CSP Type         | Storage          | Description                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DRBG Seed Material            | SP800-90<br>DRBG | SDRAM            | Seed material for the DRBG. Generated in hardware on the Cavium RNG.                                                                                                                                                                                                                                                                                |
| ciscoDefaultIdCert            | RSA              | Flash            | 2048 bit RSA private key for the 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-SHA 1 key for SNMPv3 authentication.                                                                                                                                                                                                                                                                             |
| Supervisor user password      | Shared secret    | Supervisor NVRAM | The plaintext password for the Supervisor User.                                                                                                                                                                                                                                                                                                     |
| Enable password               | Shared secret    | Supervisor NVRAM | The plaintext password for the Supervisor Crypto Officer.                                                                                                                                                                                                                                                                                           |
| 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.                                                |



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

| Name                                     | CSP Type      | Storage | Description                                                                                                                                                                                                                                                      |
|------------------------------------------|---------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                   |
| bsnDefaultIdCert                         | RSA           | Flash   | 1536-bit RSA private key used to authenticate to the access point, generated during the manufacturing process.                                                                                                                                                   |
| bsnSslWebadminCert                       | RSA           | Flash   | 2048-bit RSA private key used for HTTPS-TLS, generated during the manufacturing process.                                                                                                                                                                         |
| 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)                     | Shared secret | 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 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 Key                          | 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                        | 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.                                                                                                                                                      |

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

| Name                                 | CSP Type      | Storage | Description                                                                                                                                                                                                                               |
|--------------------------------------|---------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 approved SP800-90 DRBG. 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. |
| 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.                                                                                                                                |

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

| Name                              | CSP Type       | Storage | Description                                                                                                                                                                        |
|-----------------------------------|----------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                              |
| ANSI X9.31 PRNG Seed Key          | ANSI X9.31     | SDRAM   | Seed key for the PRNG.                                                                                                                                                             |
| ANSI X9.31 PRNG Encryption Key    | ANSI X9.31     | SDRAM   | AES-128 Encryption key for the PRNG.                                                                                                                                               |

**Table 4**      **Public Keys**

| <b>Name</b>              | <b>CSP Type</b> | <b>Storage</b> | <b>Description</b>                                                                                                                           |
|--------------------------|-----------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| bsnOldDefaultCaCert      | RSA             | Flash          | Verification certificate, used for CAPWAP authentication.                                                                                    |
| bsnDefaultRootCaCert     | RSA             | Flash          | Verification certificate, used for CAPWAP authentication.                                                                                    |
| bsnDefaultCaCert         | RSA             | Flash          | Verification certificate, used for CAPWAP authentication.                                                                                    |
| bsnDefaultBuildCert      | RSA             | Flash          | Verification certificate, used to validate the controller's firmware image.                                                                  |
| cscsDefaultNewRootCaCert | RSA             | Flash          | Verification certificate, used with CAPWAP to authenticate the access point.                                                                 |
| cscsDefaultMfgCaCert     | RSA             | Flash          | Verification certificate, used with CAPWAP to authenticate the access point.                                                                 |
| cscsDefaultDevCaCert     | 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 client certificates during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method. |

**Table 5**      **Key/CSP Access by Service**

| <b>Service</b>               | <b>Key Access</b>                                                                                                                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Self Test and Initialization | <ul style="list-style-type: none"> <li>Initializes DRBG seed</li> </ul>                                                                                                                                            |
| Firmware Update              | <ul style="list-style-type: none"> <li>Upgrade firmware to new release version</li> </ul>                                                                                                                          |
| System Status                | <ul style="list-style-type: none"> <li>None</li> </ul>                                                                                                                                                             |
| Key Management               | <ul style="list-style-type: none"> <li>Read/Write AAA Shared Secret, PSK, RADIUS AES KeyWrap KEK, RADIUS AES KeyWrap MACK, EAP-FAST Server Key</li> <li>Destroy all keys (with Key Zeroization command)</li> </ul> |
| Module Configuration         | <ul style="list-style-type: none"> <li>Modify user passwords</li> <li>Modify TACACS+ shared secret</li> </ul>                                                                                                      |

**Table 5 Key/CSP Access by Service**

| <b>Service</b>                                | <b>Key Access</b>                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisor Authentication<br>Data Zeroization | <ul style="list-style-type: none"> <li>Supervisor user passwords</li> </ul>                                                                                                                                                                                                                                           |
| SNMPv3                                        | <ul style="list-style-type: none"> <li>Authenticate using SNMPv3 user password</li> </ul>                                                                                                                                                                                                                             |
| TACACS+                                       | <ul style="list-style-type: none"> <li>Authenticate, authorize and accounting using TACACS+ shared secrets</li> </ul>                                                                                                                                                                                                 |
| IPSec                                         | <ul style="list-style-type: none"> <li>Use AAA Shared Secret, RadiusOverIPSecEncryptionKey, RadiusOverIPSecIntegrityKey</li> </ul>                                                                                                                                                                                    |
| CAPWAP                                        | <ul style="list-style-type: none"> <li>Verify with ciscoDefaultNewRootCaCert and ciscoDefaultMfgCaCert</li> <li>Sign with ciscoDefaultIdCert Private Key</li> <li>Read (and transmit) ciscoDefaultIdCert Certificate</li> <li>Establish and then encrypt/decrypt with CAPWAP Session Key</li> </ul>                   |
| MFP                                           | <ul style="list-style-type: none"> <li>Derive Infrastructure MFP MIC key from DRBG and distribute to connected access points</li> </ul>                                                                                                                                                                               |
| HTTPS TLS                                     | <ul style="list-style-type: none"> <li>Sign with bsnSslWebadminCert Private Key</li> <li>Read (and transmit) bsnSslWebadminCert Public Key</li> <li>Establish TLS Pre-Master Key</li> <li>Establish and then perform cryptographic operations with TLS Encryption Key and TLS Integrity Key</li> </ul>                |
| Local EAP Authenticator<br>(EAP-TLS)          | <ul style="list-style-type: none"> <li>Sign with VendorDeviceCert Private Key</li> <li>Read (and transmit) VendorCACert</li> <li>Establish EAP-TLS tunnel Pre-master secret</li> <li>Derives EAP-TLS Master secret and tunnel encryption &amp; integrity keys</li> <li>Derives EAP-TLS peer encryption Key</li> </ul> |

**Table 5**      **Key/CSP Access by Service**

| <b>Service</b>                     | <b>Key Access</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local EAP Authenticator (EAP-FAST) | <p>In-band PAC Provisioning without certificates:</p> <ul style="list-style-type: none"> <li>• Establish EAP-TLS pre-master secret using Non-SP 800-56A Compliant Diffie-Hellman key exchange</li> <li>• Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys</li> <li>• Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client</li> </ul> <p>In-band PAC Provisioning with certificates:</p> <ul style="list-style-type: none"> <li>• Sign with VendorDeviceCert Private Key</li> <li>• Read (and transmit) VendorCACert</li> <li>• Read and verify Client certificate</li> <li>• Establish EAP-TLS pre-master secret using authenticated Diffie-Hellman key exchange</li> <li>• Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys</li> <li>• Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client</li> </ul> <p>EAP-FAST Tunnel Establishment:</p> <ul style="list-style-type: none"> <li>• Read EAP-FAST Server Key</li> <li>• Decrypt client PAC to recover client EAP-FAST PAC-Key</li> <li>• Derive EAP-FAST Master secret and tunnel encryption/integrity keys and EAP-FAST Session-Key Seed.</li> </ul> <p>Authentication:</p> <ul style="list-style-type: none"> <li>• Derive EAP-FAST Inner Method Session Key according to the inner EAP algorithm</li> <li>• Derive EAP-FAST Master Session Key using the Session-Key Seed and Inner Method Session Key(s)</li> </ul> |
| 802.11i                            | <ul style="list-style-type: none"> <li>• Compute 802.11i KCK, 802.11i KEK, 80211.i TK, and 802.11i PTK from 802.11i PMK or 802.11i PSK</li> <li>• Generate 802.11i GTK</li> <li>• Encrypt/decrypt using 802.11i KEK</li> <li>• Authenticate data using 802.11i KCK</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DTLS data encrypt                  | <ul style="list-style-type: none"> <li>• Use DTLS Master Secret to derive DTLS Encryption Key and DTLS Integrity Key</li> <li>• Use DTLS Encryption Key and DTLS Integrity Key</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 5 Key/CSP Access by Service**

| Service                 | Key Access                                                                                                                                             |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS                  | <ul style="list-style-type: none"> <li>• Decrypt 802.11i PMK using KeyWrap KEK</li> <li>• Authenticate data using KeyWrap MACK</li> </ul>              |
| TLS for syslog messages | <ul style="list-style-type: none"> <li>• Establish TLS tunnel Pre-Master Secret</li> <li>• Derives TLS Encryption Key and TLS Integrity Key</li> </ul> |

## Key Establishment

The module uses RSA key wrapping which provides 112 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

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 you enter the command, power cycle the module and hold down the **Esc** key to initiate a memory test that clears residual keys from the RAM.

## Disallowed Cryptographic Functions

The Controller supports the following cryptographic algorithms that shall not be used in the FIPS approved mode of operation:

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

## Self Tests

The following power-on self tests are performed by the module:

- Firmware integrity test on the IOS and CAPWAP firmware.
- Power on self test of AES-CBC, AES-ECB, AES-CCM, SHA-1, HMAC SHA-1, SP800-90 DRBG, ANSI X9.31 RNG, FIPS186-2 RNG, TDES, EAP-FAST KDF, and RSA algorithms.

Power-on self Tests are performed automatically when power is applied to the module. Power-on self tests may be run on-demand at any time by cycling power to the module. Power-on self tests are Known Answer Tests or KATs.

The following conditional self tests are performed by the module:

- Continuous random number generator test for Approved and non-Approved RNGs.
- Firmware update test using RSA.

## Installing the Opacity Shield on Catalyst 6506, 6506-E, 6509 and 6509-E Switches

The Catalyst 6500 series opacity shield is designed to be installed while the system is operating without creating an electrical hazard or damage to the system. You will need some clearance between adjacent racks in order to perform this procedure. This procedure is applicable to the following Catalyst 6500 series switches:

- Catalyst 6506 switch
- Catalyst 6506-E switch
- Catalyst 6509 switch
- Catalyst 6509-E switch



### Note

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

Follow these steps to install an opacity shield on the Catalyst 6506, 6506-E, 6509 and 6509-E Switches:

- Step 1** The opacity shield is designed to be installed on a Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switch chassis that is already rack-mounted. If your Catalyst 6500 series switch chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the *Catalyst 6500 Series Switches Installation Guide*. If your Catalyst 6500 series switch chassis is already rack-mounted, proceed to [Step 2](#).
- Step 2** Open the FIPS kit packaging. The kit contains the following items:
- A packaged opacity shield assembly with installation hardware for the Catalyst 6506 and Catalyst 6506-E switch chassis (part number 800-27009).
  - A packaged opacity shield assembly with installation hardware for the Catalyst 6509 and Catalyst 6509-E switch chassis (part number 800-26335).
  - An envelope with 60 FIPS tamper-evidence labels.
  - An envelope containing a disposable ESD wrist strap.
- Step 3** Select the appropriate opacity shield kit for your system and set the other opacity shield kit aside.
- Step 4** Open the protective packaging and remove the opacity shield and the two bags of installation hardware. The bag with the part number 69-1482 contains the installation hardware for non-E chassis; the other bag (part number 69-1497) contains the installation hardware for -E chassis. Select the bag of installation hardware appropriate for your installation. Set the second bag of fasteners aside; you will not need them for this installation.
- Step 5** Open the bag of installation hardware and remove the following items:



- (Bag with part number 69-1482)—Two M3 thumbscrews, four M3 snap rivet fasteners. The snap rivet fasteners come assembled; you need to separate the two pieces of the snap rivet fastener by removing the snap rivet pin from the snap rivet sleeve before you install them in the opacity shield.
- (Bag with part number 69-1497)—Two M4 thumbscrews, four M4 snap rivet fastener sleeves, and four M4 snap rivet pins.

**Step 6** Start the two thumbscrews in the corresponding threaded holes in the opacity shield; two or three turns is sufficient. Do not thread the screws too far into the opacity shield. The opacity shield for the Catalyst 6509 or Catalyst 6509-E chassis is identified by a 6509-E that is silk-screened adjacent to several of the threaded holes; the opacity shield for the Catalyst 6506 or Catalyst 6506-E chassis is identified by a 6506-E that is silk-screened adjacent to several of the threaded holes.

Figure 3 shows how opacity shield is positioned on the 6506 or 6506-E switch. Figure x shows how opacity shield is positioned on the 6509 or 6509-E switch.

**Step 7** Open the envelope containing the disposable ESD wrist strap. Attach the disposable ESD wrist strap to your wrist. Attach the other end of the wrist strap to exposed metal on the chassis.

**Step 8** Position the opacity shield over the air intake side of the chassis so that the two thumbscrews on the opacity shield are aligned with the unused L-bracket screw holes on the chassis.

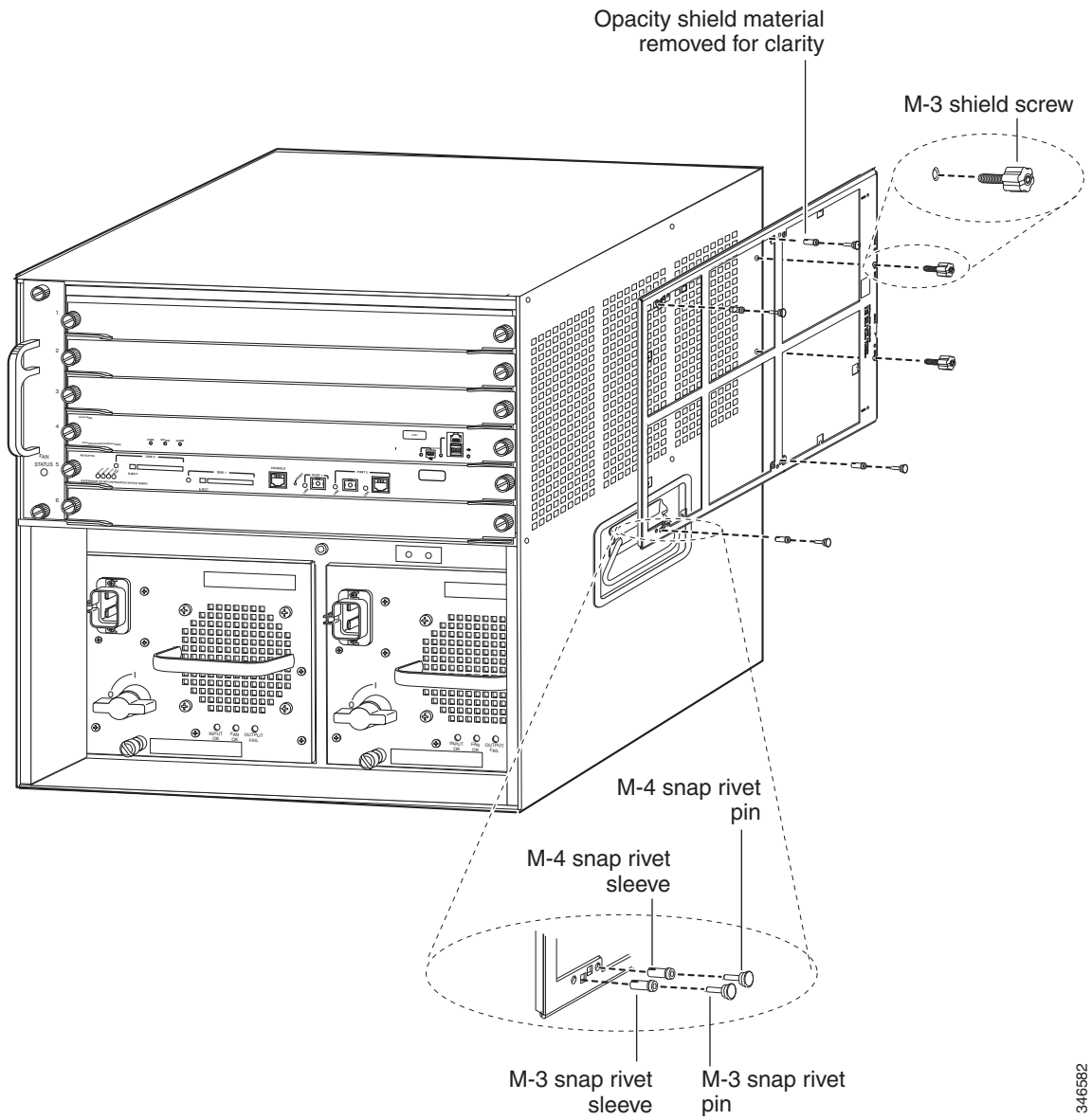
**Step 9** Press the opacity shield firmly against the air intake side of the chassis and hand tighten the two thumbscrews to secure the opacity shield to the chassis.

**Step 10** Position the rivet sleeve over either one of the square cutouts on the opacity shield (non-E chassis) or over the one of the round cutouts on the opacity shield (-E chassis). Press the rivet sleeve through the cutout, through the opacity shield material, and through one of the chassis air vent perforations.

**Step 11** Take the rivet pin and push it through the rivet sleeve until you hear a click.

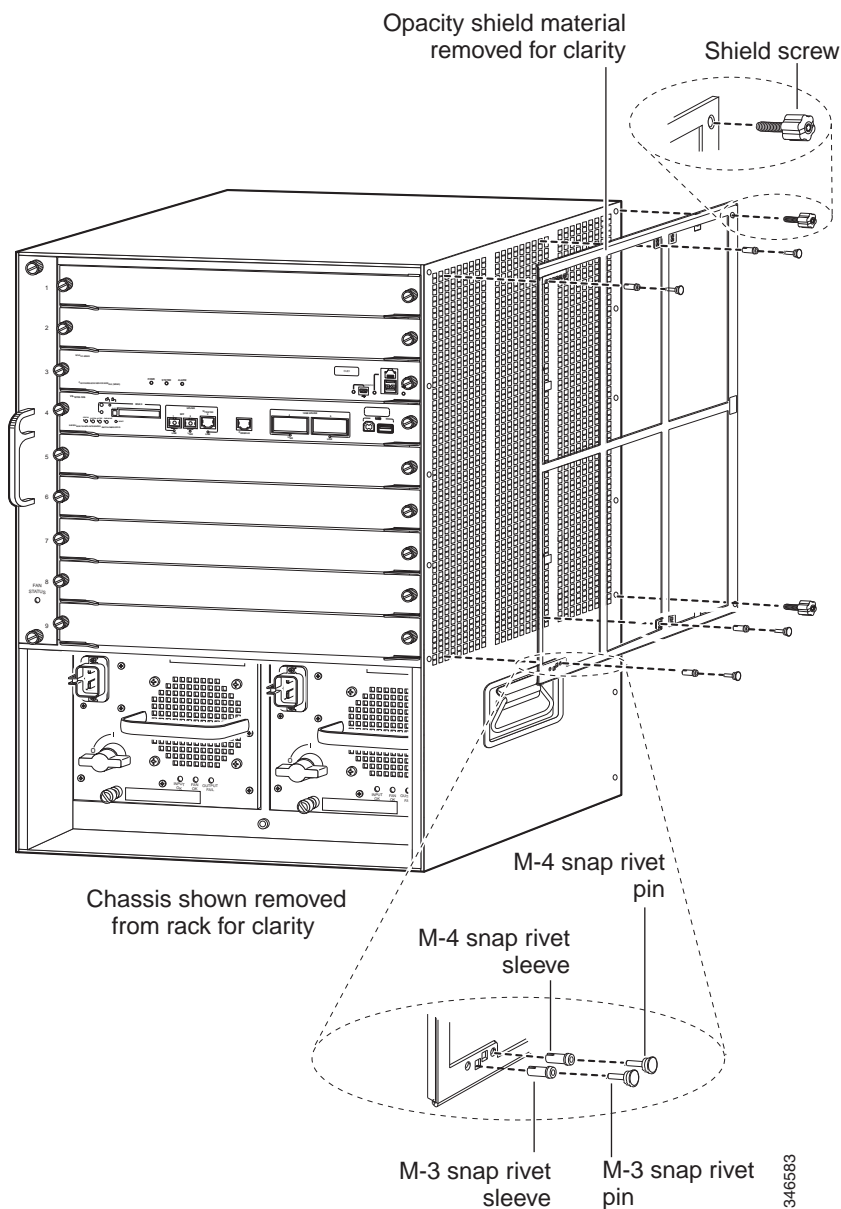
**Step 12** Repeat step 10 and step 11 for the remaining three snap rivet fasteners.

**Figure 3** Installing the Opacity Shield on the Catalyst 6506 or Catalyst 6506E Switch



346582

**Figure 4** Installing the Opacity Shield on the Catalyst 6509 or Catalyst 6509E Switch



## Physical Security

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches are entirely encased by a thick steel chassis. Nine module slots are provided on the Catalyst 6509 switch and Catalyst 6509-E switch and six module slots are provided on the Catalyst 6506 switch and Catalyst 6506-E switch. On-board LAN connectors and console connectors are provided on the supervisor blades, and console connectors are provided on the WiSM2s. The power cable connection and a power switch are provided on the power supply of all the models.

The Crypto Officer is responsible for the application and maintenance of the physical security policy. Verify that the Supervisor Blade is installed in chassis slot 5 and the WiSM2 is installed in chassis slot 4. Install slot covers over the remaining chassis slots. The slot covers are included with each chassis, and additional slot covers may be ordered from Cisco.

After the switch has been configured to meet FIPS 140-2 Level 2 requirements, the switch cannot be accessed without indicating signs of tampering. To seal the system with tamper-evidence labels, follow these steps:

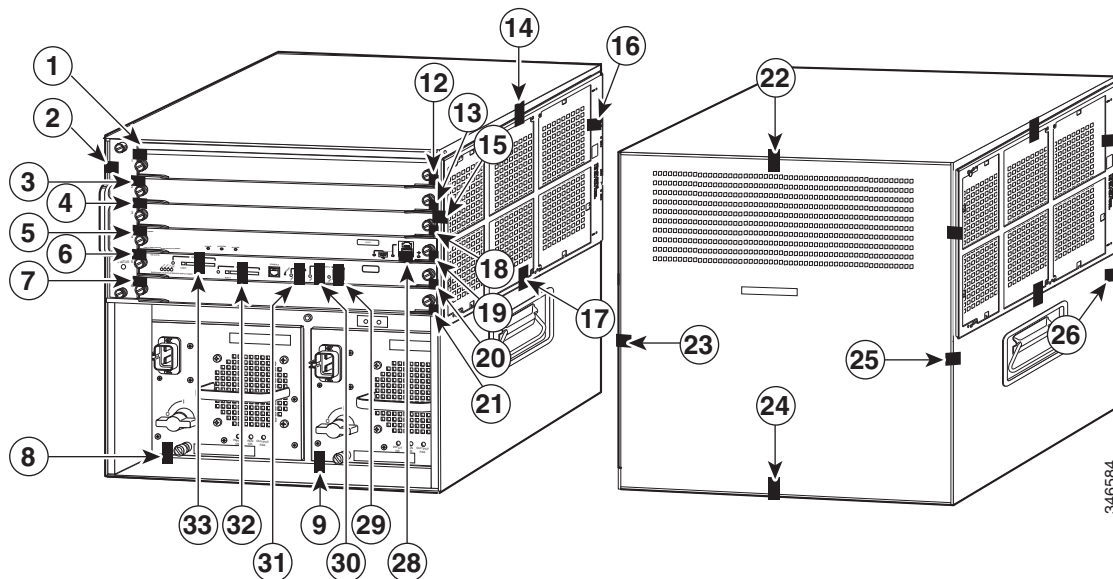
- 
- Step 1** Remove any grease, dirt, or oil from the cover by using alcohol-based cleaning pads before applying the tamper-evidence labels. The chassis temperature should be above 10° C (50° F).
- Step 2** Place labels on the chassis as shown in [Figure 5](#) and [Figure 6](#).
- a. Fan tray—The tamper-evidence label should be placed so that one half of the label adheres to the front of the fan tray and the other half adheres to the left side of the chassis. Any attempt to remove the fan tray will damage the tamper seal, which indicates tampering has occurred.
  - b. Modules—For each Supervisor Blade 720, WiSM2 Module or blank module cover installed in the chassis, place a tamper-evidence label so that one half of the label adheres to the module and the other half adheres to the right side of the chassis. Place another tamper-evidence label so that one half of the label adheres to the module and the other half adheres to the fan tray on the left side. Any attempt to remove a supervisor blade, WiSM2 Module, or blank module cover will damage a tamper seal, which indicates tampering has occurred.
  - c. Power supply—For each power supply or power supply blank cover installed in the chassis, place a tamper-evidence label so that one half of the label adheres to the front of the power supply or power supply blank cover and the other half adheres to the chassis. Any attempt to remove a power supply will damage the tamper seal, which indicates tampering has occurred.
  - d. Opacity shield—Four labels should be applied to the opacity shield (mounted on the right side of the chassis) as follows:
    - Place one label so that one half of the label adheres to the top of the opacity shield and the other half adheres to the chassis.
    - Place one label so that one half of the label adheres to the left side of the opacity shield and the other half adheres to the chassis.
    - Place one label so that one half of the label adheres to the right side of the opacity shield and the other half adheres to the chassis.
    - For the Catalyst 6509 switch chassis only, place one label so that one half of the label adheres to the bottom of the opacity shield and the other half adheres to the right side of the chassis.
- Step 3** Place labels on the supervisor blade installed in the chassis as shown in the figures below.
- a. Place a tamper-evidence label so that one half of the label adheres to the PCMCIA slot and the other half adheres to the supervisor blade faceplate. Any attempt to install or remove a Flash PC card will damage the tamper seal, which indicates tampering has occurred.
  - b. Place a tamper-evidence label so that one half of the label adheres to the GBIC transceiver installed in the supervisor blade network interface uplink port and the other half adheres to the supervisor blade 2 faceplate. Any attempt to remove a GBIC transceiver will damage the tamper seal, which indicates tampering has occurred.
  - c. Place a tamper-evidence label so that it completely covers an unpopulated network interface uplink port. Any attempt to install a GBIC transceiver in the network interface uplink port will damage the tamper seal, which indicates tampering has occurred.

**Step 4** Place labels on the WiSM2 installed in the chassis as shown in the figures below.

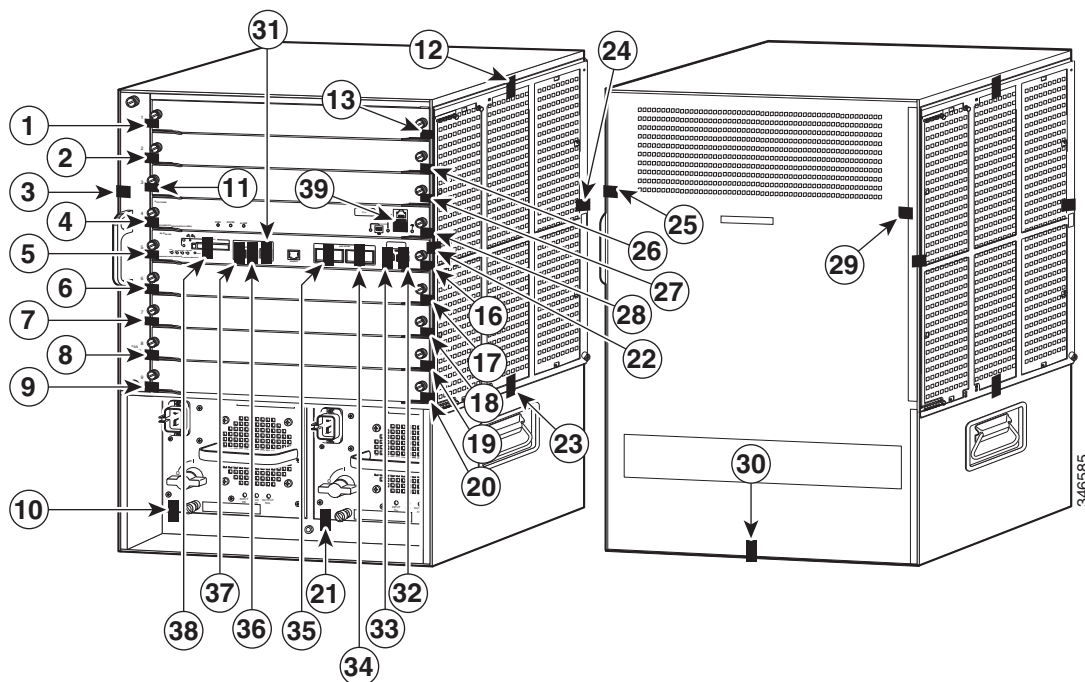
  
**Note**

The tamper seal label adhesive completely cures within five minutes.

**Figure 5** Catalyst 6506 and Catalyst 6506E Switch Chassis Tamper-Evidence Label Placement



**Figure 6** Catalyst 6509 and Catalyst 6509E Switch Chassis Tamper-Evidence Label Placement



The tamper-evidence seals are made from a special thin-gauge vinyl with self-adhesive backing. Any attempt to open the chassis, remove the modules or power supplies, or remove the opacity shield will damage the tamper-evidence seals or the painted surface and metal of the chassis. The tamper-evidence seals must be inspected for damage to verify that the module has not been tampered with.

Tamper-evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word OPEN may appear if the label was peeled back. If it is deemed necessary by the Crypto Officer to replace the tamper evident stickers, please reference FIPS kit CVPN6500FIPS/KIT=, version D0.

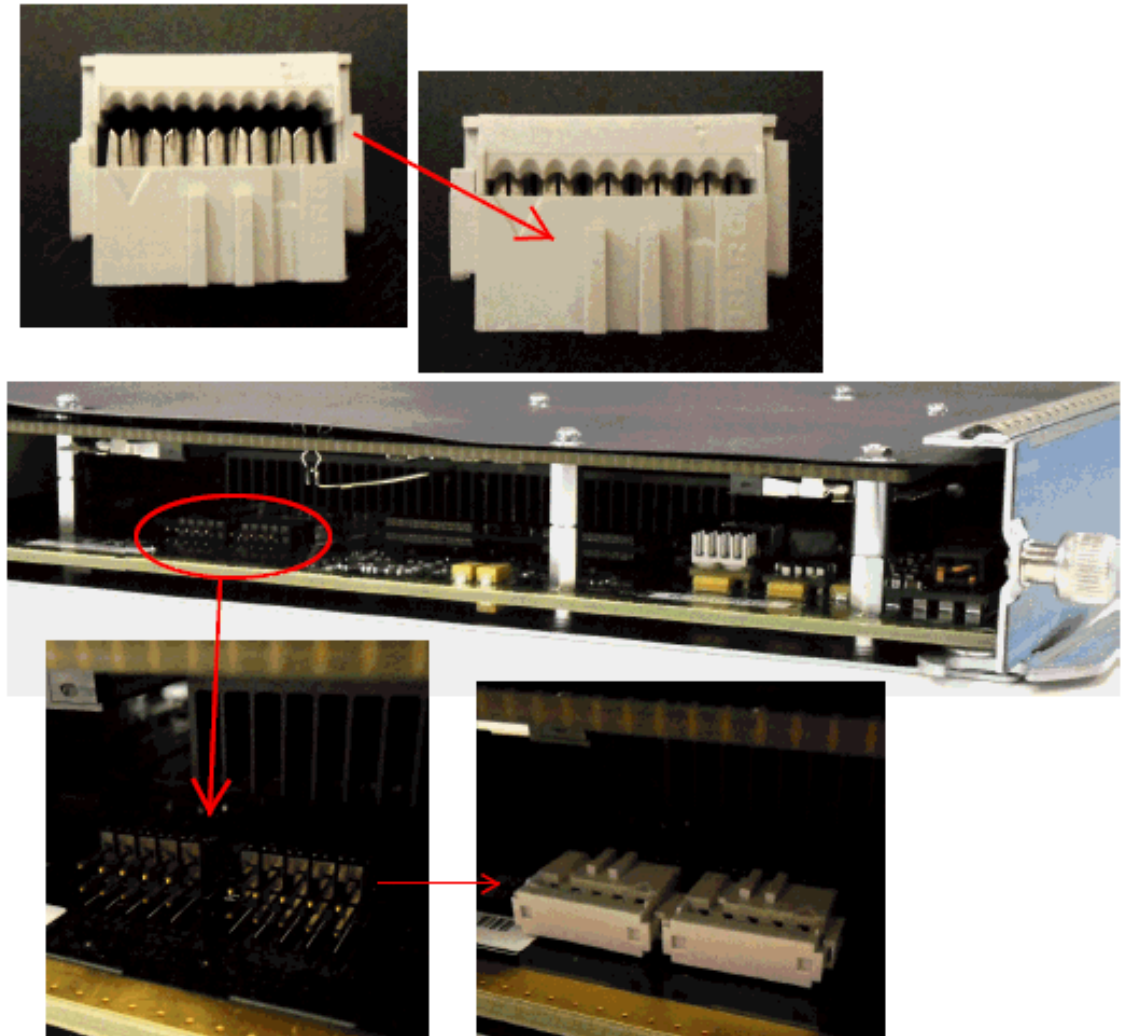
## Installing Pin Covers

Several pins are visible through the side of the module. Cover these pins with mating connectors and the foldable pin cap as shown in [Figure 7](#) through [Figure 10](#).

## Installing Mating Connectors

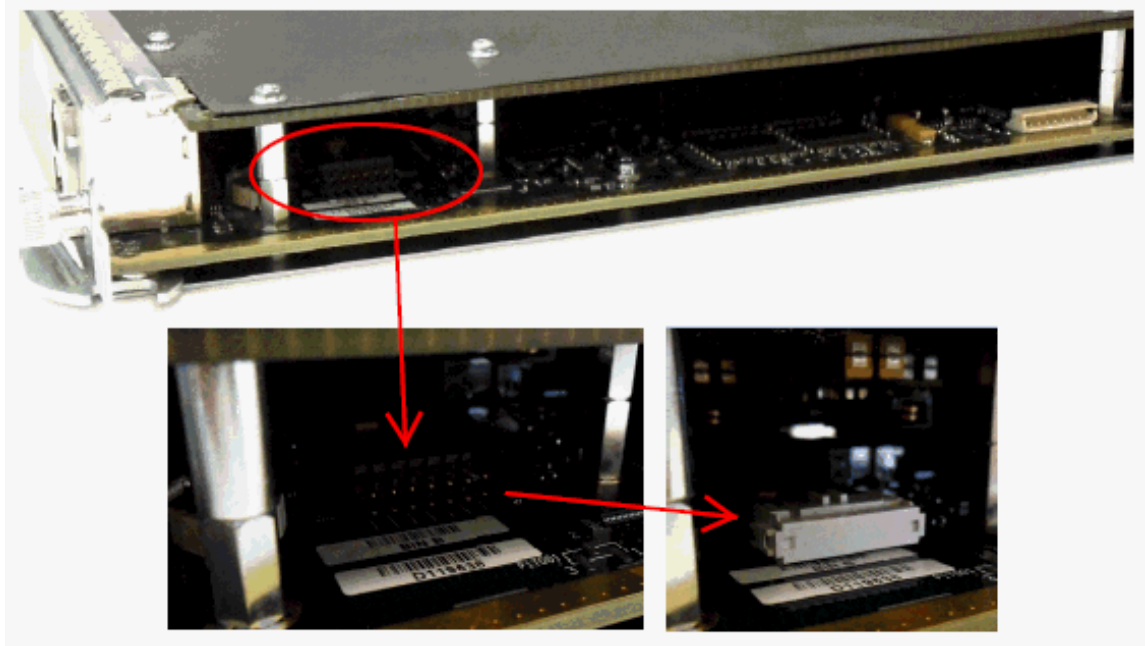
Use two 10-pin mating connectors to cover the pins visible on the left side of the module. Assemble the connectors by pressing the two halves together. Press the assembled connectors onto the pins.

**Figure 7** *Ten-pin Mating Connectors: Assemble and install on left side of the module*



Use one 14-pin mating connector to cover the pins visible on the left side of the module. Assemble the connector by pressing the two halves together. Press the assembled connector onto the pins.

**Figure 8** *Fourteen-pin Mating Connector: Assemble and install on right side of module*

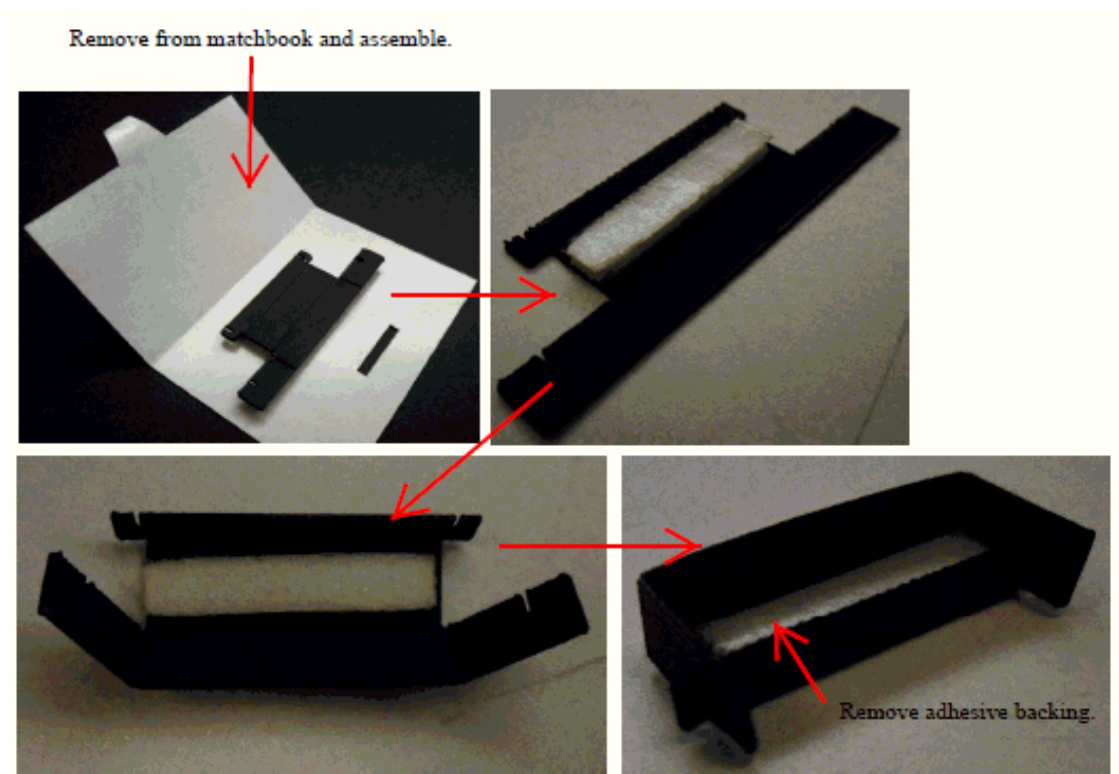


## Installing the Foldable Pin Cap

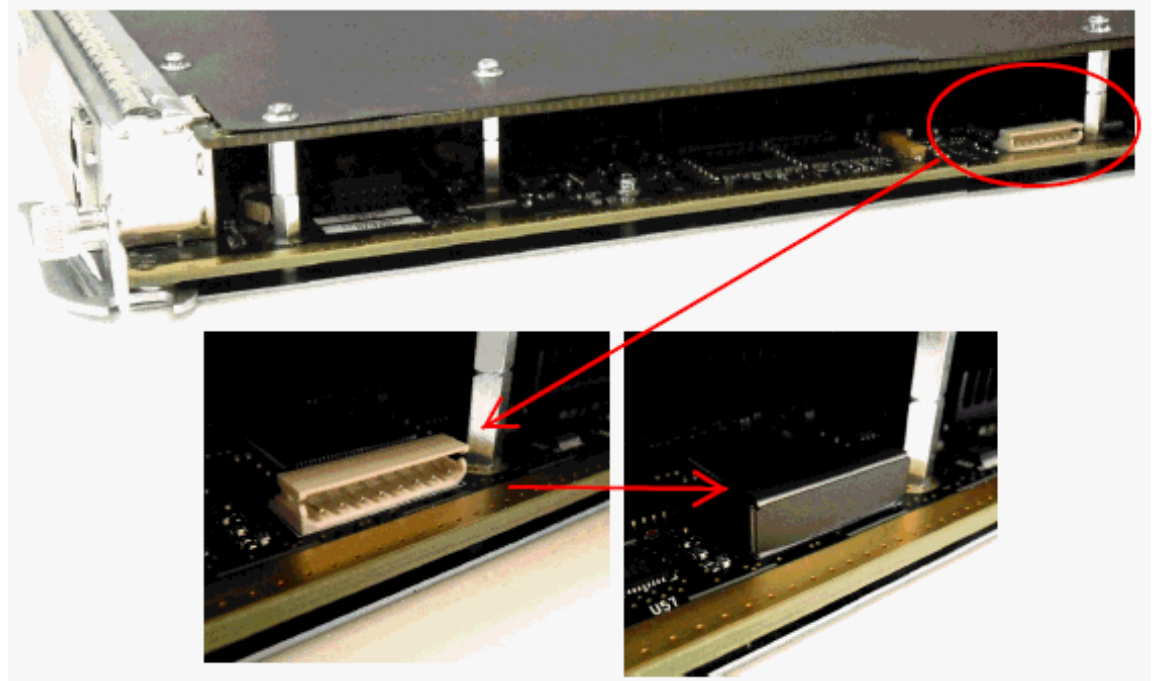
Use the foldable pin cap to conceal the eight-pin connector on the right side of the module. Fold the cap along the edges and insert the tabs into the slots. Remove the backing from the adhesive strip and press the cap in place over the pins as shown in [Figure 9](#) and [Figure 10](#).



**Figure 9** *Assembling the Folding Cap*



**Figure 10** *Pressing the Cap in Place Over the Pins*



## Mitigation of Attacks

The Controllers in the WiSM2 module provide 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 access points in joining the trusted network. The Cisco access points and Controllers support mutual authentication via x.509 certificates that are installed from the factory.
- Protection against MiTM attacks against access point control traffic. All control and bridging traffic between Controllers and access points is protected with DTLS using AES-CBC encryption.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

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

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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](http://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)

© 2010-2014 Cisco Systems, Inc. All rights reserved.