FIPS 140-2 Non-Proprietary Security Policy
for
Alcatel-Lucent Enterprise OmniSwitch AOS 6.7.1.R04 Cryptographic Module




Module Version No: 6.7.1.R04
FIPS Security Level: 1
Document Version: 1.3
Date: November 29, 2017

Prepared For:

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA
USA 91301
www.enterprise.alcatel-lucent.com

Prepared By:

EWA-Canada, Ltd.
1223 Michael Street, Suite 200
Ottawa, Ontario
Canada K1J 7T2
www.ewa-canada.com

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This non-proprietary Security Policy for the OmniSwitch AOS 6.7.1.R04 Cryptographic Module Cryptographic Module by Alcatel-Lucent Enterprise describes how the module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode of operation.

This document was prepared as part of the Level 1 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 - FIPS 140-2 Section Security Levels

1.2 Background

Federal Information Processing Standards Publication (FIPS PUB) 140-2 – *Security Requirements for Cryptographic Modules* details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSE) Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:

http://csrc.nist.gov/groups/STM/cmvp/index.html

More information about Alcatel-Lucent Enterprise and the OmniSwitch Products can be found on the Altacel Lucent Enterprise website:

http://enterprise.alcatel-lucent.com/

1.3 Document Organization

This non-proprietary Security Policy is part of the Alcatel-Lucent Enterprise OmniSwitch AOS 6.7.1.R04 Cryptographic Module FIPS 140-2 submission package . Other documentation in the submission package includes:

- Product documentation
- Vendor evidence documents
- Finite state model
- Additional supporting documents

The Alcatel-Lucent Enterprise OmniSwitch AOS 6.7.1.R04 Cryptographic Module is also referred to in this document as the AOS Cryptographic Module, cryptographic module, or the module.

1.4 Module Platforms

The following hardware appliances have been tested with AOS 6.7.1.R04

Series	Model
6350	6350-10 6350-P10 6350-24 6350-P24 6350-48 6350-P48
6450	6450-10 6450-10L 6450-P10 6450-10M 6450-P10L 6450-P10S 6450-24 6450-24L 6450-24X 6450-P24 6450-P24L 6450-P24X 6450-U24 6450-U24S 6450-U24X 6450-U24SXM 6450-24XM 6450-48 6450-48L 6450-48X 6450-P48 6450-P48L 6450-P48X

Table 2 - FIPS 140-2 Compatible Platforms

1.5 Platform Series Overview

1.5.1 **OmniSwitch 6350**

The Alcatel-Lucent Enterprise OmniSwitch® 6350 family is a series of fxed-confguration Gigabit Ethernet switches available as 10-, 24- and 48-port, Power-over-Ethernet (PoE) and non-PoE models to create the exact network for your small business.

The network capabilities of the OmniSwitch 6350 family include advanced security, quality of service and high availability features for your business-class data, voice and wireless technologies. These switches are simple to deploy, confgure and manage.

All OmniSwitch 6350 switches use the field-proven ALE Operating System (AOS) to deliver highly available, secure, self-protective, easily managed, and eco-friendly networks.

The OmniSwitch 6350 family is embedded with the latest technology innovations and offers maximum investment protection.

Small business network solution deployments beneft from the OmniSwitch 6350 family.

1.5.2 OmniSwitch 6450

The Alcatel-Lucent Enterprise OmniSwitch® 6450 Stackable Fast Ethernet and Gigabit Ethernet LAN value switch family offers versatile, 24/48-port fxed confguration switches with 10 GigE uplinks and provides upgrade paths for 10 Gigabit Ethernet (GigE) stacking, 10 GigE uplinks and metro Ethernet services.

Promoting a design optimized for flexibility, scalability, and low power consumption, the OmniSwitch 6450 is an outstanding edge solution. It uses the field-proven ALE Operating System (AOS) to deliver highly available, secure, self-protective, easily managed and eco-friendly networks.

The OmniSwitch 6450 family is embedded with the latest technology innovations and offers maximum investment protection.

The following types of deployments beneft from the OmniSwitch 6450 family:

- Edge of small-to-mid-sized networks
- Branch office enterprise and campus workgroups
- Residential and commercially managed service applications
- Service provider network deployments

2 Module Overview

The OmniSwitch AOS 6.7.1.R04 Cryptographic Module is a software module which provides cryptographic functionality to Alcatel-Lucent Enterprise software applications present on the Alcatel-Lucent Enterprise OmniSwitch series of routers. For the purposes of FIPS 140-2, the module is classified as a software module with a multi-chip standalone embodiment.

2.1 Cryptographic Module Specification

The physical boundary of the module is the OmniSwitch chassis enclosure on which the module is running. The logical cryptographic boundary contains the AOS Cryptographic Module which provides cryptographic functionality for calling applications, and is denoted in the below figure by a dashed line. The physical and logical boundaries is depicted in the figure below.

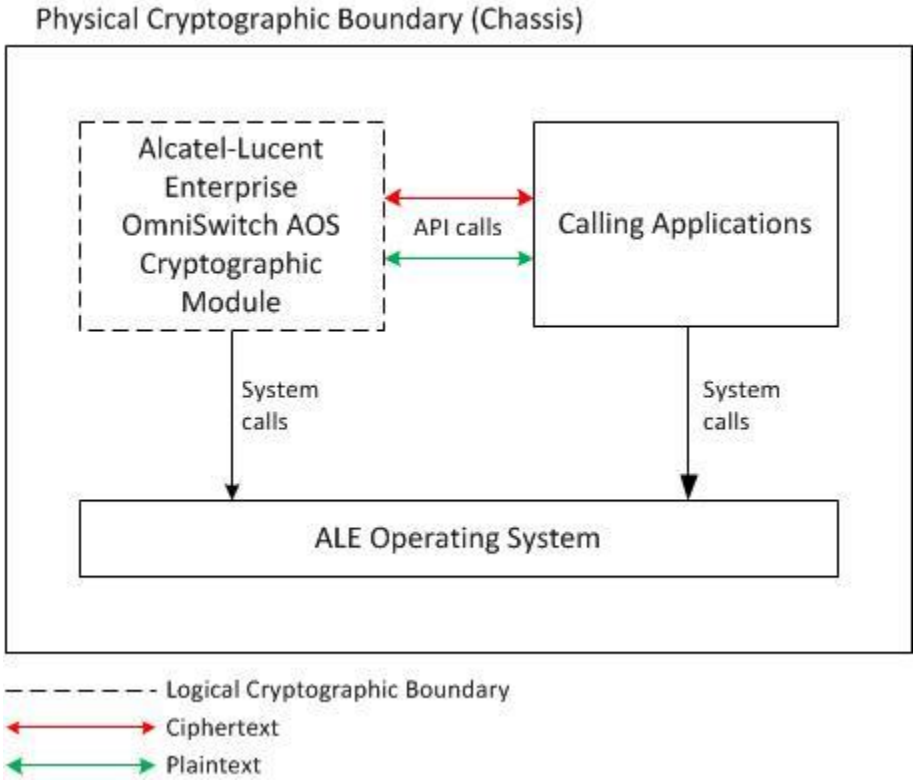

Figure 1 - Block Diagram

2.2 Cryptographic Module Ports and Interfaces

The module's physical ports and interfaces are those of the hardware on which the module is operating. For the OmniSwitch series of routers, the physical ports and interfaces would be as follows:

- Ethernet, RJ-45, USB, SFP, SFP+
- LEDs
- Power supplies

Being a software module, the logical interfaces are defined by API function calls and their associated input and output parameters (including return codes). Table 3 below shows how OmniSwitch physical ports and interface map to the logical interfaces of the module as defined in FIPS 140-2:

FIPS 140-2 Interface	Physical Interface	Module Interface
Data Input	Ethernet, SFP, SFP+	API Input Parameters
Data Output	Ethernet, SFP, SFP+	API Output Parameters
Control Input	USB, RJ-45, Ethernet, SFP, SFP+	API Function Calls
Status Output	USB, RJ-45, Ethernet, SFP, SFP+, LEDs	API Output Parameters and Return Codes
Power Input	Hardware Power Connector, Ethernet (PoE)	N/A

Table 3 - Module Interface Mappings

2.3 Roles & Services

2.3.1 Roles

The module has two operator roles: Crypto Officer and User. The roles are assumed implicitly upon the invocation of the module services. The Crypto Officer is an administrative role that initializes the module and uses cryptographic services provided by the module, while the Users are the calling applications that utilize the cryptographic functions.

The module does not support concurrent operators.

2.3.2 Services

Table 4 below specifies the services that are available to a module operator. In the CSP Access column, Read and Execute mean the CSP is used by the API call to perform the service, and Write means the CSP is generated, modified or deleted by the API call.

Service	Operator	Description	Input	Output	CSP	Access
Encryption	User	Encrypts plaintext data	Plaintext data, Initialization vector, Key	Encrypted data	AES-CBC Key	Execute
Decryption	User	Decrypts encrypted data	Encrypted data, Initialization vector, Key	Plaintext data	AES-CBC Key	Execute
Generate Random Number	User	Generates random bits	Seed value	Random bits	DRBG Entropy, DRBG Seed	Read/Execute
Generate Symmetric Key	User	Generate symmetric key	Key size	Key	AES-CBC Key, TLS Session Encryption Key, SSH Session Key	Execute/Write
Generate Asymmetric Key	User	Generates asymmetric key pair	Key size	Asymmetric key pair	Diffie-Hellman Private Key, Diffie-Hellman Public Key, RSA Public Key, RSA Private Key	Read/Write/Execute
Hash	User	Calculates a hash using SHA	Plaintext data	Hashed data	N/A	N/A
Keyed Hash	User	Calculates a hash using HMAC-SHA	HMAC key and Plaintext data	Hashed data	HMAC key	Read/Write/Execute
Installation, Uninstallation, and Initialization	Crypto Officer	Install, initialize, configure, uninstall	N/A	N/A	N/A	N/A
Key Agreement	User	Perform key agreement on behalf of calling process. Not used to establish keys into the module	DH public key and private Key	DH agreement key	Diffie-Hellman Private Key, Diffie-Hellman Public Key	Read/Write/Execute

Service	Operator	Description	Input	Output	CSP	Access
Key Transport	User	Encrypt or Decrypt a key value on behalf of the calling process	Encrypt: key value, RSA Key Transport Key Decrypt: Encrypted Key value, RSA Key Transport Key	Encrypt: Encrypted key value Decrypt: key value	RSA Public Key, RSA Private Key	Read/Write/Execute
Self-Test	User/Crypto Officer	Performs self-tests	N/A	Pass or fail return code	N/A	Execute/Read
Show Status	User/Crypto Officer	Displays module status and version	N/A	Module status	N/A	Execute
Signature Sign	User	Generates a digital signature	Signing key; plaintext	Digital signature	RSA Public Key, RSA Private Key	Execute
Signature Verify	User	Verifies a digital signature	Digital signature; Public Key,	Result of verification	RSA Public Key, RSA Private Key	Execute
Zeroize	User/Crypto Officer	Zeroize CSPs	N/A	N/A	All except Integrity key	Write

Table 4 - Services

2.4 Authentication Mechanisms

The module does not support authentication.

2.5 Physical Security

The module is a software module and does not implement any physical security.

2.6 Operational Environment

The AOS Cryptographic Module was tested on the following OmniSwitch platforms:

Series	Model	OS & Version
6350	6350-10 6350-P10 6350-24 6350-P24 6350-48 6350-P48	ALE Operating System (AOS) 6.7.1.R04
6450	6450-10 6450-10L 6450-P10 6450-10M 6450-P10L 6450-P10S 6450-24 6450-24L 6450-24X 6450-P24 6450-P24L 6450-P24X 6450-U24 6450-U24S 6450-U24X 6450-U24SXM 6450-24XM 6450-48 6450-48L 6450-48X 6450-P48 6450-P48L 6450-P48X	

Table 5 - Operational Environments

2.7 Cryptographic Key Management

2.7.1 Algorithm Implementations

2.7.1.1 Approved Algorithms

A list of FIPS-Approved algorithms implemented by the module can be found in Table 6.

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or	Use
#4284 #4339	AES	FIPS 197, SP800-38A	CBC	128/192/256 bits	Data Encryption and Decryption
Vendor Affirmed	CKG[1]	SP 800-133			Key Generation
#1389 #1390	CVL TLS 1.0/1.1, TLS 1.2, SSH	SP 800-135	-	-	Key Derivation
#1344 #1383	DRBG	SP800-90A	Hash_DRBG HMAC_DRBG CTR_DRBG	-	Deterministic Random Bit Generation
#2820 #2879	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-1-96[2] HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	512/1024 bits	Message Authentication
#2305 #2343	RSA	FIPS 186-4	-	2048 bits[3]	Key Generation

[1] Resulting symmetric keys are an unmodified output from an Approved DRBG.
[2] Used in the SSHv2 protocol. This usage is in compliance with FIPS 140-2 Implementation Guidance A.8 Use of HMAC-SHA-1-96 and Truncated HMAC.
[3] RSA Key Generation for 3072-bit modulus has been tested but is not used by the module.

#2305 #2343	RSA	FIPS 186-4	SHA-1 SHA-256 SHA-384 SHA-512 (ANSI X9.31 and PKCS1 v1.5)	2048 bits	Digital Signature Generation and Verification
#2423 #2424	RSA	FIPS 186-4	SHA-1 SHA-256 SHA-384 SHA-512 (SSA-PSS)	2048 bits	Digital Signature Generation and Verification
#3522 #3575	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	-	Message Digest

Table 6 - FIPS-Approved Algorithm Implementations

2.7.1.2 Non-Approved but Allowed Algorithms

A list of non-Approved algorithms implemented by the module can be found in Table 7.

Algorithm	Caveat	Use
Diffie-Hellman	Provides 112 bits of encryption strength.	Key establishment
MD5		TLS 1.0/1.1 KDF
RSA Key Wrapping	Provides 112 bits of encryption strength	Key establishment
NDRNG		Used to provide seed input into the module's Approved DRBG.[4]

Table 7 - Non-Approved Algorithm Implementations

2.7.1.3 Non-Approved Algorithms

[4] The estimated amount of entropy provided by the NDRNG is 0.99 per 1 bit of data.

A list of non-Approved algorithms implemented by the module can be found in Table 8.

Algorithm	Use
MD5	Hashing Algorithm
SHA-1	Signature Generation

Table 8 - Non-Approved Algorithm Implementations

2.7.2 Key Management Overview

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
AES-CBC Key (128/192/256 bit)	TLSv1.1, TLSv1.2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
DRBG Entropy	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG “Key” Value	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG “C” Value	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG Seed	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG “V” Value	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
Diffie-Hellman Private Key	DH (2048-bit) private key agreement key	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
Diffie-Hellman Public Key	DH (2048-bit) public key agreement key	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-1 Integrity Key	Module Integrity	Module Binary	Plaintext	None	None	None	CO: R User: R
HMAC-SHA-1	SSHv2, MAC-based end-user and device authentication	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-1-96	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-224	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-256	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-384	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ

HMAC-SHA-512	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
RSA Public Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
RSA Private Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
TLS pre-master secret	Shared secret used in TLS exchange for TLS sessions.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS master secret	Shared secret used in TLS exchange for TLS sessions.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS session authentication key	Used to authenticate TLS traffic.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS session encrypton key	Used to encrypt TLS traffic.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH session authentication key	Used by SSH for data integrity.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH session key	Used by SSH for session encryption.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH RSA private key	The RSA private key used for SSH authentication.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ

Table 9 - Cryptographic Keys, Key Components, and CSPs

Access includes Write (W), Read (R), and Zeroize (Z).

The SSH and TLS protocols have not been reviewed or tested by the CAVP or the CMVP.

2.7.3 Key Generation & Input

The module implements SP 800-90A compliant DRBG services for creation of symmetric keys, and for generation of RSA keys as shown in Tables 6 and 9. Resulting symmetric keys are an unmodified output from an Approved DRBG.

For random number generation the calling application should use entropy sources that meet the security strength required in SP 800-90A. This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met. CSPs are passed to the module in plaintext as API parameters. Private and secret keys as well as seed and entropy are also provided to the module by the calling application.

2.7.4 Key Output

The module does not output CSPs, other than the explicit results of key generation requests.

2.7.5 Storage

Keys are provided to the module by the calling process and are destroyed when released by the appropriate API function call or during a power cycle. The module does not perform the persistent storage of keys or CSPs. Generated data will always be associated with the relevant calling process. The module code ensures that no data can be associated with calling daemons beyond the relevant caller. The implementation of the zeroization process leaves no traces of data left for successive calls of the same or other services.

2.7.6 Zeroization

Zeroization of sensitive data is performed automatically by an API function call for temporarily stored CSPs. There are also functions provided to explicitly destroy CSPs related to random number generation services.The calling application is responsible for parameters passed in and out of the module. Private and secret keys as well as seed and entropy are destroyed when the API function calls return. No key information is output through the data output interface when the module zeroizes keys.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The AOS Cryptographic Module runs on the OmniSwitch series of routers that have been tested and conform to the FCC EMI/EMC requirements in 47 Code of Federal Regulation, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

2.9 Self Tests

2.9.1 Power Up Self Tests

The module performs the following tests automatically upon power up:

Algorithm	Type	Description
AES	KAT[5]	Encryption and decryption are tested separately, ECB mode, 128 bit length
CVL	KAT	SP 800-135 TLS 1.0/1.1,TLS 1.2, and SSH
CTR-based DRBG	KAT	AES, 256 bit with and without derivation function
Hash-based DRBG	KAT	SHA-256
HMAC-based DRBG	KAT	HMAC-SHA-256
SHS[6]	KAT	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
HMAC	KAT	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512
Module Integrity	KAT	HMAC-SHA1
RSA	KAT	Signature generation and verification are tested separately using 2048 bit key, SHA-256, PKCS#1

Table 10 - Power-On Self-Tests

Power-on self tests return 1 if all self tests succeed, and 0 if not. If a self-test fails, the module enters an error state and all data output is inhibited. During self-tests, cryptographic functions cannot be performed until the tests are complete. If a self-test fails, subsequent invocation of any cryptographic function calls will fail. The only way to recover from a self-test failure is by reloading the module.

2.9.2 Conditional Self Tests

The module performs the following conditional self tests:

Algorithm	Modes and Key Sizes

DRBG	• Continuous Random Number Generation Test
	• SP 800-90B DRBG Health Tests
	  ○ Instantiate
	  ○ Reseed
	  ○ Generate
	  ○ Uninstantiate

NDRNG	Continuous Random Number Generation Test
RSA	Pairwise consistency test for both Sign/Verify and Encrypt/Decrypt

Table 11 - Conditional Self-Tests

In the event of a DRBG self-test failure the calling application must uninstantiate and re-instantiate the DRBG per SP 800-90A requirements.

[5] KAT: Known Answer Test

[6] With exception of SHA-1 which has it own Known-Answer Test, all of the SHA KATs are tested as part of HMAC KATs

2.10 Design Assurance

Configuration management for the module is provided by Agile, and Perforce for software. Each configuration item along with major and minor versions are identified through these tools.

Documentation version control is performed manually by updating the document date as well as the major and minor version numbers in order to uniquely identify each version of a document.

2.11 Mitigation of Other Attacks

The module does not claim to mitigate any attacks outside the requirements of FIPS 140-2.

3 Secure Operation

The AOS Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in FIPS-Approved mode of operation.

When the FIPS enable command is entered on OmniSwitch, FIPS 140-2 compliant encryption is used by the OmniSwitch devices in the various management interfaces such as SFTP, HTTPS, SSH and SSL.

These strong cryptographic algorithms ensure secure communication with the device to provide interoperability, high quality, cryptographically-based security for IP networks through the use of appropriate security protocols, cryptographic algorithms, and keys and prevent any form of hijacking/hacking or attack on the device through the secure mode of communication.

When configured according to the instructions below in section 3.1 and 3.2 the module does not support a non-FIPS mode of operation.

3.1 Initialization and Configuration

The following procedure is used to configure the FIPS mode on the switch:

1. Enable the FIPS (CC) mode on an OmniSwitch using the following command:

```
-> system common-criteria enable
WARNING: Common Criteria configuration is applied only after
REBOOT
```

2. Reboot the system, a reconfirmation message is displayed. Type “Y” to confirm reload.

```
-> reload working no rollback-timeout
-> Confirm Activate (Y/N) : y
```

3. Use the **show system common-criteria** to view the configured and running status of the FIPS mode on the Switch.

```
-> show system common-criteria
Common Criteria mode Configured status: Enabled
Common Criteria mode Running status: Enabled
```

4. Copy the current configuration to the certified memory partition using the command:

```
-> copy working certified
```

3.2 Crypto Officer Guidance

The Crypto-Officer (CO) is responsible for initializing and configuring the module into the FIPS-Approved mode of operation. Prior to following the guidance in the section “Initialization and configuration”, the CO is responsible for the completing the following prerequisites:

• The SSH/SFTP/SSL clients should support the secure FIPS standard cryptographic algorithms to communicate with an OmniSwitch device on FIPS mode.

• The use of the IPsec protocol must be disabled before configuring the module for use in the Approved mode of operation. While in the non-Approved mode of operation, the module also supports the use of the FTP, Telnet, and SNMP protocols, which are disabled upon following the guidance in the section, “Initialization and configuration”.

• User-specific certificates/ keys have to be generated using FIPS compliant cryptographic algorithms. There are no checks in the OpenSSL module to verify the FIPS compliance of the certificate/keys in the flash.

Additional information and guidance is available in the “OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide”.

3.3 User Guidance

The User role is assumed by non-CO operators, calling applications, or the OS.

4 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
EFP	Environmental Failure Protection
EMI/EMC	Electromagnetic Interference / Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
HMAC	(Keyed-) Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NRBG	Non-Deterministic Random Bit Generator
NVM	Non-Volatile Memory
QVGA	Quarter Video Graphics Array
ROM	Read Only Memory
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus

Table 10 - Acronym Definitions