Cisco Catalyst 9200L Series Switches

Cisco Systems, Inc.

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

Version 1.1

June 26, 2021

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 9200L Series Switches running Cisco IOS-XE Firmware Version 16.12 or 17.3. This security policy describes how the modules listed below meet the security requirements of FIPS 140-2 level 1, and how to operate the switches with on-board crypto enabled in a secure FIPS 140-2 mode. The Cisco Catalyst 9200L Series has the following primary SKUs that are covered in this validation effort:

Cisco Catalyst 9200L-24P-4G

Cisco Catalyst 9200L-24P-4X

Cisco Catalyst 9200L-24T-4G

Cisco Catalyst 9200L-24T-4X

Cisco Catalyst 9200L-48P-4G

Cisco Catalyst 9200L-48P-4X

Cisco Catalyst 9200L-48T-4G

Cisco Catalyst 9200L-48T-4X

Cisco Catalyst 9200L-24P8X-2Y

Cisco Catalyst 9200L-24P8X-4X

Cisco Catalyst 9200L-48P12X-4X

Cisco Catalyst 9200L-48P8X-2Y

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 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program.

1.2 Modules Validation Level

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

Table 1: Modules Validation Level

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

1.3 References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the switches from the following sources:

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

Cisco Catalyst 9200L Series Switches -

https://www.cisco.com/c/en/us/products/switches/catalyst-9200-series-switches/index.html

For answers to technical or sales related questions, please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

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

1.4 Terminology

In this document, the Cisco Catalyst 9200L Series Switches is referred to as C9200L switches, the switches, the devices, the cryptographic modules, or the modules.

1.5 Document Organization

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

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

This document provides an overview of the Cisco Catalyst 9200L Series Switches and explains the secure configuration and operation of the modules. This introduction section is followed by Section 2, which details the general features and functionality of the switches. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

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

2 Cisco Systems Catalyst 9200L Series Switches

Catalyst 9200L Series switches provide security features that protect the integrity of the hardware as well as the software and all data that flows through the switch. It provides resiliency that keeps your business up and running seamlessly. Combine that with open APIs of Cisco IOS-XE and programmability of the UADP ASIC technology, Catalyst 9200L Series switches give you what you need now with investment protection on future innovations.

With full PoE+ capability, power and fan redundancy, stacking bandwidth up to 160 Gbps, modular uplinks, Layer 3 feature support, and cold patching, Catalyst 9200L Series switches are the industry's unparalleled solution with differentiated resiliency and progressive architecture for cost-effective branch-office access.

The illustration below shows a representation of Cisco Catalyst 9200L Series switch models. All the switch models have similar appearance. The internal capabilities and port numbers distinguish the models.

Figure 1: Cisco Catalyst 9200L 24/48 Port Series Switches

Cisco Catalyst 9200L series has multigigabit switches with Ethernet, SFP+ and PoE+ ports and the switches also support Cisco StackWise feature. The switches include cryptographic algorithms implemented in IOS-XE firmware as well as hardware ASICs. The modules support IKE/IPSec, TLS, SESA (Symmetric Early Stacking Authentication), SNMPv3, SSHv2, and MACsec.

The cryptographic modules have two mode of operations: FIPS mode and non-FIPS mode. The non-FIPS mode is default for the switches. It is the Crypto-Officer's responsibility to install and configure the modules in FIPS mode of operation. Detailed instructions to setup FIPS mode of operation can be found in *Secure Operation* section of this document.

2.1 Cryptographic Modules Interfaces and Physical Characteristics

The modules are multiple-chip standalone cryptographic modules. The cryptographic boundary is defined as encompassing the "top," "front," "left," "right," "rear," and "bottom" surfaces of the chassis for the switches and the casing for the switches. Included in the physical boundary is the ACT2Lite Cryptographic Module (CMVP Certificate #3637). Cisco Catalyst 9200L Series Switches provide support for the following features:

Table 2 - Cisco Catalyst 9200L Series Switches Models and Descriptions

Switch Model	Description
C9200L-24P-4G	Stackable 24x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P-4X	Stackable 24x1G ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4G	Stackable 24x1G ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4X	Stackable 48x1G PoE+ ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4G	Stackable 48x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4X	Stackable 48x1G ports; 4x1G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4G	Stackable 48x1G ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4X	Stackable 8xMultigigabit Ethernet PoE+ ports and 16x1G PoE+ ports; 2x25G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P8X-2Y	Stackable 12xMultigigabit Ethernet PoE+ ports and 36x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P8X-4X	Stackable 12xMultigigabit Ethernet PoE+ ports and 36x1G PoE+ ports; 4x10G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P12X-4X	Stackable 8xMultigigabit Ethernet PoE+ ports and 40x1G PoE+ ports; 2x25G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P8X-2Y	Stackable 8xMultigigabit Ethernet PoE+ ports and 40x1G PoE+ ports; 2x25G fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.

All the switch models have similar components but might have slight cosmetic differences on the bezels.

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

Table 3: Catalyst 9200L Physical Interface/Logical Interface Mapping

FIPS 140-2 Logical Interface	Physical Interfaces and Cabling
Data Input Interface, Data Output Interface	24 or 48 downlink ports of one of the following types: • 10/100/1000 • 10/100/1000 PoE+ Uplink ports either 1G SFP or 10G SFP+

FIPS 140-2 Logical Interface	Physical Interfaces and Cabling
Control Input Interface	10/100/1000 Ethernet out-of-band management port RJ-45 console port Universal Serial Connector (USB) type A Mini-USB type B StackWise-80 port connectors Mode button
Status Output Interface	10/100/1000 Ethernet out-of-band management port RJ-45 console port Universal Serial Connector (USB) type A Mini-USB type B StackWise-80 port connectors Light Emitting Diodes (LEDs) • Console LED • System LED • Master LED • Stack LED • PoE LED • Port LEDs • Beacon LED • RJ-45 Console ort LED • Fan LED • Uplink LEDs
Power Interface	AC power connector

The following physical interfaces are prohibited from usage in FIPS mode of operation:

- Universal Serial Bus (USB)
- Wireless Console Access with Bluetooth

2.2 Roles, Services and Authentication

The modules support identity-based authentication. Each user is authenticated upon initial access to the modules. There are two roles in the switches that may be assumed: the Crypto-Officer (CO) role and the User role. The administrator of the switches assumes the CO role in order to configure and maintain the switches, while the Users are processes that exercise security services over the network.

2.2.1 User Role

The role is assumed by users obtaining secured data services. From a logical view, user activity exists in the data-plane via defined Data Input/Output Interfaces. Users are authenticated using EAP methods and 802.1X-REV, and their data is protected with 802.1AE protocols. EAP and 802.1X-REV can use password-based credentials for User role authentication – in such a case the user passwords must be at least eight (8) characters long. The password must contain at least one special character and at least one number character along with six additional characters taken from the 26-upper case, 26-lower case, 10-numbers and 32-special characters (procedurally enforced). This requirement gives (26 + 26 + 10 + 32 =) 94 options of character to choose from. Without repetition of characters, the number of probable combinations is the combined probability from 6 characters (94x93x92x91x90x89) times one special character (32) times 1 number (10), which turns out to be (94x93x92x91x90x89x32x10 =) 187,595,543,116,800. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the switches.

EAP and 802.1X-REV can also authenticate the User role via certificate credentials by using 2048-bit RSA keys – in such a case the security strength is 112 bits, so the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 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 8.65×10^{31} attempts per second, which far exceeds the operational capabilities of the modules.

The services available to the User role accessing the CSPs, the type of access – read (r), write (w), execute (e) and zeroized/delete (d) are listed below:

Table 4 - User Services

Services	Description	Keys and CSPs Access
Secured Dataplane	MACsec Network Functions: authentication, access control, confidentiality and data integrity services provided by the MACsec protocol	Diffie- Hellman (DH) private key, Diffie-Hellman (DH) public key, Diffie- Hellman (DH) Shared Secret, MACsec Security Association Key (SAK), MACsec Connectivity Association Key (CAK), MACsec Key Encryption Key (KEK), MACsec Integrity Check Key (ICK) (w, e, d)
Bypass Services	Traffic without cryptographic processing except authentication. The rule must have been previously configured by the Crypto Officer.	Diffie- Hellman (DH) private key, Diffie-Hellman (DH) public key, Diffie- Hellman (DH) Shared Secret (w, e, d)

2.2.2 Crypto-Officer Role

This role is assumed by an authorized CO connecting to the switches via CLI through the console port and performing management functions and modules configuration. Additionally, the stack master is considered CO for stack members. From a logical view, CO activity exists only in the control plane. IOS-XE prompts the CO for their username and password, and, if the password is validated against the CO's password in IOS-XE memory, the CO is allowed entry to the IOS-XE executive program. A CO can assign permission to access the CO role to additional accounts, thereby creating additional COs.

CO passwords must be at a minimum eight (8) characters long. The Secure Operation sections procedurally enforces the password must contain at least one special character and at least one number character along with six additional characters taken from the 26-upper case, 26-lower case, 10-numbers and 32-special characters (procedurally enforced). This requirement gives (26 + 26 + 10 + 32 =) 94 options of character to choose from. Without repetition of characters, the number of probable combinations is the combined probability from 6 characters (94x93x92x91x90x89) times one special character (32) times 1 number (10), which turns out to be (94x93x92x91x90x89x32x10 =) 187,595,543,116,800. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the modules.

Additionally, on a stack, the CO is authenticated via possession of a SESA Authorization key that is 128 bits long. So, an attacker would have a 1 in 2^{128} chance of a successful authentication 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 5.67×10^{36} attempts per second, which is less than 1 in 100,000 and far exceeds the operational capabilities of the modules.

The Crypto-Officer role is responsible for the configuration of the switches. The services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w), execute (e) and zeroized/delete (d) are listed below:

Table 5 - Crypto-Officer Services

Services	Description	Keys and CSPs Access
Define Rules and Filters	Define network interfaces and settings, create command aliases, set the protocols the switch will support, enable interfaces and network services, set system date and time, and load authentication information. Log off users, shutdown or reload the switch, manually back up switch configurations, view complete configurations, manage user rights, and restore switch configurations. Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	Enable password (r, w, e, d)
View Status Functions	View the switch configuration, routing tables, active sessions, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Enable password (r, w, e, d)
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set pre-shared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	[IKE session encrypt key, IKE session authentication key, ISAKMP pre-shared, IKE authentication private Key, IKE authentication public key, skeyid, skeyid_d, SKEYSEED, IPsec session encryption key, IPsec session authentication key] (w, d) and Enable password (r)
SESA	Configure Secure Stacking (SESA) manually on each of the member switches.	SESA Authorization Key, SESA Master Session Key, SESA Derived Session Keys (w, e, d)
HTTPs	HTTP server over TLS (1.2)	TLS Server private key, TLS Server public key, TLS pre-master secret, TLS encryption keys, TLS integrity keys, DRBG entropy input, DRBG V, DRBG Key (w, e, d)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	DH private DH public key, DH Shared Secret, SSH RSA private key, SSH RSA public key, SSH integrity key, SSH session key, DRBG entropy input, DRBG V, DRBG Key (w, e, d)
SNMPv3	Configure SNMPv3 MIB and monitor status	[SNMPv3 Password, snmpEngineID] (r, w, d), SNMP session key, DRBG entropy input, DRBG V, DRBG Key (w, e, d)

Services	Description	Keys and CSPs Access
IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_d, SKEYSEED,IKE session encrypt key, IKE session authentication key, ISAKMP pre-shared, IKE authentication private Key, IKE authentication public key, IPsec session encryption key, IPsec session authentication key, DRBG entropy input, DRBG V, DRBG Key (w, e, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
User services	The Crypto Officer has access to all User services.	User Password (r, w, e, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 7, Zeroization column.	All CSPs (d)

2.2.3 Unauthorized Role

The services for someone without an authorized role are: passing traffic through the devices, view the status output from the modules' LED pins, and cycle power.

2.2.4 Services Available in Non-FIPS Mode of Operation

The cryptographic modules in addition to FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes a non-approved mode of operation exist. The modules are considered to be in a non-FIPS mode of operation when it is not configured per section 3 (Secure Operation of the Switches). The FIPS approved services listed in table 8 become non-approved services when using any non-approved algorithms or non-approved key or curve sizes.

Table 6 - Non-approved algorithms in the Non-FIPS mode services

Services [1]	Non-Approved Algorithms
IPsec	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
SSH	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES

[1] These approved services become non-approved when using any of non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

	Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
SNMP v1/v2	Hashing: MD5 Symmetric: DES

2.3 *Cryptographic Algorithms*

The modules implement a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms

The switches support the following FIPS-2 approved algorithm implementations:

Table 7 – Algorithm Certificates

Algorithms	CAVP #C462: IOS Common Cryptographic Module (IC2M) Rel5	CAVP #4769: UADP MSC 1.0	CAVP #C1301: Firmware Image Signing
AES	CBC (128, 192, 256), CFB128 (128, 192, 256), CMAC (128, 256), CTR (128, 192, 256), ECB (128, 192, 256), GCM (128, 192, 256)	ECB (128, 256) GCM (128, 256)	N/A
CVL (SP800-56A)	KAS-ECC Component-Ephemeral Unified (EC: P-256 SHA-256, ED: P-384 SHA-384) KAS-FFC Component-dhEphem (FC: SHA-256)	N/A	N/A
DRBG	CTR-AES (256)	N/A	N/A
HMAC	HMAC SHA-1, HMAC SHA2-256, HMAC SHA2-384, HMAC SHA2-512	N/A	N/A
ECDSA	KeyGen, KeyVer, SigGen, SigVer (Curve: P-256, P-384)	N/A	N/A
CVL (SP800-135)	IKEv1 IKEv2 SNMP SSH TLS	N/A	N/A
KBKDF (SP800-108)	Counter: HMAC-SHA-1	N/A	N/A
RSA	KeyGen (186-4) 2048-, 3072-bits modulus SigGen (186-4 PKCS 1.5) 2048-, 3072-bits modulus, SigVer (186-2 PKCS 1.5) 1024-, 1536-, 2048-, 3072-, 4096-bits modulus SigVer (186-4 PKCS 1.5) 1024-, 2048-, 3072-bits modulus	N/A	RSA 2048 with SHA-512 SIgVer

SHS	SHA-1, SHA2-256, SHA2-384, SHA2-512	N/A	SHA-512
Triple-DES	CBC (keying option: 1)	N/A	N/A
CKG	Vendor affirmed	N/A	N/A

KTS (AES Cert. #C462; key establishment methodology provides between 128 and 256 bits of encryption strength)

Notes:

There are some algorithm modes that were tested but not implemented by the modules. Only the algorithms, modes, and key sizes that are implemented by the modules are shown in this table.

The modules' AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS, RFC 7296 for IPSec/IKEv2 and IEEE 802.1AE and its amendments for MACsec.

The modules are compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The 64-bit counter portion of the 96-bit IV is set by the modules within its cryptographic boundary. When the IV exhausts the maximum number of possible values (0 to 2^{64} - 1) for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the modules' power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The modules use RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a rekeying with IKEv2 to establish a new encryption key. In case the modules' power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The AES GCM IV is generated internally in the cryptographic module in accordance with IEEE 802.1AE and its amendments. The IV length used is 96 bits (per SP 800-38D and FIPS 140-2 IG A.5). If the module loses power, then new AES GCM keys should be established. The module should only be used with CMVP FIPS 140-2 validation modules when supporting the MACsec protocol for providing Peer, Authenticator functionality. The link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

No parts of the SSH, TLS and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP. Each of TLS, SSH and IPSec protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS), RFC 4253 (SSH) and RFC 6071 (IPSec) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the modules limit the number of encryptions with the same key to 2^{20}.

In accordance with FIPS 140-2 IG D.12, the cryptographic modules perform Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133rev1. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

Diffie-Hellman (CVL Cert. #C462 with CVL Cert. #C462, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength) when used with modulus size of 2048 bits or greater

EC Diffie-Hellman (CVL Cert. #C462 with CVL Cert. #C462, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength) when used with modulus size of 2048 bits or greater

NDRNG[2] to seed FIPS approved DRBG (256 bits)

[2] ACT2Lite Cryptographic Module (CMVP Certificate #3637)

Non-FIPS Approved Algorithms

The cryptographic modules implement the following non-Approved algorithms that are not used in FIPS mode of operation:

MD5 (MD5 does not provide security strength to TLS protocol)
HMAC-MD5
RC4
DES

2.4 Cryptographic Key/CSP Management

The modules securely administer both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the CO role login and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Note that the command '**fips zeroize'** will zeroize a large majority of the listed CSPs. This command essentially results in a device reboot and therefore forces a power cycle, zeroizing all the keys listed below with "Power cycle" in the Zeroization Method column.

Table 8 lists the secret and private cryptographic keys and CSPs used by the modules.

Table 8 – Cryptographic Keys and CSPs

ID	Algorithm	Size	Description	Storage	Zeroization Method
General Keys/CSPs					
DRBG V	SP 800-90A CTR_DRBG	128-bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Power cycle
DRBG key	SP 800-90A CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90 CTR_DRBG	DRAM (plaintext)	Power cycle
DRBG entropy input	SP 800-90A CTR_DRBG	256-bits	HW based entropy source output used to construct seed	DRAM (plaintext)	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	256-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source	DRAM (plaintext)	Power cycle

User password	Password	Variable (8+ characters)	Used to authenticate local users	NVRAM (plaintext)	Zeroized by overwriting with new password
Enable secret	Password	Variable (8+ characters)	Used to authenticate local users at a higher privilege level	NVRAM (plaintext)	Zeroized by overwriting with new password
Diffie-Hellman public key	DH	2048-4096 bits	The public exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Power cycle
Diffie-Hellman private key	DH	224-379 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Automatically after shared secret generated.
Diffie-Hellman shared secret	DH	2048-4096 bits	This is the shared secret agreed upon as part of DH exchange	DRAM (plaintext)	Power cycle
EC Diffie-Hellman public key	ECDH	P-256, P-384	Public key used in EC Diffie-Hellman exchange. This key is derived per the EC Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle
EC Diffie-Hellman private key	ECDH	P-256, P-384	Private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle
EC Diffie-Hellman shared secret	ECDH	P-256, P-384	Shared secret used in EC Diffie-Hellman exchange	DRAM (plaintext)	Power cycle
SSH					
SSHv2 RSA public key	RSA	2048-3072 bits modulus	SSH public key used in SSH session establishment	NVRAM (plaintext)	'# crypto key zeroize rsa'
SSHv2 RSA private key	RSA	2048-3072 bits modulus	SSH private key used in SSH session establishment	NVRAM (plaintext)	'# crypto key zeroize rsa'
SSHv2 integrity key	HMAC	160-512 bits	Used for SSH integrity protection.	DRAM (plaintext)	Automatically when SSH session terminated
SSHv2 session key	Triple-DES/AES	168-bits/256-bits	This is the SSH session symmetric key.	DRAM (plaintext)	Automatically when SSH session terminated
TLS					

TLS server public key	RSA/ECDSA	RSA: 2048-3072 bits modulus ECDSA: P-256, P-384	Public key used in TLS negotiations.	NVRAM (plaintext)	'#crypto key zeroize { rsa | ecdsa }'
TLS server private key	RSA/ECDSA	RSA: 2048-3072 bits modulus ECDSA: P-256, P-384	Identity certificates for module itself and also used in TLS negotiations.	NVRAM (plaintext)	'#crypto key zeroize { rsa | ecdsa }'
TLS pre-master secret	Keying material	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated.
TLS Master Secret	Keying material	48-bits	Keying material used to derive other HTTPS/TLS keys. This key was derived from the TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when session terminated.
TLS encryption key	Triple-DES/AES	168-bits/256-bits	This is the TLS session key	DRAM (plaintext)	Automatically when session terminated.
TLS Integrity Key	HMAC-SHA 256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when session terminated.
SESA					
SESA authorization key	pre-shared key	128 bits	Used to authorize members of stacked units. Entered by CO.	NVRAM (plaintext)	'no fips authorization-key'
SESA master session Key	AES	128 bits	Used to derive SESA session key	DRAM (plaintext)	Upon completion of key exchange
SESA derived session key	AES	128 bits and 192 bits	Used to protect traffic over stacking ports	DRAM (plaintext)	Upon bringing down the stack
SNMPv3					
snmpEngineID	Shared secret	32-bits	Unique string to identify the SNMP engine	NVRAM (plaintext)	'# no snmp-server engineID local engineid-string', overwritten with new engine ID
SNMPv3 password	shared secret	256 bits	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication	DRAM (plaintext)	Power cycle

SNMPv3 session key	AES	128-bit	Encrypts SNMPv3 traffic	DRAM (plaintext)	Power cycle
IPSec					
skeyid	Shared Secret	160 bits	Used for key agreement in IKE. This key was derived in the module	DRAM (plaintext)	Power cycle
skeyid_d	Shared Secret	160 bits	Used for key agreement in IKE	DRAM (plaintext)	Power cycle
SKEYSEED	Keying material	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IKE session encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Derived in the module used for IKEv1/v2 payload integrity verification	DRAM (plaintext)	Power cycle
IKE session authentication key	HMAC-SHA1	160 bits	HMAC-SHA1 key	DRAM (plaintext)	Power cycle
IKE authentication private Key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA private key used in IKEv1/v2 authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE authentication public key	RSA/ECDSA	RSA (2048 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA public key used in IKEv1/v2 authentication. The key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
ISAKMP preshared	pre-shared key	Variable (8+ characters)	This key was configured by CO and used for User role authentication using IKE Pre-shared key based authentication mechanism	NVRAM (plaintext)	'# no crypto isakmp key..'
IPSec session encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Derived in the module used for IKEv1/v2 payload integrity verification	DRAM (plaintext)	Power cycle

IPSec session authentication key	HMAC-SHA1	160 bits	HMAC-SHA1 key	DRAM (plaintext)	Power cycle
MACsec					
MACsec Security Association Key (SAK)	AES-GCM	128-, 256-bits	Used for creating Security Associations (SA) for encrypting/decrypting the MACsec data plane traffic. Derived from the CAK using the SP800-108 KDF.	DRAM (plaintext)	Automatically when session expires
MACsec Connectivity Association Key (CAK)	AES-GCM	128-, 256-bits	A CO configured pre-shared secret key possessed by members of a MACsec connectivity association (via MKA) to secure control plane traffic	NVRAM (plaintext)	'# no key-string..'
MACsec Key Encryption Key (KEK)	AES-CMAC	128/256 bits	Used to transmit SAKs to other members of a MACsec connectivity association. Derived from the CAK using the SP800-108 KDF.	DRAM (plaintext)	Automatically when session expires
MACsec Integrity Check Key (ICK)	AES-GCM	128/256 bits	Used to prove an authorized peer sent the message. Derived from the CAK using the SP800-108 KDF.	DRAM (plaintext)	Automatically when session expires

2.5 Self-Tests

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

2.5.1 Power-On Self-Tests (POSTs)

- Firmware Integrity Test (RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-512)
- IC2M Algorithm Implementation Known Answer Tests:
  - AES-CBC (encrypt/decrypt) KATs
  - AES GCM KAT
  - AES-CMAC KAT
  - SP 800-90A CTR_DRBG KAT
  - SP 800-90A Section 11 Health Tests
  - FIPS 186-4 ECDSA Sign/Verify (Curve: P-256)
  - HMAC-SHA-1, -256, -384, 512 KATs
  - ECC Primitive "Z" KAT
  - FFC Primitive "Z" KAT
  - FIPS 186-4 RSA (sign/verify) KATs (Size. 2048)
  - SHA-1, -256, -384, -512 KATs
  - KBKDF (Counter) KAT
  - Triple-DES CBC (encrypt/decrypt) KATs
- UADP ASIC Hardware Algorithm Implementation Known Answer Tests:
  - AES-ECB (encrypt/decrypt) KATs

2.5.2 Conditional Tests

- Conditional Bypass test
- IC2M Algorithm Implementation Conditional Tests:
  - Pairwise consistency test for RSA
  - Pairwise consistency test for ECDSA
  - Continuous Random Number Generation test for approved DRBG
- NDRNG Continuous Health Tests:
  - Adaptive Proportion Test (APT)
  - Repetition Count Test (RCT)

The devices perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before each role starts to perform services.

2.6 Physical Security

The cryptographic modules entirely contained within production-grade enclosure. The chassis of the modules have removable covers.

3 Secure Operation

The switches meet all the overall Level 1 requirements for FIPS 140-2. Follow the setup instructions provided below to place the modules in FIPS-approved mode. Operating this Switches without maintaining the following settings will remove the modules from the FIPS approved mode of operation.

3.1 System Initialization and Configuration

1. The CO must create the "enable" password for the CO role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the CO first engages the "enable" command. The CO enters the following syntax at the "#" prompt:

   Switch(config)# enable secret [PASSWORD]

2. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for users. From the "configure terminal" command line, the CO enters the following syntax:

   Switch(config)# username *name* [privilege *level*] {password *encryption-type password*}

   Switch(config)# line con 0

   Switch(config-line)# login local

3. Disable manual boot:

   Switch(config)#no boot manual

4. Disable Telnet and configure Secure Shell for remote command line:

   Switch(config)# line vty *line_number [ending_line_number]*

   or

   Switch(config)# transport input ssh

5. Disable the following interfaces by configuration:

   a. USB 3.0

      Switch(config)# hw-module switch 1 usbflash1 unmount

   b. Wireless Console Access with Bluetooth

      Switch(config)# hw-module beacon rp active off

6. To ensure all FIPS 140-2 logging is received, set the log level:

   Switch(config)# logging console error

7. The CO enables FIPS mode by configuring the Authorization key:
   Switch(config)# fips authorization-key <128 bit, i.e, 16 hex byte key>

8. The CO shall only assign users to a privilege level 1 (the default).

9. The CO shall not assign a command to any privilege level other than its default.

Note: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer. For transition from FIPS to non-FIPS mode, the Crypto Officer has to zeroize the module to delete all plaintext, secret keys and CSPs as defined in the Table 8 of the non-proprietary FIPS 140-2 Security Policy document and the Crypto Officer has to issue "no fips authorization key <128-bits (16 octet) key to be used>" command in addition to those defined in Table 8 of the security policy document.

3.2 Verify FIPS Mode of Operation

Use the command lines to display the FIPS configuration information. The switch CLI output shows running status for FIPS mode of operation.

1. To ensure FIPS mode of operation is enabled.

    Switch#show fips status
    Switch and Stacking are running in fips mode
    or
    Switch#show fips status
    Switch and Stacking are not running in fips mode