Cisco Systems, Inc.

Cisco ASA FX-OS on 4K/9K Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

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

© 2021-2026 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 13
2.7 Algorithm Specific Information 28
2.8 RBG and Entropy 29
2.9 Key Generation 30
2.10 Key Establishment 30
2.11 Industry Protocols 31
3 Cryptographic Module Interfaces 31
3.1 Ports and Interfaces 31
4 Roles, Services, and Authentication 32
4.1 Authentication Methods 32
4.2 Roles 33
4.3 Approved Services 35
4.4 Non-Approved Services 71
4.5 External Software/Firmware Loaded 72
4.6 Bypass Actions and Status 72
4.7 Cryptographic Output Actions and Status 73
4.8 Additional Information 73
5 Software/Firmware Security 73
5.1 Integrity Techniques 73
5.2 Initiate on Demand 73
6 Operational Environment 73
6.1 Operational Environment Type and Requirements 73
7 Physical Security 74
7.1 Mechanisms and Actions Required 74
7.2 User Placed Tamper Seals 74
7.3 Filler Panels 79

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

8 Non-Invasive Security 84
9 Sensitive Security Parameters Management 84
9.1 Storage Areas 84
9.2 SSP Input-Output Methods 84
9.3 SSP Zeroization Methods 85
9.4 SSPs 87
9.5 Transitions 128
10 Self-Tests 128
10.1 Pre-Operational Self-Tests 128
10.2 Conditional Self-Tests 129
10.3 Periodic Self-Test Information 142
10.4 Error States 147
11 Life-Cycle Assurance 147
11.1 Installation, Initialization, and Startup Procedures 147
11.2 Administrator Guidance 149
11.3 Non-Administrator Guidance 149
12 Mitigation of Other Attacks 149

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation 10
Table 5: Approved Algorithms - [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module] 12
Table 6: Vendor-Affirmed Algorithms 13
Table 7: Non-Approved, Not Allowed Algorithms 13
Table 8: Security Function Implementations 28
Table 9: Entropy Certificates 29
Table 10: Entropy Sources 29
Table 11: Ports and Interfaces 31
Table 12: Authentication Methods 33
Table 13: Roles 34
Table 14: Approved Services 70
Table 15: Non-Approved Services 72
Table 16: Mechanisms and Actions Required 74
Table 17: Storage Areas 84
Table 18: SSP Input-Output Methods 85
Table 19: SSP Zeroization Methods 86
Table 20: SSP Table 1 103
Table 21: SSP Table 2 127
Table 22: Pre-Operational Self-Tests 128
Table 23: Conditional Self-Tests 142
Table 24: Pre-Operational Periodic Information 142
Table 25: Conditional Periodic Information 147
Table 26: Error States 147

List of Figures

Figure 1 FPR 4112, FPR 4115, FPR 4125, FPR 4145 – Front Panel 6
Figure 2 FPR 4112, FPR 4115, FPR 4125, FPR 4145 - Back Panel 6
Figure 3 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Front Panel 7
Figure 4 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Back Panel 7
Figure 5: FPR4100 Series Front view (no TEL present on front) 74
Figure 6: FPR4100 Series Back view 75
Figure 7: FPR4100 Series Left Side 75
Figure 8: FPR4100 Series Rear view 75
Figure 9: FPR4100 Series Top view 75
Figure 10: FPR4100 Series Bottom view 76
Figure 11: FPR9300 Series Front view 76
Figure 12: FPR9300 Series Right view (Right side has no TELs) 76
Figure 13: FPR9300 Series Left view (Left side has no TELs) 77
Figure 14: FPR9300 Series Rear view 77
Figure 15: FPR9300 Series Top view 78
Figure 16: FPR9300 Series Bottom view 79

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 General

1.1 Overview

This is Cisco Systems, Inc. non-proprietary security policy for the Cisco ASA FX-OS on 4K/9K Cryptographic Module (hereinafter referred to as FXOS or Module), version 2.14(1.143). The following details how this module meets the security requirements of FIPS 140-3, SP 800-140 and ISO/IEC 19790 for a Security Level 2 Hardware cryptographic module.

The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. The following table indicates the actual security levels for each area of the cryptographic module.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

This module is a multi-chip standalone hardware cryptographic module deployed under the Next-Generation Firewall (NGFW) with Firepower eXtensible Operating System (FX-OS) which provides a web interface to configure platform settings and interfaces, provision devices, and monitor system status.

The Cisco Firepower 4100 and Cisco Firepower 9300 Series, when deployed as next-generation firewall (NGFW) appliances, use FX-OS Cryptographic Module and the embedded Cisco® Adaptive Security Appliance Cryptographic Module (ASA-CM). The [ASA-CM] has been submitted to CMVP Cert. #5287.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case, and shown in the figures below and in the Physical Security section. The FPR 4112, FPR 4115, FPR 4125 and FPR 4145 have the same exterior features while FPR 9300 SM-40, FPR 9300 SM-48, and FPR 9300 SM-56 have the same exterior features. Where they differ is in Firewall throughput, IPS throughput, IPsec VPN throughput and number of VPN peers allowed.

Figure 1 FPR 4112, FPR 4115, FPR 4125, FPR 4145 – Front Panel

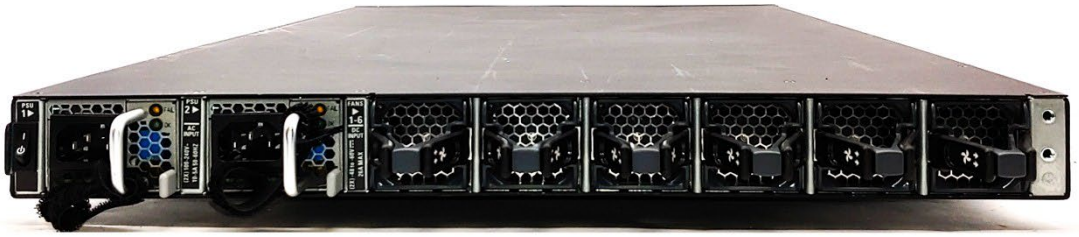


Figure 2 FPR 4112, FPR 4115, FPR 4125, FPR 4145 - Back Panel

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 3 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Front Panel

Figure 4 FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 – Back Panel

The hardware version can be verified by using the command `show version` as an example, this command will output “Hardware: FPR4K-SM-32S.” Additionally, the front panels of chassis for the FPR 4112, FPR 4115, FPR 4125, FPR 4145 (Figure 1) are identical, and display “Cisco 4100 series” on the front panel. The chassis for the FPR 9300 SM40, FPR 9300 SM48 and FPR 9300 SM56 (Figure 3) show “Cisco 9k.”

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FPR 4112	FPR4K-SM-12S	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Silver 4116 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 4115	FPR4K-SM-24S	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Silver 4116 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FPR 4125	FPR4K-SM-32S	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Gold 6130T (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 4145	FPR4K-SM-44S	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Gold 6152 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-40	FPR9K-SM-40	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Gold 6138T (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-48	FPR9K-SM-48	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Platinum 8160 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A
FPR 9300 SM-56	FPR9K-SM-56	2.14(1.143)	Intel i3-3115C (Ivy Bridge); Intel Xeon Platinum 8176 (Skylake) & NITROX-V, Marvell Semiconductor, NITROX	N/A

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode of Operation	The module is always in the approved mode of operation after initial operations are performed.	Approved	Approved mode indicator: "FIPS Mode Admin State: Enabled"
Non-Approved Mode of Operation	The module is configured to have the Approved Mode disabled (Which is not recommended by Cisco). In the Non-Approved Mode, both Non-Approved and Approved algorithms can be configured.	Non-Approved	Non-Approved mode indicator: "FIPS Mode Admin State: Disabled"

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table 3: Modes List and Description

The module supports an Approved and a Non-Approved mode of operation.

Mode change instructions and status indicators:

The module will operate in the Approved mode of operation once the configuration steps for the Approved mode in section 11.1 are completed. The module upon successful completion of all pre-operational self-tests and cryptographic algorithm self-tests from both hardware and firmware implementations will be operational.

Although **not recommended by Cisco**. the module can be configured into the Non-Approved mode by following the configuration steps for the Non-Approved mode in section 11.1.

Degraded Mode Description:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

CiscoSSL FOM Cryptographic Implementation

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4446	Key Length - 128, 256	SP 800-38A
AES-GCM	A4446	Key Length - 128, 256	SP 800-38D
Counter DRBG	A4446	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4446	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 3072 Hash Algorithm - SHA-1	SP 800-135 Rev. 1
KDF SNMP (CVL)	A4446	Password Length - Password Length: 256, 64	SP 800-135 Rev. 1
KDF SSH (CVL)	A4446	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A4446	Key Generation Mode - B.3.4 Modulo - 2048, 3072, 4096 Hash Algorithm - SHA2-256 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A4446	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4446	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4446	Key Length - 128, 256	SP 800-38A
AES-CBC	C1026	Key Length - 128, 256	SP 800-38A
AES-GCM	A4446	Key Length - 128, 256	SP 800-38D
AES-GCM	C1026	Key Length - 128, 256	SP 800-38D
Counter DRBG	A4446	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA-1	C1026	-	FIPS 198-1
HMAC-SHA2-224	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	C1026	-	FIPS 198-1
HMAC-SHA2-384	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	C1026	-	FIPS 198-1
HMAC-SHA2-512	A4446	Key Length - Key Length: 256-448 Increment 8, Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	C1026	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4446	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived	SP 800-135 Rev. 1

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm	CAVP Cert	Properties	Reference
		Keying Material Length: 3072 Hash Algorithm - SHA-1	
KDF SNMP (CVL)	A4446	Password Length - Password Length: 256, 64	SP 800-135 Rev. 1
KDF SSH (CVL)	A4446	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A4446	Key Generation Mode - B.3.4 Modulo - 2048, 3072, 4096 Hash Algorithm - SHA2-256 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A4446	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA-1	C1026	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-224	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	C1026	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	C1026	Message Length - Message Length: 0-102400 Increment 8	FIPS 180-4
SHA2-512	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	C1026	Message Length - Message Length: 0-102400 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4446	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 5: Approved Algorithms - [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per section 4 example 1

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Properties	Implementation	Reference
			in SP800-133rev2 (vendor affirmed) and FIPS 140-3 IG D.H. A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG (A4446)

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
3DES	Used for symmetric encryption in SSHv2, TLSv1, TLSv1.2, IPsec/IKEv2, and SNMPv3
[ASA-CM] 3DES	Used for symmetric encryption in ASA-CM SSHv2, TLSv1, TLSv1.2, IPsec/IKEv2, and SNMPv3 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]
ChaCha20-poly1305	Used for authenticated symmetric encryption in SSHv2, and TLSv1.3
[ASA-CM] ChaCha20-poly1305	Used for authenticated symmetric encryption in ASA-CM SSHv2, and TLSv1.3 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC (SSHv2)	CKG KAS-Full	KAS ECC used in SSHv2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2,	KAS-ECC-SSC Sp800-56Ar3: (A4446) Curves: P-256, P-384, P-521 KDF SSH: (A4446) Counter DRBG:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
			Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	(A4446) CKG: () Key Type: Asymmetric
[ASA-CM] KAS-ECC (SSHv2)	CKG KAS-Full	KAS ECC used in ASA-CM SSHv2 service [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A4446) Curves: P-256, P-384, P-521 KDF SSH: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
KAS-FFC (SSHv2)	CKG KAS-Full	KAS FFC used in SSHv2 service	Caveat:Key establishment methodology provides between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation: MODP-2048, MODP-3072, MODP-4096 Safe Primes Key Generation: (A4446) KDF SSH: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] KAS-FFC (SSHv2)	CKG KAS-Full	KAS FFC used in ASA-CM SSHv2 service [Cisco Adaptive	Caveat: Key establishment methodology provides	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		Security Appliance on 4K/9K Cryptographic Module]	between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	Parameter Generation: MODP-2048, MODP-3072, MODP-4096 Safe Primes Key Generation: (A4446) KDF SSH: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
KAS-ECC (TLSv1.2)	CKG KAS-Full	KAS ECC keygen used in TLSv1.2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A4446) Curves: P-256, P-384, P-521 TLS v1.2 KDF RFC7627: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] KAS-ECC (TLSv1.2)	CKG KAS-Full	KAS ECC used in ASA-CM TLSv1.2 service [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Caveat: Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG	KAS-ECC-SSC Sp800-56Ar3: (A4446) Curves: P-256, P-384, P-521 TLS v1.2 KDF RFC7627: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
			2.4.B SP 800-135rev1 CVL	
KAS-FFC (TLSv1.2)	CKG KAS-Full	KAS FFC keygen used in TLSv1.2 service	Caveat:Key establishment methodology provides between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation: ffdhe2048, ffdhe3072, ffdhe4096 Safe Primes Key Generation: (A4446) TLS v1.2 KDF RFC7627: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] KAS-FFC (TLSv1.2)	CKG KAS-Full	KAS FFC used in ASA-CM TLSv1.2 service [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Caveat: Key establishment methodology provides between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation: ffdhe2048, ffdhe3072, ffdhe4096 Safe Primes Key Generation: (A4446) TLS v1.2 KDF RFC7627: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
KAS-ECC (IKEv2)	CKG KAS-Full	KAS ECC keygen used in IKEv2 service	Caveat:Key establishment methodology	KAS-ECC-SSC Sp800-56Ar3:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
			provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	(A4446) Curves: P-256, P-384, P-521 KDF IKEv2: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] KAS-ECC (IKEv2)	CKG KAS-Full	KAS ECC used in ASA-CM IKEv2 service [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A4446) Curves: P-256, P-384, P-521 KDF IKEv2: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
KAS-FFC (IKEv2)	CKG KAS-Full	KAS FFC keygen used in IKEv2 service	Caveat:Key establishment methodology provides between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation: MODP-2048, MODP-3072, MODP-4096 Safe Primes Key Generation: (A4446) KDF IKEv2: (A4446) Counter DRBG: (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
				CKG: () Key Type: Asymmetric
[ASA-CM] KAS-FFC (IKEv2)	CKG KAS-Full	KAS FFC used in ASA-CM IKEv2 service [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Caveat:Key establishment methodology provides between 112 and 152 bits of security strength IG:IG D.F Scenario 2, Path 2 (Split) Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation: MODP-2048, MODP-3072, MODP-4096 Safe Primes Key Generation: (A4446) KDF IKEv2: (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved "Combination" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
[ASA-CM] KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via ASA-CM TLSv1.2 service by using AES and HMAC [Cisco Adaptive Security Appliance on 4K/9K	Standard:SP 800-38F IG D.G:Approved "Combination" method Caveat:Key establishment methodology	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		Cryptographic Module]	provides 128 or 256 bits of security strength	384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved "Authenticated" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-GCM: (A4446) Key Length: 128, 256
[ASA-CM] KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via ASA-CM TLSv1.2 service by using AES-GCM [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Standard:SP 800-38F IG D.G:Approved "Authenticated" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-GCM: (A4446) Key Length: 128, 256
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved "Combination" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
[ASA-CM] KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via ASA-CM SSHv2 service by	Standard:SP 800-38F IG	AES-CBC: (A4446) Key Length:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		using AES and HMAC [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	D.G:Approved "Combination" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved "Authenticated" method Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-GCM: (A4446) Key Length: 128, 256
[ASA-CM] KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via ASA-CM SSHv2 service by using AES-GCM [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Standard:SP 800-38F IG D.G:Approved "Authenticated" method Caveat: Key establishment methodology provides 128 or 256 bits of security strength	AES-GCM: (A4446) Key Length: 128, 256
RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for SSHv2, TLSv1.2, and IKEv2 services		RSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for ASA-CM SSHv2, TLSv1.2, and		RSA KeyGen (FIPS186-4): (A4446) Counter

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		DRBG: (A4446) CKG: () Key Type: Asymmetric
ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2, TLSv1.2 and IKEv2 services		ECDSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for ASA-CM SSHv2, TLSv1.2 and IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		ECDSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) CKG: () Key Type: Asymmetric
RSA SigGen (SSHv2, TLSv1.2, IKEv2)	DigSig-SigGen	RSA SigGen for SSHv2, TLSv1.2, and IKEv2 services		RSA SigGen (FIPS186-4): (A4446)
[ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2)	DigSig-SigGen	RSA SigGen for ASA-CM SSHv2, TLSv1.2, and IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		RSA SigGen (FIPS186-4): (A4446)
ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	DigSig-SigGen	ECDSA SigGen for TLSv1.2, and IKEv2 services		ECDSA SigGen (FIPS186-4): (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
[ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	DigSig-SigGen	ECDSA SigGen for ASA-CM TLSv1.2, and IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		ECDSA SigGen (FIPS186-4): (A4446)
RSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	RSA SigVer for SSHv2, TLSv1.2, and IKEv2 services		RSA SigVer (FIPS186-4): (A4446)
[ASA-CM] RSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	RSA SigVer for ASA-CM SSHv2, TLSv1.2, and IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		RSA SigVer (FIPS186-4): (A4446)
ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	ECDSA SigVer for TLSv1.2 and IKEv2 services		ECDSA SigVer (FIPS186-4): (A4446)
[ASA-CM] ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	ECDSA SigVer for ASA-CM TLSv1.2 and IKEv2 services [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		ECDSA SigVer (FIPS186-4): (A4446)
Session Encryption/Decryption (SSHv2)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CBC: (A4446) Key Length: 128, 256 AES-GCM: (A4446) Key Length: 128, 256

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
[ASA-CM] Session Encryption/Decryption (SSHv2)	BC-Auth BC-UnAuth	ASA-CM SSHv2 session protection [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		AES-CBC: (A4446) Key Length: 128, 256 AES-GCM: (A4446) Key Length: 128, 256
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-GCM: (A4446) Key Length: 128, 256 AES-CBC: (A4446) Key Length: 128, 256
[ASA-CM] Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	ASA-CM TLSv1.2 session protection [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		AES-GCM: (A4446) Key Length: 128, 256 AES-CBC: (A4446) Key Length: 128, 256
Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	IPSec/IKE session protection		AES-CBC: (A4446) AES-GCM: (A4446)
[ASA-CM] Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	ASA-CM IPSec/IKE session protection [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		AES-CBC: (A4446, C1026) AES-GCM: (A4446, C1026)
Session Encryption/Decryption (SNMPv3)	BC-UnAuth	SNMPv3 sesssion protection		AES-CBC: (A4446)
[ASA-CM] Session Encryption/Decryption (SNMPv3)	BC-UnAuth	ASA-CM SNMPv3 sesssion protection [Cisco Adaptive		AES-CBC: (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		Security Appliance on 4K/9K Cryptographic Module]		
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
[ASA-CM] Session Authentication (SSHv2)	MAC	ASA-CM SSHv2 session authentication [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
[ASA-CM] Session Authentication (TLSv1.2)	MAC	ASA-CM TLSv1.2 session authentication [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)
Session Authentication (IPSec/IKEv2)	MAC	IPSec/IKEv2 session authentication		HMAC-SHA-1: (A4446) HMAC-SHA2-

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
				256: (A4446) HMAC-SHA2-384: (A4446) HMAC-SHA2-512: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) SHA2-512: (A4446)
[ASA-CM] Session Authentication (IPSec/IKEv2)	MAC	ASA-CM IPSec/IKEv2 session authentication [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		HMAC-SHA-1: (A4446, C1026) HMAC-SHA2-256: (A4446, C1026) HMAC-SHA2-384: (A4446, C1026) HMAC-SHA2-512: (A4446, C1026) SHA-1: (A4446, C1026) SHA2-256: (A4446, C1026) SHA2-384: (A4446, C1026) SHA2-512: (A4446, C1026)
Session Authentication (SNMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A4446) SHA-1: (A4446) HMAC-SHA2-384: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) HMAC-SHA2-224: (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
				SHA2-224: (A4446) HMAC-SHA2-256: (A4446)
[ASA-CM] Session Authentication (SNMPv3)	MAC	ASA-CM SNMPv3 session authentication [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		HMAC-SHA-1: (A4446) SHA-1: (A4446) HMAC-SHA2-384: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) HMAC-SHA2-224: (A4446) SHA2-224: (A4446) HMAC-SHA2-256: (A4446)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys		KDF SSH: (A4446)
[ASA-CM] SSHv2 Keying Materials Development	KAS-135KDF	ASA-CM SSHv2 session keying materials, used to derive SSHv2 session keys [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		KDF SSH: (A4446)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLS session keys		TLS v1.2 KDF RFC7627: (A4446)
[ASA-CM] TLSv1.2 Keying Materials Development	KAS-135KDF	ASA-CM TLSv1.2 session keying materials, used to derive TLS		TLS v1.2 KDF RFC7627: (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
		session keys [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		
IPSec/IKEv2 Keying Materials Development	KAS-135KDF	IPSec/IKEv2 session keying materials, used to derive IPSec/IKEv2 session keys		KDF IKEv2: (A4446)
[ASA-CM] IPSec/IKEv2 Keying Materials Development	KAS-135KDF	ASA-CM IPSec/IKEv2 session keying materials, used to derive IPSec/IKEv2 session keys [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		KDF IKEv2: (A4446)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A4446)
[ASA-CM] SNMPv3 Keying Materials Development	KAS-135KDF	ASA-CM SNMPv3 session keying materials, used to derive SNMPv3 session keys [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		KDF SNMP: (A4446)
Firmware Load Test	MAC	MAC for firmware load test		HMAC-SHA2-512: (A4446)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Description	Properties	Algorithms
[ASA-CM] Firmware Load Test	MAC	MAC for ASA-CM firmware load test [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		HMAC-SHA2-512: (A4446)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A4446)
[ASA-CM] DRBG Function	DRBG	Used for ASA-CM DRBG generation [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]		Counter DRBG: (A4446)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

- The module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1d following RFC 5647 for SSH. A new IV parameter is generated by the module for each AES-GCM encryption. As shown in Section 7.1 of RFC 5647, the IV consists of a 4-byte fixed field and an 8-byte invocation counter. The initial IV value is generated as shown in Figure 1 of RFC 5647 and the fixed field of this IV remains the same for the duration of the session. Therefore, the method for minimizing the (key, IV) collision probability within the same session depends entirely on the management of the invocation field of the IV. The invocation counter is treated as a 64-bit integer and is incremented by one when performing an AES-GCM encryption of a new binary packet. The formation of binary packets is explained in Section 7.2 of RFC 5647.

- The module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1a following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical.The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. 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 handshake to establish a new encryption key. In case the

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1b following RFC 7296 for IPsec. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are. 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 handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module was algorithm tested based on the FIPS 186-4 standard Digital Signatures. According to IG C.K, this module is 186-5 compliant as all 186-4 CAVP tests performed are mathematically identical to the 186-5 CAVP tests. The Module does not support 186-4 DSA or RSA X9.31 for Signature Generation or Signature Verification.

2.8 RBG and Entropy

Cert Number	Vendor Name
E3	Cisco Systems, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Cisco Jitter Entropy Source	Non-Physical	Intel i3-3115C (Ivy Bridge), Intel Xeon Platinum 8160 (Skylake), Intel Xeon Platinum 8176 (Skylake), Intel Xeon Silver 4116 (Skylake), Intel Xeon Gold 6130T (Skylake), Intel Xeon Gold 6138T (Skylake), Intel Xeon Gold 6152 (Skylake)	256 bits	Full Entropy	A2810 (SHA3-256)

Table 10: Entropy Sources

The module employs a Deterministic Random Bit Generator (DRBG) implementation based on SP800-90Arev1. This DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

The DRBG implemented is an AES-256 Counter DRBG, seeded by the entropy source described in the table above. The Counter DRBG utilizes the Derivation Function. It does not employ prediction resistance.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy). Additionally, the DRBG is reseeded with a 256-bits long entropy input (corresponding to 256 bits of entropy).

2.9 Key Generation

The module generates RSA, ECDSA, ECDH, and DH asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

KAS-FFC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.
- The module supports the use of the safe primes defined in RFC 4419 (SSH), RFC 7919 (TLS) and RFC 3526 (IKE). Note that the module only implements domain parameter generation, key pair generation and verification, and shared secret computation.
    - SSH (RFC 4419):
        - MODP-2048 (ID = 14)
        - MODP-3072 (ID = 15)
        - MODP-4096 (ID = 16)
    - TLS (RFC 7919):
        - ffdhe2048 (ID = 256)
        - ffdhe3072 (ID = 257)
        - ffdhe4096 (ID = 258)
    - IKE (RFC 3526):
        - MODP-2048 (ID = 14)
        - MODP-3072 (ID = 15)
        - MODP-4096 (ID = 16)

KAS-ECC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

- The modules NIST recommended curves correspond to the curves uses in these industry protocols

    - TLS (RFC 4492):
        - P-256 (secp256r1)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

        - P-384 (secp384r1)
        - P-521 (secp521r1)

    - IKE (RFC 5903):
        - P-256 (secp256r1)
        - P-384 (secp384r1)
        - P-521 (secp521r1)

The module also provides the following key transport mechanisms:

- Key wrapping using AES-GCM with a security strength of 128 or 256 bits.
- Key wrapping using AES-CBC with a security strength of 128 or 256 bits with HMAC-SHA-1, HMAC-SHA2-256 or HMAC-SHA2-384.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, SNMPv3 and IPsec/IKEv2 industrial protocols. Please refer to the Security Function Implementations Table for more information. No parts of IPSec/IKEv2, SNMPv3, SSH and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Ethernet Port, SFP (1G) port, SFP+ (10G) port, and Console Port	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port and Console Port	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port, Console Port and RESET	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port, Console Port and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	Power	Provide the Power Supply to the module.

Table 11: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

the module (data input, data output, control input, control output and status output) as above. The module's data output interface will be disabled when performing pre-operational self-tests, loading new firmware, zeroizing keys, or when in an error state.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	The minimum length is eight (8) characters (94 possible characters). The configuration supports at most ten failed attempts to authenticate in a one-minute period.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000.	The probability of successfully authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000.
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112),	RSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details.	The probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	which is less than 1/100,000.			
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.	ECDSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details.	The probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details.

Table 12: Authentication Methods

The module implements identity-based authentication. The module supports Crypto Officer role and the User role. The module also allows the concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Password RSA-Based Certificate ECDSA-Based Certificate
[ASA-CM] Crypto Officer	Identity	CO	Password RSA-Based Certificate ECDSA-Based Certificate

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Type	Operator Type	Authentication Methods
User	Identity	User	Password RSA-Based Certificate ECDSA-Based Certificate
[ASA-CM] User	Identity	User	Password RSA-Based Certificate ECDSA-Based Certificate

Table 13: Roles

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provide Module's current status (return codes and/or syslog messages)	N/A	Command used to show Module's Status	Module's Operational Status	None	Crypto Officer User
[ASA-CM] Show Status	Provide ASA-CM Module's current status (return codes and/or syslog messages)	N/A	Command used to show Module's Status	Module's Operational Status	None	[ASA-CM] Crypto Officer User
Show Version	Provide Module's name and version information	N/A	Command to show version	Module's ID and versioning information	None	Crypto Officer User
[ASA-CM] Show Version	Provide ASA-CM Module's name and version information	N/A	Command to show version	Module's ID and versioning information	None	[ASA-CM] Crypto Officer [ASA-CM] User
Perform Self-Tests	Perform Self-Tests (Pre-operational self-test and Conditional Self-Tests)	N/A	Command to trigger Self-Test	Status of the self-tests results	None	Crypto Officer User Unauthenticated
[ASA-CM] Perform Self-Tests	Perform ASA-CM Self-Tests (Pre-operational	N/A	Command to trigger Self-Test	Status of the self-tests results	None	[ASA-CM] Crypto Officer [ASA-CM] User Unauthenticated

© 2021-2026 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	self-test and Conditional Self-Tests)					
Perform Zeroization	Perform Zeroization	N/A	Command to zeroize the module	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State V value: Z - DRBG Key: Z - User Password: Z - Crypto Officer Password: Z - Firmware Load Test Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH RSA Private Key: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH RSA Public Key: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLS DH Private Key: Z - TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS RSA Private Key: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - IPSec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE ECDSA Public

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED: Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z
[ASA-CM] Perform Zeroization	Perform Zeroization on ASA-CM	N/A	Command to zeroize the module	Status of the SSPs zeroization	None	[ASA-CM] Crypto Officer - [ASA-CM] DRBG Entropy Input: Z - [ASA-CM] DRBG Seed: Z - [ASA-CM] DRBG Internal State V value: Z - [ASA-CM] DRBG Key: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- [ASA-CM] User Password: Z - [ASA-CM] Crypto Officer Password: Z - [ASA-CM] Firmware Load Test Key: Z - [ASA-CM] SSH DH Private Key: Z - [ASA-CM] SSH DH Public Key: Z - [ASA-CM] SSH Peer DH Public Key: Z - [ASA-CM] SSH DH Shared Secret: Z - [ASA-CM] SSH ECDH Private Key: Z - [ASA-CM] SSH ECDH Public Key: Z - [ASA-CM] SSH Peer ECDH Public Key: Z - [ASA-CM] SSH ECDH Shared Secret: Z - [ASA-CM] SSH RSA Private Key: Z - [ASA-CM] SSH

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RSA Public Key: Z - [ASA-CM] SSH ECDSA Private Key: Z - [ASA-CM] SSH ECDSA Public Key: Z - [ASA-CM] SSH Session Encryption Key: Z - [ASA-CM] SSH Session Authentication Key: Z - [ASA-CM] TLS DH Private Key: Z - [ASA-CM] TLS DH Public Key: Z - [ASA-CM] TLS Peer DH Public Key: Z - [ASA-CM] TLS DH Shared Secret: Z - [ASA-CM] TLS ECDH Private Key: Z - [ASA-CM] TLS ECDH Public Key: Z - [ASA-CM] TLS Peer ECDH

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: Z - [ASA-CM] TLS ECDH Shared Secret: Z - [ASA-CM] TLS ECDSA Private Key: Z - [ASA-CM] TLS ECDSA Public Key: Z - [ASA-CM] TLS RSA Private Key: Z - [ASA-CM] TLS RSA Public Key: Z - [ASA-CM] TLS Master Secret: Z - [ASA-CM] TLS Session Encryption Key: Z - [ASA-CM] TLS Session Authentication Key: Z - [ASA-CM] IPSec/IKE DH Private Key: Z - [ASA-CM] IPSec/IKE DH Public Key: Z - [ASA-CM] IPSec/IKE Peer DH Public Key: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- [ASA-CM] IPSec/IKE DH Shared Secret: Z - [ASA-CM] IPSec/IKE ECDH Private Key: Z - [ASA-CM] IPSec/IKE ECDH Public Key: Z - [ASA-CM] IPSec/IKE Peer ECDH Public Key: Z - [ASA-CM] IPSec/IKE ECDH Shared Secret: Z - [ASA-CM] IPSec/IKE ECDSA Private Key: Z - [ASA-CM] IPSec/IKE ECDSA Public Key: Z - [ASA-CM] IPSec/IKE RSA Private Key: Z - [ASA-CM] IPSec/IKE RSA Public Key: Z - [ASA-CM] IPSec/IKE Pre-shared Secret: Z - [ASA-CM] SKEYSEED: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- [ASA-CM] IPSec/IKE Session Encryption Key: Z - [ASA-CM] IPSec/IKE Authentication Key: Z - [ASA-CM] SNMPv3 Shared Secret: Z - [ASA-CM] SNMPv3 Encryption Key: Z - [ASA-CM] SNMPv3 Authentication Key: Z
Configure Network	Sets configuration of the systems	N/A	Commands to configure the network	Status of the completion of network configuration status	None	Crypto Officer
[ASA-CM] Configure Network	Sets configuration of the ASA-CM systems	N/A	Commands to configure the network	Status of the completion of network configuration status	None	[ASA-CM] Crypto Officer
Crypto Officer Authentication	CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	Crypto Officer - Crypto Officer Password: W,Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
[ASA-CM] Crypto Officer Authentication	ASA-CM CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	[ASA-CM] Crypto Officer - [ASA-CM] Crypto Officer Password: W,Z
User Authentication	User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	User - User Password: W,Z
[ASA-CM] User Authentication	ASA-CM User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	[ASA-CM] User - [ASA-CM] User Password: W,Z
Configure Bypass Capability	Sets the Bypass capability	N/A	CLI Bypass commands	Status of the completion of Bypass capability configuration	None	Crypto Officer
[ASA-CM] Configure Bypass Capability	Sets the Bypass capability for the ASA-CM	N/A	CLI Bypass commands	Status of the completion of Bypass capability configuration	None	[ASA-CM] Crypto Officer
Configure SSHv2 Function	Configure SSHv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and SSHv2 configuration success status message	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	Crypto Officer - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						State V value: W,E - DRBG Key: W,E
[ASA-CM] Configure SSHv2 Function	Configure ASA-CM SSHv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and SSHv2 configuration success status message	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	[ASA-CM] KTS (TLSv1.2 with AES and HMAC) [ASA-CM] KTS (TLSv1.2 with AES-GCM) [ASA-CM] KTS (SSHv2 with AES and HMAC) [ASA-CM] KTS (SSHv2 with AES-GCM) [ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2) [ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] DRBG Function	[ASA-CM] Crypto Officer - [ASA-CM] SSH RSA Private Key: W,E - [ASA-CM] SSH RSA Public Key: W,E - [ASA-CM] SSH ECDSA Private Key: W,E - [ASA-CM] SSH ECDSA Public Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E
Configure HTTPS over TLSv1.2 Function	Configure HTTPS over TLSv1.2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and HTTPS	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES	Crypto Officer - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		over TLSv1.2 configuration success status message			and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	- TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
[ASA-CM] Configure HTTPS over TLSv1.2 Function	Configure ASA-CM HTTPS over TLSv1.2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and HTTPS over TLSv1.2 configuration success status message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	[ASA-CM] KTS (TLSv1.2 with AES and HMAC) [ASA-CM] KTS (TLSv1.2 with AES-GCM) [ASA-CM] KTS (SSHv2 with AES and HMAC) [ASA-CM] KTS (SSHv2 with AES-GCM) [ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2) [ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] DRBG Function	[ASA-CM] Crypto Officer - [ASA-CM] TLS ECDSA Private Key: W,E - [ASA-CM] TLS ECDSA Public Key: W,E - [ASA-CM] TLS RSA Private Key: W,E - [ASA-CM] TLS RSA Public Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						State V value: W,E - [ASA-CM] DRBG Key: W,E
Configure IPsec/IKEv2 Function	Configure IPSec/IKEv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" with IPsec/IKEv2 configuration success status message	Commands to configure IPsec/IKEv2	Status of the completion of IPsec/IKEv2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) DRBG Function	Crypto Officer - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
[ASA-CM] Configure IPsec/IKEv2 Function	Configure ASA-CM IPSec/IKEv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" with IPsec/IKEv2 configuration	Commands to configure IPsec/IKEv2	Status of the completion of IPsec/IKEv2 configuration	[ASA-CM] KTS (TLSv1.2 with AES and HMAC) [ASA-CM] KTS (TLSv1.2 with AES-GCM) [ASA-CM] KTS (SSHv2 with AES and	[ASA-CM] Crypto Officer - [ASA-CM] IPSec/IKE ECDSA Private Key: W,E - [ASA-CM] IPSec/IKE

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		success status message			HMAC) [ASA-CM] KTS (SSHv2 with AES-GCM) [ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2) [ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] DRBG Function	ECDSA Public Key: W,E - [ASA-CM] IPSec/IKE RSA Private Key: W,E - [ASA-CM] IPSec/IKE RSA Public Key: W,E - [ASA-CM] IPSec/IKE Pre-shared Secret: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E
Configure SNMPv3 Function	Configure SNMPv3 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and SNMPv3 configuration success status message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM)	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
[ASA-CM] Configure SNMPv3 Function	Configure ASA-CM SNMPv3 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and SNMPv3 configuration success status message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	[ASA-CM] KTS (TLSv1.2 with AES and HMAC) [ASA-CM] KTS (TLSv1.2 with AES-GCM) [ASA-CM] KTS (SSHv2 with AES and HMAC) [ASA-CM] KTS (SSHv2 with AES-GCM)	[ASA-CM] Crypto Officer - [ASA-CM] SNMPv3 Shared Secret: W,E - [ASA-CM] SNMPv3 Encryption Key: W,E - [ASA-CM] SNMPv3 Authentication Key: W,E
Run SSHv2 Function	Execute SSHv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful SSHv2 log message	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-ECC (SSHv2) KAS-FFC (SSHv2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (SSHv2) Session Authentication (SSHv2)	Crypto Officer - SSH DH Private Key: W,E - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SSHv2 Keying Materials Development DRBG Function	- SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E User - SSH DH Private Key: W,E - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
[ASA-CM] Run SSHv2 Function	Execute ASA-CM SSHv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	[ASA-CM] KAS-ECC (SSHv2) [ASA-CM] KAS-FFC (SSHv2) [ASA-CM] KTS (SSHv2 with AES and	[ASA-CM] Crypto Officer - [ASA-CM] SSH DH Private Key: W,E - [ASA-CM] SSH

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		SSHv2 log message			HMAC) [ASA-CM] KTS (SSHv2 with AES-GCM) [ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2) [ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] RSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] Session Encryption/Decryption (SSHv2) [ASA-CM] Session Authentication (SSHv2) [ASA-CM] SSHv2 Keying Materials Development [ASA-CM] DRBG Function	DH Public Key: W,E - [ASA-CM] SSH Peer DH Public Key: W,E - [ASA-CM] SSH DH Shared Secret: W,E - [ASA-CM] SSH ECDH Private Key: W,E - [ASA-CM] SSH ECDH Public Key: W,E - [ASA-CM] SSH Peer ECDH Public Key: W,E - [ASA-CM] SSH ECDH Shared Secret: W,E - [ASA-CM] SSH RSA Private Key: W,E - [ASA-CM] SSH RSA Public Key: W,E - [ASA-CM] SSH ECDSA Private Key: W,E - [ASA-CM] SSH ECDSA Public Key: W,E - [ASA-CM] SSH Session Encryption Key:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - [ASA-CM] SSH Session Authentication Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E [ASA-CM] User - [ASA-CM] SSH DH Private Key: W,E - [ASA-CM] SSH DH Public Key: W,E - [ASA-CM] SSH Peer DH Public Key: W,E - [ASA-CM] SSH DH Shared Secret: W,E - [ASA-CM] SSH ECDH Private Key: W,E - [ASA-CM] SSH ECDH Public

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E - [ASA-CM] SSH Peer ECDH Public Key: W,E - [ASA-CM] SSH ECDH Shared Secret: W,E - [ASA-CM] SSH RSA Private Key: W,E - [ASA-CM] SSH RSA Public Key: W,E - [ASA-CM] SSH ECDSA Private Key: W,E - [ASA-CM] SSH ECDSA Public Key: W,E - [ASA-CM] SSH Session Encryption Key: W,E - [ASA-CM] SSH Session Authentication Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						State V value: W,E - [ASA-CM] DRBG Key: W,E
Run HTTPS over TLSv1.2 Function	Execute HTTPS over TLSv1.2 function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful HTTPS over TLSv1.2 log message	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (TLSv1.2) Session Authentication (TLSv1.2) TLSv1.2 Keying Materials Development DRBG Function	Crypto Officer - TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E User - TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
[ASA-CM] Run HTTPS over TLSv1.2 Function	Execute ASA-CM HTTPS over TLSv1.2 function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful HTTPS over TLSv1.2 log message	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	[ASA-CM] KAS-ECC (TLSv1.2) [ASA-CM] KAS-FFC (TLSv1.2) [ASA-CM] KTS (TLSv1.2 with AES and HMAC) [ASA-CM] KTS (TLSv1.2 with AES-GCM) [ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2)	[ASA-CM] Crypto Officer - [ASA-CM] TLS DH Private Key: W,E - [ASA-CM] TLS DH Public Key: W,E - [ASA-CM] TLS Peer DH Public Key: W,E - [ASA-CM] TLS DH Shared

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					[ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] RSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] Session Encryption/Decryption (TLSv1.2) [ASA-CM] Session Authentication (TLSv1.2) [ASA-CM] TLSv1.2 Keying Materials Development [ASA-CM] DRBG Function	Secret: W,E - [ASA-CM] TLS ECDH Private Key: W,E - [ASA-CM] TLS ECDH Public Key: W,E - [ASA-CM] TLS Peer ECDH Public Key: W,E - [ASA-CM] TLS ECDH Shared Secret: W,E - [ASA-CM] TLS ECDSA Private Key: W,E - [ASA-CM] TLS ECDSA Public Key: W,E - [ASA-CM] TLS RSA Private Key: W,E - [ASA-CM] TLS RSA Public Key: W,E - [ASA-CM] TLS Master Secret: W,E - [ASA-CM] TLS Session Encryption Key: W,E - [ASA-CM] TLS Session Authentication

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E [ASA-CM] User - [ASA-CM] TLS DH Private Key: W,E - [ASA-CM] TLS DH Public Key: W,E - [ASA-CM] TLS Peer DH Public Key: W,E - [ASA-CM] TLS DH Shared Secret: W,E - [ASA-CM] TLS ECDH Private Key: W,E - [ASA-CM] TLS ECDH Public Key: W,E - [ASA-CM] TLS Peer ECDH Public Key: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- [ASA-CM] TLS ECDH Shared Secret: W,E - [ASA-CM] TLS ECDSA Private Key: W,E - [ASA-CM] TLS ECDSA Public Key: W,E - [ASA-CM] TLS RSA Private Key: W,E - [ASA-CM] TLS RSA Public Key: W,E - [ASA-CM] TLS Master Secret: W,E - [ASA-CM] TLS Session Encryption Key: W,E - [ASA-CM] TLS Session Authentication Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - [ASA-CM] DRBG Key: W,E
Run IPSec/IKEv2 Function	Execute IPsec/IKEv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and succesful IPsec/IKEv2 log message	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Session Encryption/Decryption (IPSec/IKE) Session Authentication (IPSec/IKEv2) IPSec/IKEv2 Keying Materials Development DRBG Function	Crypto Officer - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E User - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
[ASA-CM] Run IPSec/IKEv2 Function	Execute ASA-CM IPsec/IKEv2 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and succesful IPsec/IKEv2 log message	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	[ASA-CM] KAS-ECC (IKEv2) [ASA-CM] KAS-FFC (IKEv2) [ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2) [ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) [ASA-CM] RSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) [ASA-CM] Session Encryption/Decryption (IPSec/IKE) [ASA-CM] Session Authentication (IPSec/IKEv2) [ASA-CM] IPSec/IKEv2 Keying Materials Development [ASA-CM] DRBG Function	[ASA-CM] Crypto Officer - [ASA-CM] IPSec/IKE DH Private Key: W,E - [ASA-CM] IPSec/IKE DH Public Key: W,E - [ASA-CM] IPSec/IKE Peer DH Public Key: W,E - [ASA-CM] IPSec/IKE DH Shared Secret: W,E - [ASA-CM] IPSec/IKE ECDH Private Key: W,E - [ASA-CM] IPSec/IKE ECDH Public Key: W,E - [ASA-CM] IPSec/IKE Peer ECDH Public Key: W,E - [ASA-CM] IPSec/IKE ECDH Shared Secret:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - [ASA-CM] IPSec/IKE ECDSA Private Key: W,E - [ASA-CM] IPSec/IKE ECDSA Public Key: W,E - [ASA-CM] IPSec/IKE RSA Private Key: W,E - [ASA-CM] IPSec/IKE RSA Public Key: W,E - [ASA-CM] IPSec/IKE Pre-shared Secret: W,E - [ASA-CM] SKEYSEED: W,E - [ASA-CM] IPSec/IKE Session Encryption Key: W,E - [ASA-CM] IPSec/IKE Authentication Key: W,E - [ASA-CM] DRBG Entropy Input: W,E - [ASA-CM]

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E [ASA-CM] User - [ASA-CM] IPSec/IKE DH Private Key: W,E - [ASA-CM] IPSec/IKE DH Public Key: W,E - [ASA-CM] IPSec/IKE Peer DH Public Key: W,E - [ASA-CM] IPSec/IKE DH Shared Secret: W,E - [ASA-CM] IPSec/IKE ECDH Private Key: W,E - [ASA-CM] IPSec/IKE ECDH Public Key: W,E - [ASA-CM] IPSec/IKE Peer ECDH Public Key: W,E - [ASA-CM] IPSec/IKE ECDH

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Shared Secret: W,E - [ASA-CM] IPSec/IKE ECDSA Private Key: W,E - [ASA-CM] IPSec/IKE ECDSA Public Key: W,E - [ASA-CM] IPSec/IKE RSA Private Key: W,E - [ASA-CM] IPSec/IKE RSA Public Key: W,E - [ASA-CM] IPSec/IKE Pre-shared Secret: W,E - [ASA-CM] SKEYSEED: W,E - [ASA-CM] IPSec/IKE Session Encryption Key: W,E - [ASA-CM] IPSec/IKE Authentication Key: W,E - [ASA-CM] DRBG Entropy Input: W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- [ASA-CM] DRBG Seed: W,E - [ASA-CM] DRBG Internal State V value: W,E - [ASA-CM] DRBG Key: W,E
Run SNMPv3 Function	Execute SNMPv3 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful SNMPv3 log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Session Encryption/Decryption (SNMPv3) Session Authentication (SNMPv3) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E User - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E
[ASA-CM] Run SNMPv3 Function	Execute ASA-CM SNMPv3 Function	Status Mode Indicator "FIPS Mode Admin State: Enabled" and successful	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	[ASA-CM] Session Encryption/Decryption (SNMPv3) [ASA-CM] Session Authentication (SNMPv3)	[ASA-CM] Crypto Officer - [ASA-CM] SNMPv3 Shared Secret: W,E - [ASA-CM]

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		SNMPv3 log message			[ASA-CM] SNMPv3 Keying Materials Development	SNMPv3 Encryption Key: W,E - [ASA-CM] SNMPv3 Authentication Key: W,E [ASA-CM] User - [ASA-CM] SNMPv3 Shared Secret: W,E - [ASA-CM] SNMPv3 Encryption Key: W,E - [ASA-CM] SNMPv3 Authentication Key: W,E
Firmware Load Test	Execute the Firmware Load Test	Successful Firmware Loading status message	Commands to load new firmware image	Outcome of the Firmware Load Test	Firmware Load Test	Crypto Officer - Firmware Load Test Key: R
[ASA-CM] Firmware Load Test	Execute the ASA-CM Firmware Load Test	Successful Firmware Loading status message	Commands to load new firmware image	Outcome of the Firmware Load Test	[ASA-CM] Firmware Load Test	[ASA-CM] Crypto Officer - [ASA-CM] Firmware Load Test Key: R

Table 14: Approved Services

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
SSHv2	Run SSHv2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful SSHv2 log message demonstrates the non-approved service	3DES ChaCha20-poly1305	Crypto Officer, User
[ASA-CM] SSHv2	Run SSHv2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful SSHv2 log message demonstrates the non-approved service	[ASA-CM] 3DES [ASA-CM] ChaCha20-poly1305	[ASA-CM] Crypto Officer, [ASA-CM] User
TLSv1	Run TLSv1 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1 log message demonstrates the non-approved service	3DES	Crypto Officer, User
[ASA-CM] TLSv1	Run TLSv1 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1 log message demonstrates the non-approved service	[ASA-CM] 3DES	[ASA-CM] Crypto Officer, [ASA-CM] User
TLSv1.2	Run TLSv1.2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1.2 log message demonstrates the non-approved service	3DES	Crypto Officer, User
[ASA-CM] TLSv1.2	Run TLSv1.2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1.2 log message demonstrates the non-approved service	[ASA-CM] 3DES	[ASA-CM] Crypto Officer, [ASA-CM] User
TLSv1.3	Run TLSv1.3 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1.3 log message demonstrates the non-approved service	ChaCha20-poly1305	Crypto Officer, User
[ASA-CM] TLSv1.3	Run TLSv1.3 in the non-approved mode using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful TLSv1.3 log	[ASA-CM] ChaCha20-poly1305	[ASA-CM] Crypto Officer, [ASA-CM] User

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

© 2021-2026 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Name	Description	Algorithms	Role
	message demonstrates the non-approved service		
IPsec/IKEv2	Run IPsec/IKEv2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful IPsec/IKEv2 log message demonstrates the non-approved service	3DES	Crypto Officer, User
[ASA-CM] IPsec/IKEv2	Run IPsec/IKEv2 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful IPsec/IKEv2 log message demonstrates the non-approved service	[ASA-CM] 3DES	[ASA-CM] Crypto Officer, [ASA-CM] User
SNMPv3	Run SNMPv3 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful SNMPv3 log message demonstrates the non-approved service	3DES	Crypto Officer, User
[ASA-CM] SNMPv3	Run SNMPv3 using non-approved algorithms. Non-Approved mode indicator "FIPS Mode Admin State: Disabled" and successful SNMPv3 log message demonstrates the non-approved service	[ASA-CM] 3DES	[ASA-CM] Crypto Officer, [ASA-CM] User

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using HMAC-SHA2-512 (HMAC Cert. #A4446) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Bypass Actions and Status

The module implements alternating Bypass service. Traffic output from the module's data output interface can be cryptographically protected via IPSec/IKE VPN, or passed as plaintext (Bypass state), depending on the VPN tunnel establishment on the dedicated data output interface. The operator shall assume Crypto Officer role so as to configure IPSec/IKE VPN capability. If no IPSec/IKE VPN was configured, Module would enter the Bypass state.

Before the module executes the Bypass service (sending out plaintext traffic via the data output interface), the module would conduct two independent internal actions to prevent the inadvertent bypass of plaintext data due to a single error.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1. When Bypass is configured, the module generates a checksum of the configuration and saves it to persistent memory. When the module intends to use the Bypass service it generates a new checksum of the configuration, checks it against the saved checksum. If they match, the bypass service can be used.
2. The module will check if Crypto Officer has configured the dedicated data output interface with Bypass capability. If yes, the module will transition to Bypass state and deliver the traffic from that data output interface in plaintext; if not, the module will send out traffic in ciphertext.

The Crypto Officer can use commands “show access-list” and “show crypto ipsec sa” to verify the module’s Bypass status. In Bypass tests fail, the module would enter an error state, and drop the traffic.

4.7 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.8 Additional Information

The module supports unauthenticated service. The unauthenticated operator can trigger the self-test service by power-cycling the module, and is able to observe the module’s LEDs status.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is provided in the form of binary executable code. To ensure firmware security, the module is protected by RSA 2048 bits with SHA2-512 (RSA Cert. #A4446) algorithm. A Firmware Integrity Test Key (non-SSP) was preloaded to the module’s binary at the factory and used for firmware integrity test only at the pre-operational self-test. The module uses the RSA 2048 bits modulus public key to verify the digital signature. If the firmware integrity test fails, the module would enter to an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the tested platform to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper labels (15 for 4100 Models; 12 for 9300 models) with Part Number: AIR-AP-FIPSKIT=	Recommend 30 Days	Visible inspection of platform for residual evidence of tampering.
Opacity Shield (1) with Part Number: FPR4K-SM-44S (for 4100 models) and FPR-C9300-FIPSKIT= (for 9300 models)	Recommend 30 Days	Visible inspection of platform for evidence of tampering, removal or access.

Table 16: Mechanisms and Actions Required

The module utilizes a production-grade enclosure and removable cover along with tamper evidence labels as the physical security mechanisms.

Appling Tamper Evidence Labels

Step 1: Turn off and unplug the module.

Step 2: Clean the chassis of any grease, dirt, oil or any other material other than the surface coating from manufacture before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Step 3: Apply a label to cover the module as shown in the figures below.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “FIPS” may appear if the label was peeled back.

7.2 User Placed Tamper Seals

Number: Fifteen (15) on the 4100

Number: Twelve (12) on the 9300

Placement:

Figure 5: FPR4100 Series Front view (no TEL present on front)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

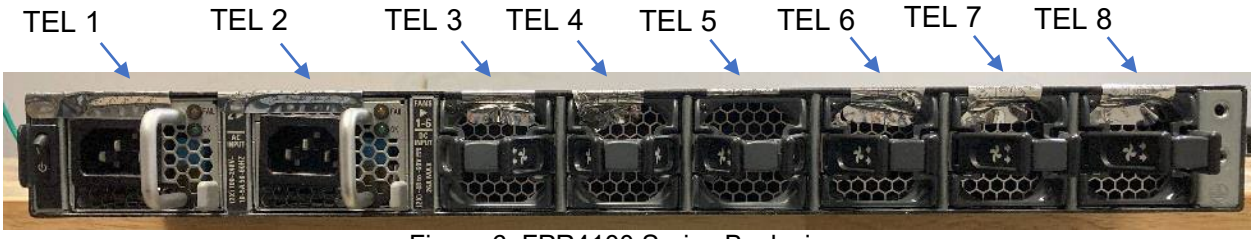


Figure 6: FPR4100 Series Back view

Figure 7: FPR4100 Series Left Side

Figure 8: FPR4100 Series Rear view

Figure 9: FPR4100 Series Top view

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 10: FPR4100 Series Bottom view

Figure 11: FPR9300 Series Front view

Figure 12: FPR9300 Series Right view (Right side has no TELs)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 13: FPR9300 Series Left view (Left side has no TELs)

Figure 14: FPR9300 Series Rear view

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 15: FPR9300 Series Top view

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 16: FPR9300 Series Bottom view

7.3 Filler Panels

FPR 4112, FPR 4115, FPR 4125, FPR 4145 Opacity Shield

FPR-4100-FIPS-KIT=

Before you begin

You need the following to install the FIPS opacity shield:

- #1 Phillips screwdriver
- The following items from the FIPS kit:
  - One FIPS opacity shield
  - Four 8-32 x 0.375-inch screws used to attach the FIPS opacity shield to the cable management brackets
  - Tamper-evident labels (TELs)
- The following items from the Firepower 4100 accessory kit:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- Two cable management brackets
- Four 8-32 x 0.375-inch screws used to attach the cable management brackets to the slide rail locking brackets

Procedure

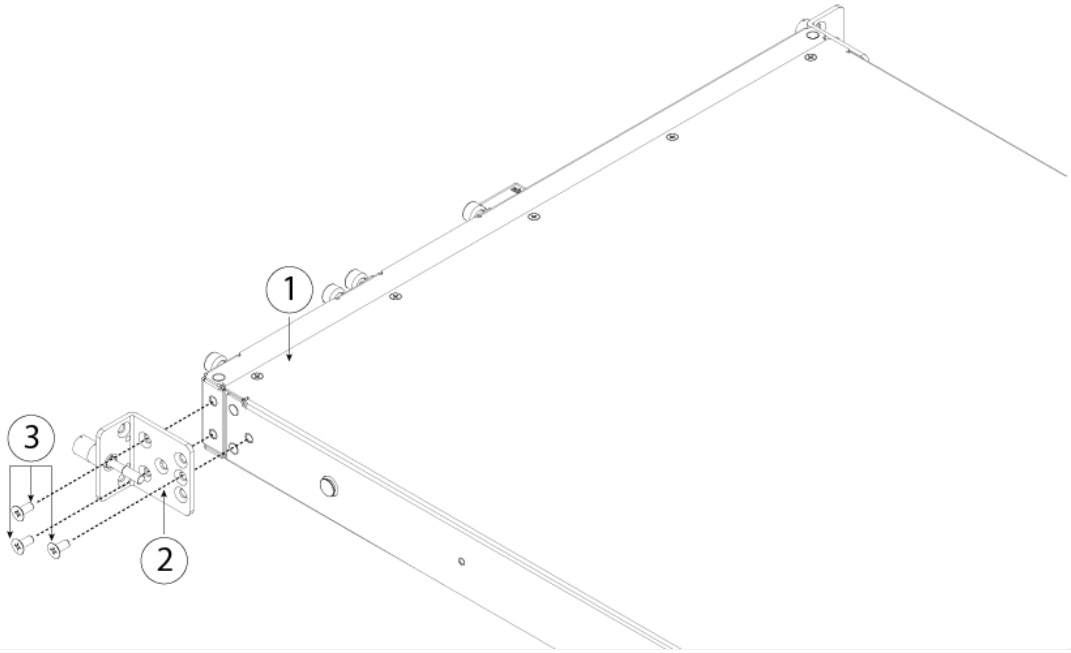
Step 1 Copy the serial number on a label and attach it to the chassis where it can be retrieved easily for future use if needed. To find the serial number, see Serial Number Location.

Step 2 Pull the chassis out of the rack until the release latches catch.

Step 3 If you have not already done so, attach a slide rail locking bracket to each side of the chassis using the six 8-32 x 0.375-inch Phillips screws provided in the accessory kit.

Note: You should have completed this step while preforming the procedure described in Rack-Mount the Chassis.

Figure 15. Attach the Slide Rail Locking Bracket to the Side of the Chassis

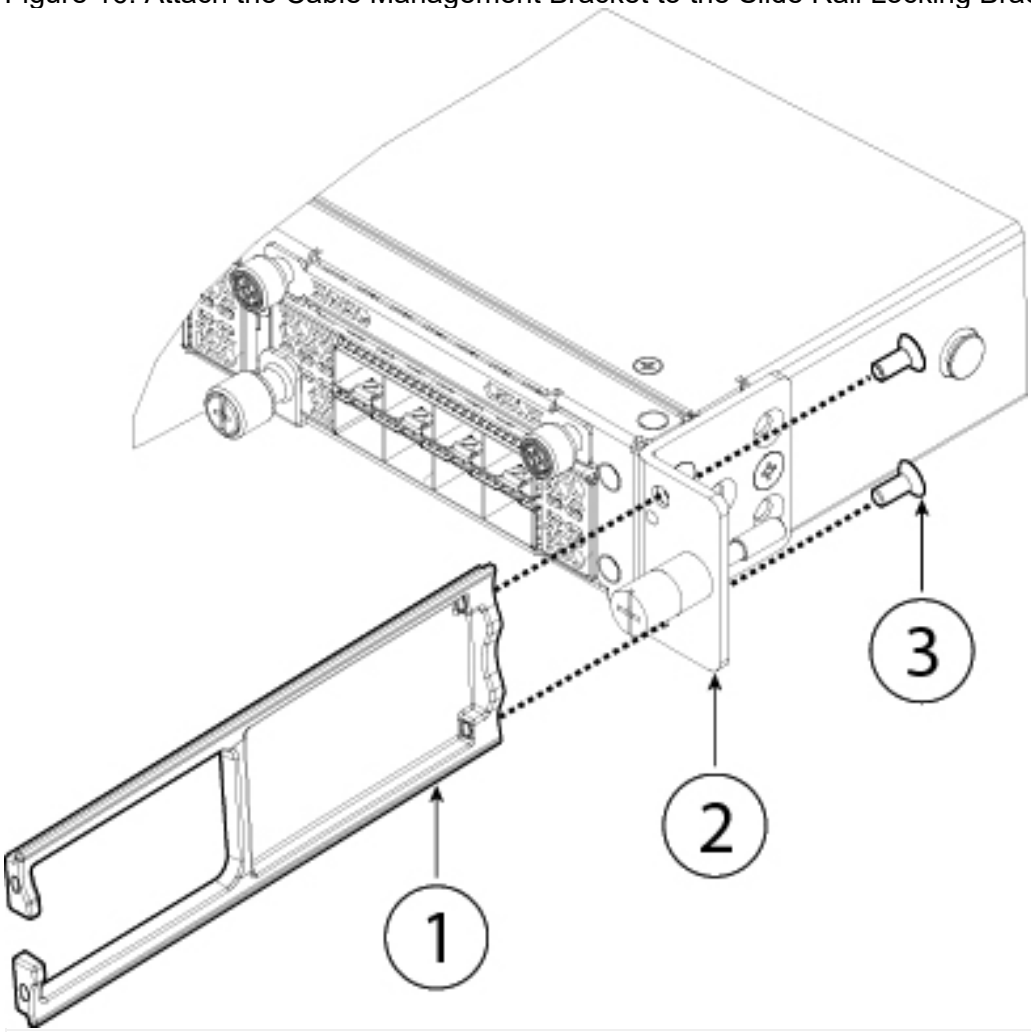


1	Chassis	**2**	Slide rail locking bracket
3	8-32 x 0.375-inch Phillips screws (three per side)		

Step 4 Attach a cable management bracket to each slide rail locking bracket using the four 8-32 x 0.375-inch Phillips screws provided in the accessory kit.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 16. Attach the Cable Management Bracket to the Slide Rail Locking Bracket



1	Cable management bracket	**2**	Slide rail locking bracket
3	8-32 x 0.375 inch Phillips screws (two per side)		

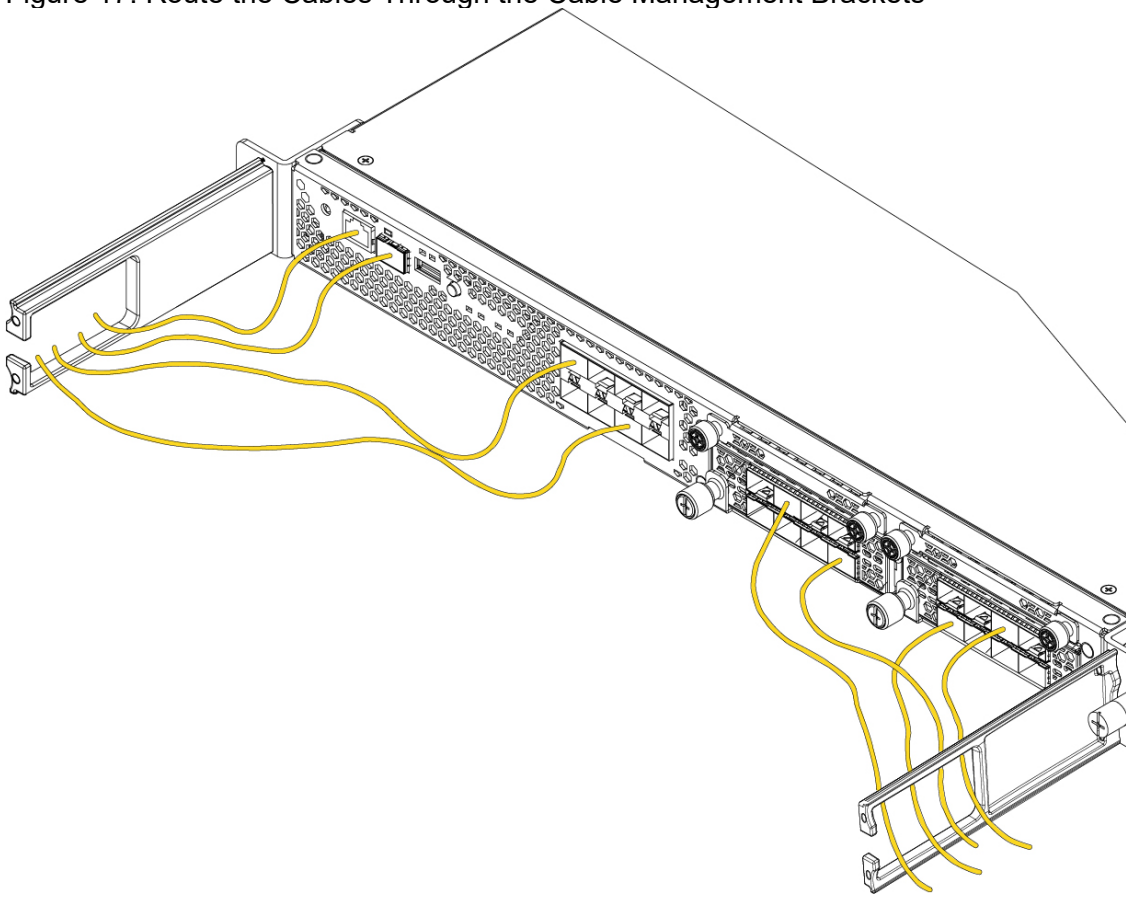
Step 5 Connect the cables to the ports. Install the cables according to your default software configuration as described in the Cisco Firepower 4100 Getting Started Guide. Make sure that the cables have enough slack to route them through the cable mounting brackets (as shown in Step 6 below).

Note: If you are installing the FIPS opacity shield after the initial product installation, the cables are connected. If the attached cables do not have enough slack to route them through the cable mounting brackets (as shown below), you will have to turn the power off on the appliance, remove the cables, route the cables through the cable mounting brackets, reattach the cables, and continue with Step 7 below.

Step 6 Route the cables through the openings in the cable management brackets.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

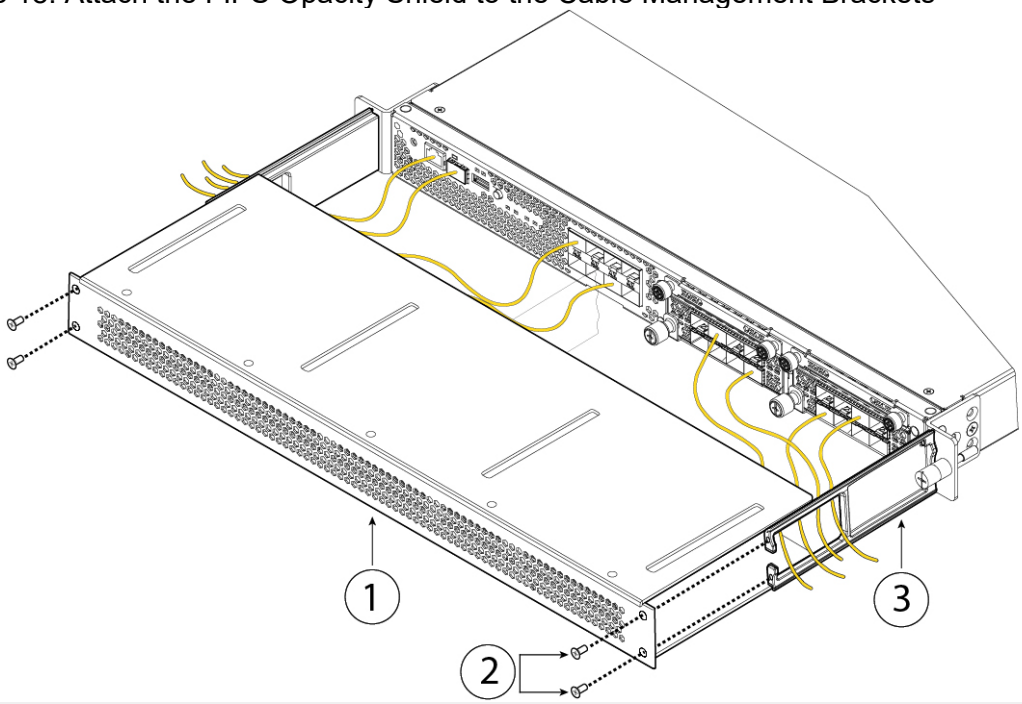
Figure 17. Route the Cables Through the Cable Management Brackets



Step 7 Attach the FIPS opacity shield to the cable management brackets using the four 8-32 x 0.375-inch Phillips screws provided in the FIPS kit.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 18. Attach the FIPS Opacity Shield to the Cable Management Brackets



1	FIPS opacity shield	**2**	8-32 x 0.375-inch Phillips screws (two per side)
3	Cable management bracket		

Step 8 Attach the TELs.

Step 9 Attach the power cable to the chassis and connect it to an electrical outlet.

Step 10 Press the power switch on the rear panel.

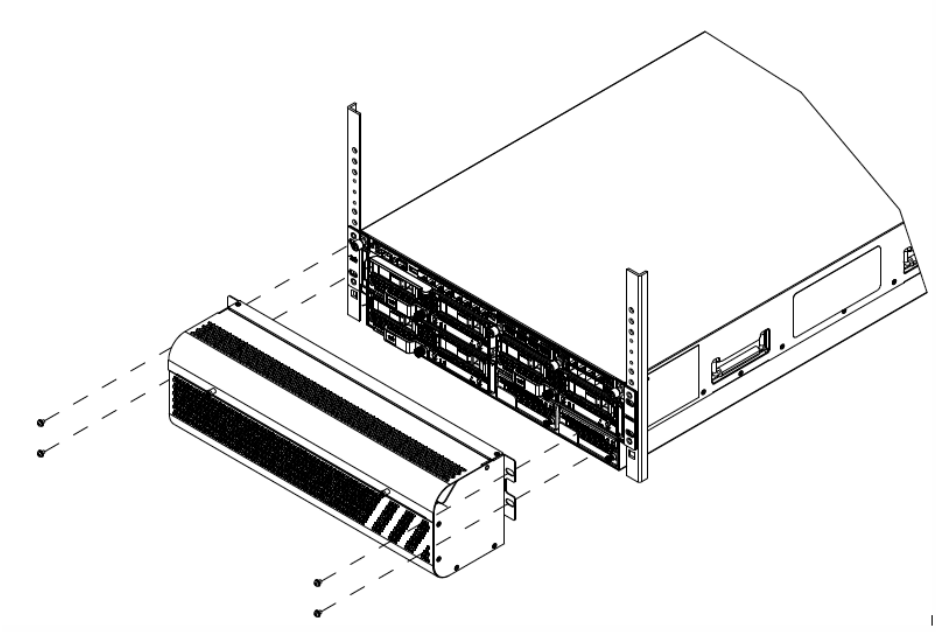
Step 11 Check the power LED on the front panel. See Front Panel LEDs for a description of the power LED. Solid green indicates that the chassis is powered on.

Note: When you toggle the power switch from ON to OFF, it takes several seconds for the system to power down. Do not remove the power cable until the power LED is off. After removing power from the chassis either by moving the power switch to OFF or unplugging the power cord, wait at least 10 seconds before turning power back ON.

FPR 9300 with SM-40, SM-48 or SM-56 Opacity Shield

FPR-C9300-FIPSKIT=

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.



8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile Memory	Dynamic
Flash	Non-Volatile Memory	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the Module's Boundary)	Module	Plaintext	Automated	Electronic	

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	Module	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via SSHv2 encrypted by AES-GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)
Password/Secret Input via TLSv1.2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)
Password/Secret Input via TLSv1.2 encrypted by AES-GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the DRAM or in the Flash of the module.	'erase configuration' command
Session Termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Zeroization Method	Description	Rationale	Operator Initiation
Reboot	Zeroization upon rebooting the module	Reboot to zeroize all temporary SSPs stored in volatile memory	Reboot

Table 19: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	384 bits - at least 256 bits	Entropy Input - CSP			DRBG Function
[ASA-CM] DRBG Entropy Input	Used to seed the ASA-CM DRBG	384 bits - at least 256 bits	Entropy Input - CSP			[ASA-CM] DRBG Function
DRBG Seed	Used in DRBG Generation	384 bits - 384 bits	DRBG Seed - CSP			DRBG Function
[ASA-CM] DRBG Seed	Used in ASA-CM DRBG Generation	384 bits - 384 bits	DRBG Seed - CSP			[ASA-CM] DRBG Function
DRBG Internal State V value	Used in DRBG Generation	128 bits - 128 bits	DRBG Internal State V value - CSP			DRBG Function
[ASA-CM] DRBG Internal State V value	Used in ASA-CM DRBG Generation	128 bits - 128 bits	DRBG Internal State V value - CSP			[ASA-CM] DRBG Function
DRBG Key	Used in DRBG Generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
[ASA-CM] DRBG Key	Used in ASA-CM DRBG Generation	256 bits - 256 bits	DRBG Key - CSP			[ASA-CM] DRBG Function
User Password	User authentication	8-30 Characters - 8-30 Characters	Password Hashes - CSP			
[ASA-CM] User Password	ASA-CM User authentication	8-30 Characters - 8-30 Characters	Password Hashes - CSP			
Crypto Officer Password	Crypto Officer authentication	8-30 Characters -	Password Hashes - CSP			

© 2021-2026 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		8-30 Characters				
[ASA-CM] Crypto Officer Password	ASA-CM Crypto Officer authentication	8-30 Characters - 8-30 Characters	Password Hashes - CSP			
Firmware Load Test Key	Used for Firmware Load Test	512 bits - 512 bits	HMAC Key - CSP			Firmware Load Test
[ASA-CM] Firmware Load Test Key	Used for ASA-CM Firmware Load Test	512 bits - 512 bits	HMAC Key - CSP			[ASA-CM] Firmware Load Test
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Private Key - CSP	KAS-FFC (SSHv2)		KAS-FFC (SSHv2)
[ASA-CM] SSH DH Private Key	Used to derive the ASA-CM SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Private Key - CSP	[ASA-CM] KAS-FFC (SSHv2)		[ASA-CM] KAS-FFC (SSHv2)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP		KAS-FFC (SSHv2)	

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
[ASA-CM] SSH DH Public Key	Used to derive ASA-CM SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP		[ASA-CM] KAS-FFC (SSHv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP			KAS-FFC (SSHv2)
[ASA-CM] SSH Peer DH Public Key	Used to derive ASA-CM SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP			[ASA-CM] KAS-FFC (SSHv2)
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	SSHv2 Keying Materials Development
[ASA-CM] SSH DH Shared Secret	Used to derive ASA-CM SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-3072, MODP-4096	Shared Secret - CSP		[ASA-CM] KAS-FFC (SSHv2)	[ASA-CM] SSHv2 Keying Materials Development

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		- 112 to 152 bits				
SSH ECDH Private Key	Used to derive the SSH ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (SSHv2)		KAS-ECC (SSHv2)
[ASA-CM] SSH ECDH Private Key	Used to derive the ASA-CM SSH ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] KAS-ECC (SSHv2)		[ASA-CM] KAS-ECC (SSHv2)
SSH ECDH Public Key	Used to derive SSH ECDHE Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (SSHv2)	
[ASA-CM] SSH ECDH Public Key	Used to derive ASA-CM SSH ECDHE Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] KAS-ECC (SSHv2)	
SSH Peer ECDH Public Key	Used to derive SSH DH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (SSHv2)
[ASA-CM] SSH Peer ECDH Public Key	Used to derive ASA-CM SSH DH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			[ASA-CM] KAS-ECC (SSHv2)
SSH ECDH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (SSHv2)	SSHv2 Keying Materials Development
[ASA-CM] SSH ECDH Shared Secret	Used to derive ASA-CM SSH Session Encryption Keys,	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		[ASA-CM] KAS-ECC (SSHv2)	[ASA-CM] SSHv2 Keying Materials Development

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	SSH Session Authentication Keys					
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
[ASA-CM] SSH RSA Private Key	Used for ASA-CM SSH session authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		[ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2)
SSH RSA Public Key	Used for SSH sessions aiuthentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
[ASA-CM] SSH RSA Public Key	Used for ASA-CM SSH sessions aiuthentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
SSH ECDSA Private Key	Used for SSH session authentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
[ASA-CM] SSH ECDSA Private Key	Used for ASA-CM SSH session authentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		[ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH ECDSA Public Key	Used for SSH sessions aiuthentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
[ASA-CM] SSH ECDSA Public Key	Used for ASA-CM SSH sessions aiuthentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
SSH Session Encryption Key	Used for SSH Session confidentiality protection	128, 256 bits - 128 or 256 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Encryption/Decryption (SSHv2)
[ASA-CM] SSH Session Encryption Key	Used for ASA-CM SSH Session confidentiality protection	128, 256 bits - 128 or 256 bits	Session Key - CSP		[ASA-CM] SSHv2 Keying Materials Development	[ASA-CM] Session Encryption/Decryption (SSHv2)
SSH Session Authentication Key	Used for SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Authentication (SSHv2)
[ASA-CM] SSH Session Authentication Key	Used for ASA-CM SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		[ASA-CM] SSHv2 Keying Materials Development	[ASA-CM] Session Authentication (SSHv2)
TLS DH Private Key	Used to Derive TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Private Key - CSP	KAS-FFC (TLSv1.2)		KAS-FFC (TLSv1.2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
[ASA-CM] TLS DH Private Key	Used to Derive ASA-CM TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Private Key - CSP	[ASA-CM] KAS-FFC (TLSv1.2)		[ASA-CM] KAS-FFC (TLSv1.2)
TLS DH Public Key	Used to Derive TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Public Key - PSP		KAS-FFC (TLSv1.2)	
[ASA-CM] TLS DH Public Key	Used to Derive ASA-CM TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Public Key - PSP		[ASA-CM] KAS-FFC (TLSv1.2)	
TLS Peer DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Public Key - PSP			KAS-FFC (TLSv1.2)
[ASA-CM] TLS Peer DH Public Key	Used to derive ASA-CM TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Public Key - PSP			[ASA-CM] KAS-FFC (TLSv1.2)
TLS DH Shared Secret	This CSP is also referred to TLS pre-master secret if Diffie-Hellman is used for TLS key agreement. This CSP is used for TLS master secret derivation	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Shared Secret - CSP		KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
[ASA-CM] TLS DH Shared Secret	This CSP is also referred to TLS pre-master secret if Diffie-Hellman is used for ASA-CM TLS key agreement. This CSP is used for ASA-CM TLS master secret derivation	ffdhe2048, ffdhe3072, ffdhe4096 - 112 to 152 bits	Shared Secret - CSP		[ASA-CM] KAS-FFC (TLSv1.2)	[ASA-CM] TLSv1.2 Keying Materials Development
TLS ECDH Private Key	Used to Derive TLS ECDH Shared Secret	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (TLSv1.2)		KAS-ECC (TLSv1.2)
[ASA-CM] TLS ECDH Private Key	Used to Derive ASA-CM TLS ECDH Shared Secret	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] KAS-ECC (TLSv1.2)		[ASA-CM] KAS-ECC (TLSv1.2)
TLS ECDH Public Key	Used to Derive TS ECDH Shared Secret	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (TLSv1.2)	
[ASA-CM] TLS ECDH Public Key	Used to Derive ASA-CM TLS ECDH Shared Secret	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] KAS-ECC (TLSv1.2)	
TLS Peer ECDH Public Key	Used to derive TLS ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
[ASA-CM] TLS Peer ECDH Public Key	Used to derive ASA-CM TLS ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			[ASA-CM] KAS-ECC (TLSv1.2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS ECDH Shared Secret	This CSP is also referred to TLS pre-master secret if EC Diffie-Hellman is used for TLS key agreement. This CSP is used for TLS master secret derivation	Curves p-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
[ASA-CM] TLS ECDH Shared Secret	This CSP is also referred to ASA-CM TLS pre-master secret if EC Diffie-Hellman is used for TLS key agreement. This CSP is used for ASA-CM TLS master secret derivation	Curves p-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		[ASA-CM] KAS-ECC (TLSv1.2)	[ASA-CM] TLSv1.2 Keying Materials Development
TLS ECDSA Private Key	Used to support CO and Admin HTTPS interfaces	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
[ASA-CM] TLS ECDSA Private Key	Used to support ASA-CM CO and Admin HTTPS interfaces	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		[ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
TLS ECDSA Public Key	Used to support CO and User HTTPS Interfaces	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
[ASA-CM] TLS ECDSA Public Key	Used to support ASA-CM CO and User HTTPS Interfaces	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
TLS RSA Private Key	Used to support CO and Admin HTTPS Interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
[ASA-CM] TLS RSA Private Key	Used to support ASA-CM CO and Admin HTTPS Interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		[ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2)
TLS RSA Public Key	Used to support CO and User HTTPS interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
[ASA-CM] TLS RSA Public Key	Used to support ASA-CM CO and User HTTPS interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
TLS Master Secret	Used to protect HTTPS Session. Pre-master secret	At least 112 bits - At least 112 bits	Master Secret - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Keying Materials Development
[ASA-CM] TLS Master Secret	Used to protect ASA-CM HTTPS Session. Pre-master secret	At least 112 bits - At	Master Secret - CSP		[ASA-CM] TLSv1.2 Keying	[ASA-CM] TLSv1.2 Keying Materials Development

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		least 112 bits			Materials Development	
TLS Session Encryption Key	Used to protect HTTPS Session. TLS Master secret	128, 256 bits - 128 or 256 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Encryption/Decryption (TLSv1.2)
[ASA-CM] TLS Session Encryption Key	Used to protect ASA-CM HTTPS Session. TLS Master secret	128, 256 bits - 128 or 256 bits	Session Key - CSP		[ASA-CM] TLSv1.2 Keying Materials Development	[ASA-CM] Session Encryption/Decryption (TLSv1.2)
TLS Session Authentication Key	Used to protect HTTPS Session. TLS master secret	at least 112 bits - at least 112 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Session Authentication (TLSv1.2)
[ASA-CM] TLS Session Authentication Key	Used to protect ASA-CM HTTPS Session. TLS master secret	at least 112 bits - at least 112 bits	Session Key - CSP		[ASA-CM] TLSv1.2 Keying Materials Development	[ASA-CM] Session Authentication (TLSv1.2)
IPSec/IKE DH Private Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Private Key - CSP	KAS-FFC (IKEv2)		KAS-FFC (IKEv2)
[ASA-CM] IPSec/IKE DH Private Key	Used to derive ASA-CM IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Private Key - CSP	[ASA-CM] KAS-FFC (IKEv2)		[ASA-CM] KAS-FFC (IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP		KAS-FFC (IKEv2)	
[ASA-CM] IPSec/IKE DH Public Key	Used to derive ASA-CM IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP		[ASA-CM] KAS-FFC (IKEv2)	
IPSec/IKE Peer DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP			KAS-FFC (IKEv2)
[ASA-CM] IPSec/IKE Peer DH Public Key	Used to derive ASA-CM IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP			[ASA-CM] KAS-FFC (IKEv2)
IPSec/IKE DH Shared Secret	Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys	MODP-2048, MODP-3072, MODP-4096	Shared Secret - CSP		KAS-FFC (IKEv2)	IPSec/IKEv2 Keying Materials Development

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		- 112 to 152 bits				
[ASA-CM] IPSec/IKE DH Shared Secret	Used to derive ASA-CM IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Shared Secret - CSP		[ASA-CM] KAS-FFC (IKEv2)	[ASA-CM] IPSec/IKEv2 Keying Materials Development
IPSec/IKE ECDH Private Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (IKEv2)		KAS-ECC (IKEv2)
[ASA-CM] IPSec/IKE ECDH Private Key	Used to derive ASA-CM IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] KAS-ECC (IKEv2)		[ASA-CM] KAS-ECC (IKEv2)
IPSec/IKE ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (IKEv2)	
[ASA-CM] IPSec/IKE ECDH Public Key	Used to derive ASA-CM IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] KAS-ECC (IKEv2)	
IPSec/IKE Peer ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (IKEv2)
[ASA-CM] IPSec/IKE Peer ECDH Public Key	Used to derive ASA-CM IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			[ASA-CM] KAS-ECC (IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE ECDH Shared Secret	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (IKEv2)	IPSec/IKEv2 Keying Materials Development
[ASA-CM] IPSec/IKE ECDH Shared Secret	Used to derive ASA-CM IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		[ASA-CM] KAS-ECC (IKEv2)	[ASA-CM] IPSec/IKEv2 Keying Materials Development
IPSec/IKE ECDSA Private Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
[ASA-CM] IPSec/IKE ECDSA Private Key	Used for ASA-CM IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		[ASA-CM] ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)
IPSec/IKE ECDSA Public Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
[ASA-CM] IPSec/IKE ECDSA Public Key	Used for ASA-CM IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		[ASA-CM] ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2,		RSA SigGen (SSHv2, TLSv1.2, IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				TLSv1.2, IKEv2)		
[ASA-CM] IPSec/IKE RSA Private Key	Used for ASA-CM IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Private Key - CSP	[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		[ASA-CM] RSA SigGen (SSHv2, TLSv1.2, IKEv2)
IPSec/IKE RSA Public Key	Used for IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
[ASA-CM] IPSec/IKE RSA Public Key	Used for ASA-CM IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Public Key - PSP		[ASA-CM] RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
IPSec/IKE Pre-shared Secret	Used for IPSec/IKE peer authentication	16-32 bytes characters - 16-32 bytes characters	shared secret - CSP			
[ASA-CM] IPSec/IKE Pre-shared Secret	Used for ASA-CM IPSec/IKE peer authentication	16-32 bytes characters - 16-32 bytes characters	shared secret - CSP			
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	160 bits - 160 bits	Keying Material - CSP		IPSec/IKEv2 Keying Materials Development	Session Authentication (IPSec/IKEv2) Session Encryption/Decryption (IPSec/IKE)
[ASA-CM] SKEYSEED	Keying material used to derive the ASA-CM IPSec/IKE	160 bits - 160 bits	Keying Material - CSP		[ASA-CM] IPSec/IKEv2 Keying	[ASA-CM] Session Authentication (IPSec/IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Session Encryption Key and IPSec/IKE Authentication Key				Materials Development	[ASA-CM] Session Encryption/Decryption (IPSec/IKE)
IPSec/IKE Session Encryption Key	Used to secure IPSec/IKEv2 session confidentiality	128, 256 bits - 128 or 256 bits	Session Key - CSP		IPSec/IKEv2 Keying Materials Development	Session Encryption/Decryption (IPSec/IKE)
[ASA-CM] IPSec/IKE Session Encryption Key	Used to secure ASA-CM IPSec/IKEv2 session confidentiality	128, 256 bits - 128 or 256 bits	Session Key - CSP		[ASA-CM] IPSec/IKEv2 Keying Materials Development	[ASA-CM] Session Encryption/Decryption (IPSec/IKE)
IPSec/IKE Authentication Key	Used to secure IPSec/IKEv2 session integrity	at least 160 bits - at least 160 bits	Session Key - CSP		IPSec/IKEv2 Keying Materials Development	Session Authentication (IPSec/IKEv2)
[ASA-CM] IPSec/IKE Authentication Key	Used to secure ASA-CM IPSec/IKEv2 session integrity	at least 160 bits - at least 160 bits	Session Key - CSP		[ASA-CM] IPSec/IKEv2 Keying Materials Development	[ASA-CM] Session Authentication (IPSec/IKEv2)
SNMPv3 Shared Secret	Used for SNMPv3 user authentication	8-32 characters - N/A	Authentication Secret - CSP			
[ASA-CM] SNMPv3 Shared Secret	Used for ASA-CM SNMPv3 user authentication	8-32 characters - N/A	Authentication Secret - CSP			
SNMPv3 Encryption Key	Used to protect SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		SNMPv3 Keying Materials Development	Session Encryption/Decryption (SNMPv3)
[ASA-CM] SNMPv3 Encryption Key	Used to protect ASA-CM SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		[ASA-CM] SNMPv3 Keying	[ASA-CM] Session Encryption/Decryption (SNMPv3)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					Materials Development	
SNMPv3 Authentication Key	Used to secure SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		SNMPv3 Keying Materials Development	Session Authentication (SNMPv3)
[ASA-CM] SNMPv3 Authentication Key	Used to secure ASA-CM SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		[ASA-CM] SNMPv3 Keying Materials Development	[ASA-CM] Session Authentication (SNMPv3)

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Seed:Used With DRBG Internal State V value:Used With DRBG Key:Used With
[ASA-CM] DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	[ASA-CM] DRBG Seed:Used With [ASA-CM] DRBG Internal State V value:Used With [ASA-CM] DRBG Key:Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Internal State V value:Used With DRBG Key:Used With
[ASA-CM] DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	[ASA-CM] DRBG Entropy Input:Used With [ASA-CM] DRBG Internal

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					State V value:Used With [ASA-CM] DRBG Key:Used With
DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With
[ASA-CM] DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	[ASA-CM] DRBG Entropy Input:Used With [ASA-CM] DRBG Seed:Used With [ASA-CM] DRBG Key:Used With
DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Internal State V value:Used With
[ASA-CM] DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	[ASA-CM] DRBG Entropy Input:Used With [ASA-CM] DRBG Seed:Used With [ASA-CM] DRBG Internal State V value:Used With
User Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input	Flash:Encrypted		Zeroization Command	

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via SSHv2 encrypted by AES and HMAC				
[ASA-CM] User Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
Crypto Officer Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
[ASA-CM] Crypto Officer Password	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by	Flash:Encrypted		Zeroization Command	

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC				
Firmware Load Test Key		Flash:Plaintext		N/A	
[ASA-CM] Firmware Load Test Key		Flash:Plaintext		N/A	
SSH DH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With
[ASA-CM] SSH DH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH DH Public Key:Paired With [ASA-CM] SSH Peer DH Public Key:Used With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH DH Private Key:Paired With
[ASA-CM] SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH DH Private Key:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
[ASA-CM] SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH DH Private Key:Used With
SSH DH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH DH Private Key:Derived From SSH DH Public Key:Derived From
[ASA-CM] SSH DH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH DH Private Key:Derived From [ASA-CM] SSH DH Public Key:Derived From
SSH ECDH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With
[ASA-CM] SSH ECDH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH ECDH Public Key:Paired With [ASA-CM] SSH Peer ECDH Public Key:Used With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH ECDH Private Key:Paired With
[ASA-CM] SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session	[ASA-CM] SSH ECDH Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination Reboot	
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH ECDH Private Key:Used With
[ASA-CM] SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH ECDH Private Key:Derived From SSH ECDH Public Key:Derived From
[ASA-CM] SSH ECDH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH ECDH Private Key:Derived From [ASA-CM] SSH ECDH Public Key:Derived From
SSH RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	SSH RSA Public Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
[ASA-CM] SSH RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] SSH RSA Public Key:Paired With
SSH RSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	SSH RSA Private Key:Paired With
[ASA-CM] SSH RSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] SSH RSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
SSH ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	SSH ECDSA Public Key:Paired With
[ASA-CM] SSH ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] SSH ECDSA Public Key:Paired With
SSH ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by	Flash:Plaintext		Zeroization Command	SSH ECDSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
[ASA-CM] SSH ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] SSH ECDSA Private Key:Paired With
SSH Session Encryption Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH Session Authentication Key:Used With
[ASA-CM] SSH Session Encryption Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH Session Authentication Key:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH Session Authentication Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	SSH Session Encryption Key:Used With
[ASA-CM] SSH Session Authentication Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SSH Session Encryption Key:Used With
TLS DH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS DH Public Key:Paired With TLS Peer DH Public Key:Used With
[ASA-CM] TLS DH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS DH Public Key:Paired With [ASA-CM] TLS Peer DH Public Key:Used With
TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS DH Private Key:Paired With
[ASA-CM] TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS DH Private Key:Paired With
TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session	TLS DH Private Key:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination Reboot	
[ASA-CM] TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS DH Private Key:Used With
TLS DH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
[ASA-CM] TLS DH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS ECDH Private Key:Derived From [ASA-CM] TLS Peer ECDH Public Key:Derived From
TLS ECDH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Public Key:Paired With TLS Peer ECDH Public Key:Used With
[ASA-CM] TLS ECDH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS ECDH Public Key:Paired With [ASA-CM] TLS Peer ECDH Public Key:Used With
TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Paired With
[ASA-CM] TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	[ASA-CM] ECDH Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination Reboot	
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Used With
[ASA-CM] TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
[ASA-CM] TLS ECDH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS ECDH Private Key:Derived From [ASA-CM] TLS Peer ECDH Public Key:Derived From
TLS ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input	Flash:Plaintext		Zeroization Command	TLS ECDSA Public Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via TLSv1.2 encrypted by AES-GCM				
[ASA-CM] TLS ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	TLS ECDSA Private Key:Paired With
[ASA-CM] TLS ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input	Flash:Plaintext		Zeroization Command	[ASA-CM] TLS ECDSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
TLS RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	TLS RSA Public Key:Paired With
[ASA-CM] TLS RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] TLS RSA Public Key:Paired With
TLS RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
[ASA-CM] TLS RSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With
TLS Master Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS ECDH Shared Secret:Derived From
[ASA-CM] TLS Master Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session	[ASA-CM] TLS ECDH Shared Secret:Derived From

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination Reboot	
TLS Session Encryption Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS Session Authentication Key:Used With
[ASA-CM] TLS Session Encryption Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS Session Authentication Key:Used With
TLS Session Authentication Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	TLS Session Encryption Key:Used With
[ASA-CM] TLS Session Authentication Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] TLS Session Encryption Key:Used With
IPSec/IKE DH Private Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE DH Public Key:Paired With IPSec/IKE Peer DH Public Key:Used With
[ASA-CM] IPSec/IKE DH Private Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE DH Public Key:Paired With [ASA-CM] IPSec/IKE Peer DH Public Key:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE DH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE DH Private Key:Paired With
[ASA-CM] IPSec/IKE DH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE DH Private Key:Paired With
IPSec/IKE Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization Command Session Termination Reboot	IPsec/IKE DH Private Key:Used With
[ASA-CM] IPSec/IKE Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPsec/IKE DH Private Key:Used With
IPSec/IKE DH Shared Secret		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	SKEYSEED:Used With
[ASA-CM] IPSec/IKE DH Shared Secret		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SKEYSEED:Used With
IPSec/IKE ECDH Private Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session	IPSec/IKE ECDH Public Key:Paired With IPSec/IKE Peer ECDH Public Key:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination Reboot	
[ASA-CM] IPSec/IKE ECDH Private Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE ECDH Public Key:Paired With [ASA-CM] IPSec/IKE Peer ECDH Public Key:Used With
IPSec/IKE ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE ECDH Private Key:Paired With
[ASA-CM] IPSec/IKE ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE ECDH Private Key:Paired With
IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE ECDH Private Key:Used With
[ASA-CM] IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE ECDH Private Key:Used With
IPSec/IKE ECDH Shared Secret		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	SKEYSEED:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
[ASA-CM] IPSec/IKE ECDH Shared Secret		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SKEYSEED:Used With
IPSec/IKE ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Public Key:Paired With
[ASA-CM] IPSec/IKE ECDSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] IPSec/IKE ECDSA Public Key:Paired With
IPSec/IKE ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
[ASA-CM] IPSec/IKE ECDSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] IPSec/IKE ECDSA Private Key:Paired With
IPSec/IKE RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input	Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Public Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via TLSv1.2 encrypted by AES-GCM				
[ASA-CM] IPSec/IKE RSA Private Key	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	[ASA-CM] IPSec/IKE RSA Public Key:Paired With
IPSec/IKE RSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Private Key:Paired With
[ASA-CM] IPSec/IKE RSA Public Key	Module Public Key Output Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input	Flash:Plaintext		Zeroization Command	[ASA-CM] IPSec/IKE RSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM				
IPSec/IKE Pre-shared Secret	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	SKEYSEED:Derived to
[ASA-CM] IPSec/IKE Pre-shared Secret	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM	DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SKEYSEED:Derived to

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SKEYSEED		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From IPSec/IKE Pre-shared Secret:Derived From
[ASA-CM] SKEYSEED		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE DH Shared Secret:Derived From [ASA-CM] IPSec/IKE ECDH Shared Secret:Derived From [ASA-CM] IPSec/IKE Pre-shared Secret:Derived From
IPSec/IKE Session Encryption Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
[ASA-CM] IPSec/IKE Session Encryption Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] IPSec/IKE DH Shared Secret:Derived From [ASA-CM] IPSec/IKE ECDH Shared Secret:Derived From
IPSec/IKE Authentication Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session Termination Reboot	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
[ASA-CM] IPSec/IKE Authentication Key		DRAM:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Session	[ASA-CM] IPSec/IKE DH Shared Secret:Derived From

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination Reboot	[ASA-CM] IPSec/IKE ECDH Shared Secret:Derived From
SNMPv3 Shared Secret	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Plaintext		Zeroization Command	SNMPv3 Encryption Key:Derive To SNMPv3 Authentication Key:Derive To
[ASA-CM] SNMPv3 Shared Secret	Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Plaintext		Zeroization Command	[ASA-CM] SNMPv3 Encryption Key:Derive To [ASA-CM] SNMPv3 Authentication Key:Derive To
SNMPv3 Encryption Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session Termination Reboot	SNMPv3 Shared Secret:Derived From

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
[ASA-CM] SNMPv3 Encryption Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SNMPv3 Shared Secret:Derived From
SNMPv3 Authentication Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session Termination Reboot	SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With
[ASA-CM] SNMPv3 Authentication Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Session Termination Reboot	[ASA-CM] SNMPv3 Shared Secret:Derived From [ASA-CM] SNMPv3 Encryption Key:Used With

Table 21: SSP Table 2

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

9.5 Transitions

- SHA-1: The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031

- FIPS 186-4/186-5: As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5. This means that no timeline exists in which any of the implemented algorithms will transition from approved to non-approved.

- 112-bit strength: The module includes an implementation of DH (MODP-2048 & ffdhe2048) for shared secret computation and RSA (2048-bit key) for key generation, digital signature generation and verification. This implementation will be non-Approved for all uses starting January 1, 2030.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A4446)	RSA SigVer 2048 bits with SHA2-512	RSA signature verification	SW/FW Integrity	Module is in normal state	RSA SigVer
[ASA-CM] RSA SigVer (FIPS186-4) (A4446)	RSA SigVer 2048 bits with SHA2-512	RSA signature verification	SW/FW Integrity	Module is in normal state	RSA SigVer [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]
Pre-Operational Bypass Test	N/A	N/A	Bypass	Module is in normal state	N/A
[ASA-CM] Pre-Operational Bypass Test	N/A	N/A	Bypass	Module is in normal state	Pre-Operational Bypass Test [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]

Table 22: Pre-Operational Self-Tests

© 2021-2026 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
[ASA-CM] AES-CBC Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Encrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] AES-CBC Encrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Encrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
AES-CBC Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
[ASA-CM] AES-CBC Decrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Decrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
[ASA-CM] AES-CBC Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Decrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
AES-GCM Authenticated Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
[ASA-CM] AES-GCM Authenticated Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] AES-GCM Authenticated Encrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Encrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
AES-GCM Authenticated Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
[ASA-CM] AES-GCM Authenticated Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] AES-GCM Authenticated Decrypt KAT (C1026)	128 bits	KAT	CAST	Module is in normal state	Decrypt [Cisco Adaptive Security Appliance	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					on 4K/9K Cryptographic Module]	
Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs	Power Up
[ASA-CM] Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
ECDSA SigGen (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT	Power Up
[ASA-CM] ECDSA SigGen (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
ECDSA SigVer (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT	Power Up
[ASA-CM] ECDSA SigVer (FIPS186-4) KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power up
[ASA-CM] Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change	Power up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					affecting the noise source	
[ASA-CM] Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Entropy data is generated from the Entropy Source - Continuous
[ASA-CM] Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to	Entropy data is generated from the Entropy Source - Continuous

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					become "stuck" on a single output value for a long period of time [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Entropy data is generated from the Entropy Source - Continuous
[ASA-CM] Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source [Cisco Adaptive Security Appliance on 4K/9K	Entropy data is generated from the Entropy Source - Continuous

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					Cryptographic Module]	
HMAC-SHA-1 KAT (A4446)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
[ASA-CM] HMAC-SHA-1 KAT (A4446)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] HMAC-SHA-1 KAT (C1026)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
HMAC-SHA2-256 KAT (A4446)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
[ASA-CM] HMAC-SHA2-256 KAT (A4446)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM]HMAC-SHA2-256 KAT (C1026)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 KAT (A4446)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
[ASA-CM] HMAC-SHA2-384 KAT (A4446)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] HMAC-SHA2-384 KAT (C1026)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
HMAC-SHA2-512 KAT (A4446)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
[ASA-CM] HMAC-SHA2-512 KAT (A4446)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
[ASA-CM] HMAC-SHA2-512 KAT (C1026)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512 [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	P-256 Curve	KAT	CAST	Module is in	Primitive Z KAT	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				normal state		
[ASA-CM] KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	P-256 Curve	KAT	CAST	Module is in normal state	Primitive Z KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
[ASA-CM] KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
KDF IKEv2 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
[ASA-CM] KDF IKEv2 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
KDF SNMP KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
[ASA-CM] KDF SNMP KAT (A4446)	N/A	KAT	CAST	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
KDF SSH KAT (A4446)	N/A	KAT	CAST	Module is in	N/A	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				normal state		
[ASA-CM] KDF SSH KAT (A4446)	N/A	KAT	CAST	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
RSA SigGen (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power Up
[ASA-CM] RSA SigGen (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
RSA SigVer (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power Up
[ASA-CM] RSA SigVer (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
SHA-1 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
[ASA-CM] SHA-1 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.2 KDF RFC7627 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
[ASA-CM] TLS v1.2 KDF RFC7627 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Power Up
ECDSA KeyGen (FIPS186-4) PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	ECDSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
[ASA-CM] ECDSA KeyGen (FIPS186-4) PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	ECDSA [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
RSA KeyGen (FIPS186-4) PCT (A4446)	2048 bit Modulus	PCT	PCT	Module is in normal state	RSA	Performs all required pair-wise consistency tests on the newly

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						generated key pairs before the first operational use.
[ASA-CM] RSA KeyGen (FIPS186-4) PCT (A4446)	2048 bit Modulus	PCT	PCT	Module is in normal state	RSA [Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
[ASA-CM] KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Performs all required pair-wise consistency tests on the newly generated key pairs before the first

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	MODP-2048	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
[ASA-CM] KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	MODP-2048	PCT	PCT	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
Firmware Load Test	HMAC-SHA2-512	KAT	SW/FW Load	Module is in normal state	N/A	When firmware has been uploaded to the module
[ASA-CM] Firmware Load Test	HMAC-SHA2-512	KAT	SW/FW Load	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	When firmware has been uploaded to the module
Conditional Bypass	N/A	N/A	Bypass	Module is in normal state	N/A	Performs conditional bypass test

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before first operational use of bypass service
[ASA-CM] Conditional Bypass	N/A	N/A	Bypass	Module is in normal state	[Cisco Adaptive Security Appliance on 4K/9K Cryptographic Module]	Performs conditional bypass test before first operational use of bypass service

Table 23: Conditional Self-Tests

The module performs on-demand self-tests initiated by the operator, by powering off and powering the module back on. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A4446)	RSA signature verification	SW/FW Integrity	Recommend every 60 days	Reboot
[ASA-CM] RSA SigVer (FIPS186-4) (A4446)	RSA signature verification	SW/FW Integrity	Recommend every 60 days	Reboot
Pre-Operational Bypass Test	N/A	Bypass	Recommend every 60 days	Reboot
[ASA-CM] Pre-Operational Bypass Test	N/A	Bypass	Recommend every 60 days	Reboot

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
[ASA-CM] AES-CBC Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-CBC Encrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
AES-CBC Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-CBC Decrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-CBC Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-GCM Authenticated Encrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-GCM Authenticated Encrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-GCM Authenticated Decrypt KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] AES-GCM Authenticated Decrypt KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] Counter DRBG Instantiate/Generate/Reseed KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] ECDSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
[ASA-CM] ECDSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
[ASA-CM] Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
[ASA-CM] Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
[ASA-CM] Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
[ASA-CM] Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
HMAC-SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA-1 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-256 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA2-256 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM]HMAC-SHA2-256 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-384 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
[ASA-CM] HMAC-SHA2-384 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA2-384 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
HMAC-SHA2-512 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA2-512 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] HMAC-SHA2-512 KAT (C1026)	KAT	CAST	Recommend every 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF IKEv2 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] KDF IKEv2 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF SNMP KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] KDF SNMP KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
KDF SSH KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] KDF SSH KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
RSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
[ASA-CM] RSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
RSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] RSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] SHA-1 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
TLS v1.2 KDF RFC7627 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
[ASA-CM] TLS v1.2 KDF RFC7627 KAT (A4446)	KAT	CAST	Recommend every 60 days	Reboot
ECDSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
[ASA-CM] ECDSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
RSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
[ASA-CM] RSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
[ASA-CM] KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
[ASA-CM] KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend every 60 days	Reboot
Firmware Load Test	KAT	SW/FW Load	N/A	N/A

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
[ASA-CM] Firmware Load Test	KAT	SW/FW Load	N/A	N/A
Conditional Bypass	N/A	Bypass	N/A	N/A
[ASA-CM] Conditional Bypass	N/A	Bypass	N/A	N/A

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If any self-test tests fail, the module is put into an error state	Self-test failure	Reboot the module	System Halt
[ASA-CM] Error State	If any self-test tests for the ASA-CM fail, the ASA-CM module is put into an error state	ASA-CM Self-test failure	Reboot the ASA-CM module	ASA-CM System Halt

Table 26: Error States

If any of the above-mentioned self-tests fail, the module reports the error and enters the Error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The validated module firmware was installed onto the respective test platforms listed in Table 2 above. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation. The Crypto Officer must configure and enforce the following initialization steps.

Secure Installation
The Crypto Officer must ensure that:

- The module is installed in a secure physical location.
- Physical access to the module is restricted to authorized personnel only.

Approved Mode of Operation:

Step 1: Install for Smart Licensing for AES licenses to require the security

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

appliances to use AES (for data traffic and SSH).

Step 2: Crypto officer shall perform zeroization operation if the module was previously used before the approved mode configuration.

Step 3: Enable “FIPS Mode” to allow the security appliances to internally enforce FIPS compliant behavior, such as run power-on self-tests, using the following commands:

security # enable fips-mode
security # enable cc-mode
security # commit-buffer
security # connect local-mgmt
security # reboot

Step 4: After step 4, please issue the following command to verify the FIPS mode:
security # show fips-mode
security # show cc-mode

Note: the output from ‘show fips-mode’ should be “FIPS Mode Admin State: Enabled”. The module cannot output “FIPS Mode Admin State: Enabled” if the module is not in the “Approved Mode.”

Step 5: SSH host key created during first-time setup of a device was hard coded to 1024 bits, you must destroy this old host key and generate a new one.
system/services # delete ssh-server host-key
system/services # commit-buffer
system/services # set ssh-server host-key rsa 2048
system/services # commit-buffer
system/services # create ssh-server host-key
system/services # commit-buffer
system/services # show ssh-server host-key

Step 6: Reboot the security appliances.

In addition, for the Secure Operations steps required for the embedded cryptographic module (ASA-CM), please refer to the Security Policy for more information. The ASA-CM module has been certified with FIPS 140-3 Cert. #5287.

Non-Approved Mode of Operation:
To change the mode of operation to the “Non-Approved” mode (**which is not recommended by Cisco**) the following commands must be used:

security # disable fips-mode
security # disable cc-mode
security # commit-buffer
security # connect local-mgmt
security # reboot

Note: This will remove the entire configuration and zeroize all SSPs.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Once the module is rebooted, use the following command to check module's non-approved mode status

security # show fips-mode
security # show cc-mode

Note: the output from 'show fips-mode' should be "FIPS Mode Admin State: Disabled"

11.2 Administrator Guidance

Further Administrator guidance can be found in the Cisco Firepower 4100/9300 FXOS Command Reference document: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/CLI_Reference_Guide/b_FXOS_CLI_reference/b_CLI_reference_chapter_0100.html

11.3 Non-Administrator Guidance

Further Non-Administrator guidance can be found in the Datasheets for Firepower series 4100 and 9300: https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html and https://www.cisco.com/c/en/us/products/collateral/security/firepower-9000-series/datasheet-c78-742471.html

12 Mitigation of Other Attacks

N/A for this module.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.