

# FIPS 140-2 Consolidated Validation Certificate



The National Institute of Standards and Technology of the United States of America



January 2022



The Canadian Centre for Cyber Security

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: \_\_\_\_\_

Dated: \_\_\_\_\_

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: \_\_\_\_\_

Dated: February 2 2022

Director, Risk Mitigation Programs  
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4119	01/03/2022	Juniper Networks ACX5448-M Router	Juniper Networks, Inc	Hardware Version: ACX5448-M-AC-AFI, ACX5448-M-AC-AFO , ACX5448-M-DC-AFI, ACX5448-M-DC-AFO; Firmware Version: JUNOS OS 20.3R1
4120	01/03/2022	Saviynt Cryptographic Module	Saviynt	Software Version: 1.0
4121	01/03/2022	DualAuth Cryptographic Module	DualAuth	Software Version: 2.2
4122	01/03/2022	FilingCloud Cryptographic Module	FilingCloud	Software Version: 2.2
4123	01/05/2022	FUJIFILM SONOSITE Cryptographic Module	FUJIFILM SONOSITE, Inc.	Software Version: 1.0
4124	01/10/2022	Hub Security Cryptographic Module	Hub Security LTD	Hardware Version: V.0002; Firmware Version: V2.0002.0050.0503.0725.080
4125	01/10/2022	Qualcomm(R) Inline Crypto Engine (SDCC)	Spectralink Corporation	Hardware Version: 3.0.0
4126	01/10/2022	Ubuntu 20.04 Azure Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 3.0
4127	01/10/2022	Ubuntu 20.04 GCP Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 3.0
4128	01/10/2022	OpenSSL_Neubus_FIPS	Neubus Inc	Software Version: 1.0
4129	01/10/2022	Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 and IW6300H-AC/DC/DCW Wireless LAN Access Points, Version IOS-XE 17.3	Cisco Systems, Inc.	Hardware Version: 1562e, 1562i, 1562d, 1562ps, 2802e, 2802i, 3802e, 3802i, 3802p, 4800, IW6300H-AC, IW6300H-DC and IW6300H-DCW with FIPS Kit: AIR-AP-FIPSKIT=; Firmware Version: IOS-XE 17.3
4130	01/11/2022	Juniper Networks EX4650, QFX5120 and QFX5210 Ethernet Switches	Juniper Networks, Inc	Hardware Version: EX4650-48Y-AFI, EX4650-48Y-AFO, EX4650-48Y-DC-AFI, EX4650-48Y-DC-AFO, QFX5120-32C-AFI , QFX5120-32C-AFO , QFX5120-32C-DC-AFI , QFX5120-32C-DC-AFO, QFX5120-48T-AFI, QFX5120-48T-AFO, QFX5120-48T-DC-AFI, QFX5120-48T-DC-AFO, QFX5120-48Y-AFI2, QFX5120-48Y-AFO2 , QFX5120-48Y-DC-AFI2, QFX5120-48Y-DC-AFO2, QFX5210- 64C-AFI , QFX5210- 64C-AFO, QFX5210-64C-DC-AFI, QFX5210-64C-DC-AFO; Firmware Version: JUNOS OS 20.2R1-S1
4131	01/13/2022	Juniper OpenSSL Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
4132	01/13/2022	Ubuntu 20.04 AWS Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 3.0
4133	01/13/2022	ECI TM200EN Encryption Module	ECI Telecom Ltd.	Hardware Version: TM100_2ENB, TM200ENB, TR10_12ENB; Firmware Version: R9.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4134	01/13/2022	Cisco 8800 Series Routers	Cisco Systems, Inc.	Hardware Version: [8808-SYS with components 8800-RP, 8800-LC-36FH, 8800-LC-48H, 8808-FC], [8812-SYS with components 8800-RP, 8800-LC-36FH, 8800-LC-48H, 8812-FC] and [8818-SYS with components 8800-RP, 8800-LC-36FH, 8800-LC-48H, 8812-FC]; Firmware Version: IOS-XR 7.0
4135	01/13/2022	CryptoComply for NSS	SafeLogic Inc.	Software Version: 5.0
4136	01/18/2022	CryptoComply for Libgcrypt	SafeLogic Inc.	Software Version: 5.0
4138	01/18/2022	NETSCOUT FIPS Object Module	NETSCOUT Systems, Inc.	Software Version: v1.0
4139	01/19/2022	Fortanix SDKMS Appliance	Fortanix, Inc.	Hardware Version: FX2200-II-T-F, FX2200-II-SX-F, FX2200-II-TN-F, FX2200-II-SXN-F; Firmware Version: 3.6.20
4140	01/24/2022	Harris AES Load Module	L3Harris Technologies, Inc.	Firmware Version: R04A01
4141	01/31/2022	Seagate® BarraCuda(TM) 515 SSD	Seagate Technology LLC	Hardware Version: ZP256MC30002, ZP512MC30002, ZP1024MC30002 and ZP2048MC30002; Firmware Version: ECPM13.0