

FIPS 140-2 Consolidated Validation Certificate



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



The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0012

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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: 1/12/2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: Jan 5, 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1644	12/06/2011	PCoIP Cryptographic Module for VMware View	VMware, Inc.	Software Version: 3.5.0
1645	12/15/2011	McAfee Web Gateway WG5000 and WG5500 Appliances	McAfee, Inc.	Hardware Versions: 5000 and 5500; Firmware Version: 7.1.0
1646	12/06/2011	Network Security Platform Sensor M-8000 P	McAfee, Inc.	Hardware Version: P/N M-8000 P, Version 1.40; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 6.1.15.35
1647	12/22/2011	Cisco Unified IP Phone 6901 and 6911	Cisco Systems, Inc.	Hardware Versions: 6901 and 6911: 1.0; Firmware Version: 9.2.1
1648	12/14/2011	Samsung Kernel Crypto API Cryptographic Module	Samsung Electronics Co., Ltd.	Software Versions: LK2.6.35.7_AGB_v1.2 and LK2.6.36.3_AHC_v1.2
1649	12/14/2011	SpectraGuard® Enterprise Server	AirTight Networks, Inc.	Firmware Version: 6.5.35
1650	12/14/2011	Cisco Unified IP Phone 6921, 6941, 6945 and 6961	Cisco Systems, Inc.	Hardware Versions: 6921: 5, 6941: 5, 6945: 4 and 6961: 4; Firmware Version: 9.2(1)SR1
1652	12/15/2011	SSG 5 and SSG 20	Juniper Networks, Inc.	Hardware Versions: (SSG-5-SB, SSG-5-SB-BT, SSG-5-SB-M, SSG-5-SH, SSG-5-SH-BT, SSG-5-SH-M, SSG-20-SB and SSG-20-SH) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6
1653	12/15/2011	Network Security Platform Sensor M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050 and M-6050	McAfee, Inc.	Hardware Versions: P/Ns M-1250 Version 1.10 [1], M-1450 Version 1.10 [1], M-2750 Version 1.50 [1], M-2850 Version 1.00 [1], M-2950 Version 1.00 [1], M-3050 Version 1.20 [1], M-4050 Version 1.20 [2] and M-6050 Version 1.40 [2]; FIPS Kit P/Ns IAC-FIPS-KT2 [1] and IAC-FIPS-KT7 [2]; Firmware Version: 6.1.15.35

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1654	12/15/2011	Brocade Mobility 7131N Dual-Radio 802.11n FIPS Access Point BR-AP7131N66040FGR and BR-AP7131N66040FWW	Brocade Communications Systems, Inc.	Hardware Versions: BR-AP7131N66040FGR and BR-AP7131N66040FWW; Firmware Version: AP7131N v4.0.1.0-003GRN
1655	12/15/2011	Concepteers Teleconsole TCS6U4W	Concepteers, LLC	Hardware Version: A2; Firmware Version: 2.0
1656	12/22/2011	Luna® PCI Cryptographic Module for Luna® IS and RSS	SafeNet, Inc.	Hardware Version: VBD-03-0100; Firmware Versions: 5.2.7 and 5.2.8
1657	12/22/2011	Cisco Catalyst 3560-X and 3750-X Switches	Cisco Systems, Inc.	Hardware Versions: (WS-C3560X-24P, WS-C3560X-24T, WS-C3560X-48P, WS-C3560X-48PF, WS-C3560X-48T, WS-C3750X-12S, WS-C3750X-24P, WS-C3750X-24S, WS-C3750X-24T, WS-C3750X-48P, WS-C3750X-48PF, WS-C3750X-48T, C3KX-NM-1G, C3KX-NM-10G, C3KX-NM-BLANK, C3KX-NM-10GT) with FIPS Kit (C3KX-FIPS-KIT); Firmware Version: 15.0(1)SE
1658	12/29/2011	SAMSUNG SSD PM810 SED FIPS 140 Module	Samsung Electronics	Hardware Versions: MZ5PA128HMCD-010D9 and MZ5PA256HMDR-010D9; Firmware Version: AXM96D1Q
1659	12/29/2011	AX Series Advanced Traffic Manager AX2500, AX2600-GCF, AX3000-GCF, AX5100 and AX5200	A10 Networks, Inc.	Hardware Versions: AX2500, AX2600-GCF, AX3000-GCF, AX5100 and AX5200; Firmware Version: 2.6.1-P2 build 28
1660	12/29/2011	McAfee Firewall Enterprise 1100F	McAfee, Inc.	Hardware Version: NSA-1100-FWEX-F and Seal Kit: SAC-1100F-FIPS-KT; Firmware Version: 7.0.1.01.E12
1661	12/29/2011	McAfee Firewall Enterprise 2150F	McAfee, Inc.	Hardware Version: NSA-2150-FWEX-F and Seal Kit: SAC-2150F-FIPS-KT; Firmware Version: 7.0.1.01.E12

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1662	12/29/2011	McAfee Firewall Enterprise 4150F	McAfee, Inc.	Hardware Version: NSA-4150-FWEX-FRR and Seal Kit: SAC-4150F-FIPS-KT; Firmware Version: 7.0.1.01.E12