Hewlett Packard Enterprise Development LP

HPE BladeSystem c-Class Virtual Connect Firmware

Firmware Version: 4.65

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.7

Prepared for:

Hewlett Packard Enterprise Development LP
11445 Compaq Center Dr. W.

Houston, TX 77070
United States of America

Phone: +1 (281) 370-0670
http://www.hpe.com

Prepared by:

Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HPE BladeSystem c-Class Virtual Connect Firmware (Firmware Version: 4.65) from Hewlett Packard Enterprise Development LP (HPE), hereafter referred to in this document as the VC Firmware or the module. This Security Policy describes how the VC Firmware meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level **1** FIPS 140-2 validation of the module.

1.2 References

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

- The HPE website (www.hpe.com) contains information on the full line of products from HPE.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals responsible for answering technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the module's capabilities and use of cryptography as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meet FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions, management methods, and applicable usage policies.

[1] U.S. – United States

2. VC Firmware

2.1 Overview

HPE's Virtual Connect is a server edge virtualization solution that provides connections over Ethernet, Fibre Channel, and iSCSI[2] between data and storage networks and a shared resource pool of HPE BladeSystem server blades. These connections are virtualized with a hardware abstraction layer so that server changes, like upgrades or replacements, are transparent to the external LAN[3] and SAN[4] environments. Virtual Connect provides four times the number of connections per physical network link by partitioning server Ethernet ports into smaller-bandwidth physical function NIC[5]s (called FlexNICs[6]).

The VC Firmware operates on three different HPE BladeSystem c-Class Virtual Connect hardware platforms (called interconnect modules) that plug directly into the rear bay of HPE BladeSystem c-Class enclosures. The platforms connect to server blades through the enclosure midplane. HPE BladeSystem is a rack-mount, enterprise-class computing infrastructure designed to maximize power while minimizing costs. A typical HPE BladeSystem environment may consist of an HPE BladeSystem c7000 enclosure, one or two HPE Onboard Administrator (OA) modules for enclosure management, one or more HPE BladeSystem c-Class Virtual Connect hardware platforms, and one or more of a range of server blades designed to provide flexible computation or storage services.

Virtual Connect provides the following advantages:

- Cleanly separates server enclosure administration from LAN and SAN administration
- Allows administrators to add, move, or replace servers without impacting production LAN and SAN availability
- Simplifies the setup and administration of server connections
- Enables HPE FlexFabric, which is a converged network solution capable of transmitting both Ethernet and storage traffic reliably in congested networks
- Supplies easy and efficient central management tools for one to hundreds of domains

Administrators use Virtual Connect management tools like Virtual Connect Enterprise Manager (VCEM) or Virtual Connect Manager (VCM) to create an I/O[7] connection profile for each server after physically making the LAN and SAN connections to the HPE BladeSystem c-Class Virtual Connect hardware platform. The I/O connection profile, or server profile, provides the linkage between the server and the connections defined in the Virtual Connect application. Server profiles contain information about server addresses, connections, and boot parameters.

VCM management capabilities are provided through firmware running on a processor on Ethernet-capable interconnect modules. Consequently, each HPE BladeSystem enclosure must have at least one HPE Virtual

[2] iSCSI – Internet Small Computer Systems Interface
[3] LAN – Local Area Network
[4] SAN – Storage Area Network
[5] NIC – Network Interface Controller
[6] A FlexNIC is a physical Peripheral Component Interconnect Express (PCIe) function that appears to the system read-only memory, operating system, and hypervisor as a discrete physical NIC with its own driver instance. It is not a virtual NIC contained in a software layer.
[7] I/O – Input/Output

Connect Ethernet-capable interconnect module. VCM provides a Web-based GUI[8] (the Web GUI) and a CLI[9] for managing a single Virtual Connect domain.

VCEM, a plug-in for HPE Systems Insight Manager (HPSIM), is an optional software application used to manage multiple Virtual Connect domains[10] (up to 1,000 BladeSystem enclosures). It provides automation and group-based management capabilities beyond what VCM offers. VCM communicates with VCEM over a SOAP[11] interface to forward server and network configuration data.

Additional information about the Virtual Connect infrastructure and technologies can be found in the technical white paper *Overview of HP Virtual Connect technologies*, available from the HPE website at http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA4-8174ENW&cc=us&lc=en.

The VC Firmware is validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A[12]
7	Cryptographic Key Management	1
8	EMI/EMC[13]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VC Firmware is a firmware module with a multi-chip embedded embodiment. The overall security level of the module is 1. The firmware image (vcfwall465.bin) runs on an HPE BladeSystem c-Class Virtual Connect hardware platform installed in an HPE BladeSystem c-Class enclosure.

The module implements the FIPS-Approved algorithms listed in Table 2.

[8] GUI – Graphical User Interface
[9] CLI – Command Line Interface
[10] Virtual Connect domain - A Virtual Connect domain consists of a BladeSystem enclosure and a set of associated modules and server blades that are managed together by a single instance of the VCM.
[11] SOAP – Simple Object Access Protocol
[12] N/A – Not Applicable
[13] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Table 2 – FIPS-Approved Cryptographic Algorithms

CAVP Cert	Algorithm	Standard	Mode / Method	Key Lengths, Curves, or Moduli	Use
4777	AES[14]	FIPS PUB 197, NIST SP[15] 800-38A	CBC[16]	128, 192, 256	Data Encryption/Decryption
			CFB[17]128	128	Data Encryption/Decryption
			CTR[18]	128, 192, 256	Data Encryption/Decryption
		FIPS PUB 197, NIST SP 800-38D	GCM[19]	128, 256	Data Encryption/Decryption and Authentication
		NIST SP 800-38F	KW[20]	128, 192, 256	Key Wrapping/Unwrapping
Vendor Affirmation	CKG[21]	NIST SP 800-133	-	-	Key Generation
1424	CVL[22]	NIST SP 800-135Rev1	TLS[23] 1.2	-	Key Derivation No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
1425	CVL[24]	NIST SP 800-135Rev1	SSH	-	Key Derivation No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
1426	CVL[25]	NIST SP 800-135Rev1	SNMP[26]v3	-	Key Derivation No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
1655	DRBG[27]	NIST SP 800-90A	CTR	-	Deterministic Random Bit Generation
3187	HMAC[28]	FIPS PUB 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication

[14] AES – Advance Encryption Standard
[15] SP – Special Publication
[16] CBC – Cipher Block Chaining
[17] CFB – Cipher Feedback
[18] CTR – Counter
[19] GCM – Galois Counter Mode
[20] KW – Key Wrap
[21] CKG – Cryptographic Key Generation
[22] CVL – Component Validation List
[23] TLS – Transport Layer Security
[24] CVL – Component Validation List
[25] CVL – Component Validation List
[26] SNMP – Simple Network Management Protocol
[27] DRBG – Deterministic Random Bit Generator
[28] HMAC – (Keyed-) Hash Message Authentication Code

CAVP Cert	Algorithm	Standard	Mode / Method	Key Lengths, Curves, or Moduli	Use
Vendor Affirmation	PBKDF[29]	NIST SP 800-132			Deriving Keys for Storage Applications
2618	RSA[30]	FIPS PUB 186-4	SHA-256, SHA-384, SHA-512	2048	Key Pair Generation
			SHA-224, SHA-256, SHA-384, SHA-512	2048	Signature Generation and Verification
3923	SHS[31]	FIPS PUB 180-4	SHA[32]-1, SHA-256, SHA-384, SHA-512	-	Message Digest
2539	Triple-DES[33]	NIST SP 800-67	TCBC[34]	-	Data Encryption/Decryption The TLS protocol governs the generation of Triple-DES keys. Refer to RFC 5246 for details relevant to the generation of the Triple-DES keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{32}.

The module implements the Allowed algorithms listed in Table 3 below.

Table 3 – Allowed Algorithms

Algorithm	Caveat	Use
FFC[35] DH[36]	Provides between 112 and 150 bits of encryption strength	Key agreement
RSA (key encapsulation)	Provides between 112 and 256 bits of encryption strength	Key establishment
NDRNG[37] (/dev/random)	N/A	Seeding for the DRBG

The module implements the Non-Approved algorithms listed in Table 4 below.

[29] PBKDF – Password-Based Key Derivation Function
[30] RSA – Rivest Shamir Adleman
[31] SHS – Secure Hash Standard
[32] SHA – Secure Hash Algorithm
[33] DES – Data Encryption Standard
[34] TCBC – Triple Data Encryption Algorithm Cipher Block Chaining
[35] FFC – Finite Field Cryptography
[36] DH – Diffie-Hellman
[37] NDRNG – Non-deterministic Random Number Generator

Table 4 – Non-Approved Algorithms

Algorithm	Use
OpenSSL *md_rand*	Provides Salt as input to the PBKDF2 function

Further, the vendor affirms compliance with the following security methods:

- NIST SP 800-132 (PBKDF2) – The module implements option 1(a) from section 5.4 of the Special Publication. Please refer to Section 3.2.3 for Crypto-Officer guidance specific to this function.
- NIST SP 800-133 (CKG) – When the module generates symmetric keys or seeds used for generating asymmetric keys, unmodified DRBG output is used as the symmetric key or as the seed for generating the asymmetric keys.

As a firmware module, the module has both a logical and physical cryptographic boundary. The logical and physical cryptographic boundaries are described in Sections 2.2.1 and 2.2.2, respectively.

2.2.1 Logical Cryptographic Boundary

The logical cryptographic boundary is drawn around the VC Firmware executing on the HPE BladeSystem c-Class Virtual Connect hardware platform.

Figure 1 shows the module's logical cryptographic boundary including the four main parts that comprise the VC Firmware.

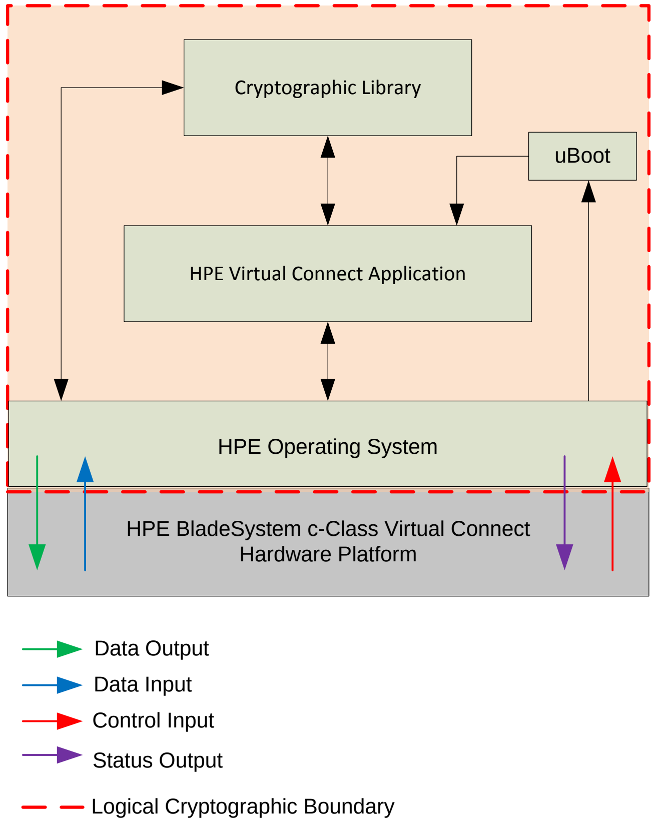

Figure 1 – VC Firmware Logical Cryptographic Boundary

2.2.2 Physical Cryptographic Boundary

As a firmware module, the cryptographic module has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the HPE BladeSystem c-Class Virtual Connect hardware platform on which it runs.

The module was tested and found compliant on the following HPE BladeSystem c-Class Virtual Connect hardware platforms:

- HPE Virtual Connect FlexFabric-20/40 F8 Module for c-Class BladeSystem with TAA[38]
- HPE Virtual Connect FlexFabric 10 Gb[39]/24-port Module for c-Class BladeSystem
- HPE Virtual Connect Flex-10/10D Module for c-Class BladeSystem

The module executes on the Freescale MPC8535 processor located on each of the HPE BladeSystem c-Class Virtual Connect hardware platforms. The module's physical cryptographic boundary is the physical perimeter of the HPE BladeSystem c-Class Virtual Connect hardware platform. This boundary fully encloses the processor and other hardware components that store and protect the VC Firmware.

[38] TAA – Trade Agreements Act. This extension on the model name signifies it is TAA-compliant, i.e., it was manufactured in a TAA designated country; otherwise, it is the same hardware and firmware as the HPE Virtual Connect FlexFabric 20/40 F8 Module for c-Class BladeSystem.
[39] Gb – Gigabit

Figure 2 presents a hardware block diagram for the HPE BladeSystem c-Class Virtual Connect hardware platforms. It illustrates the physical components and the ports and interfaces across the physical boundary.

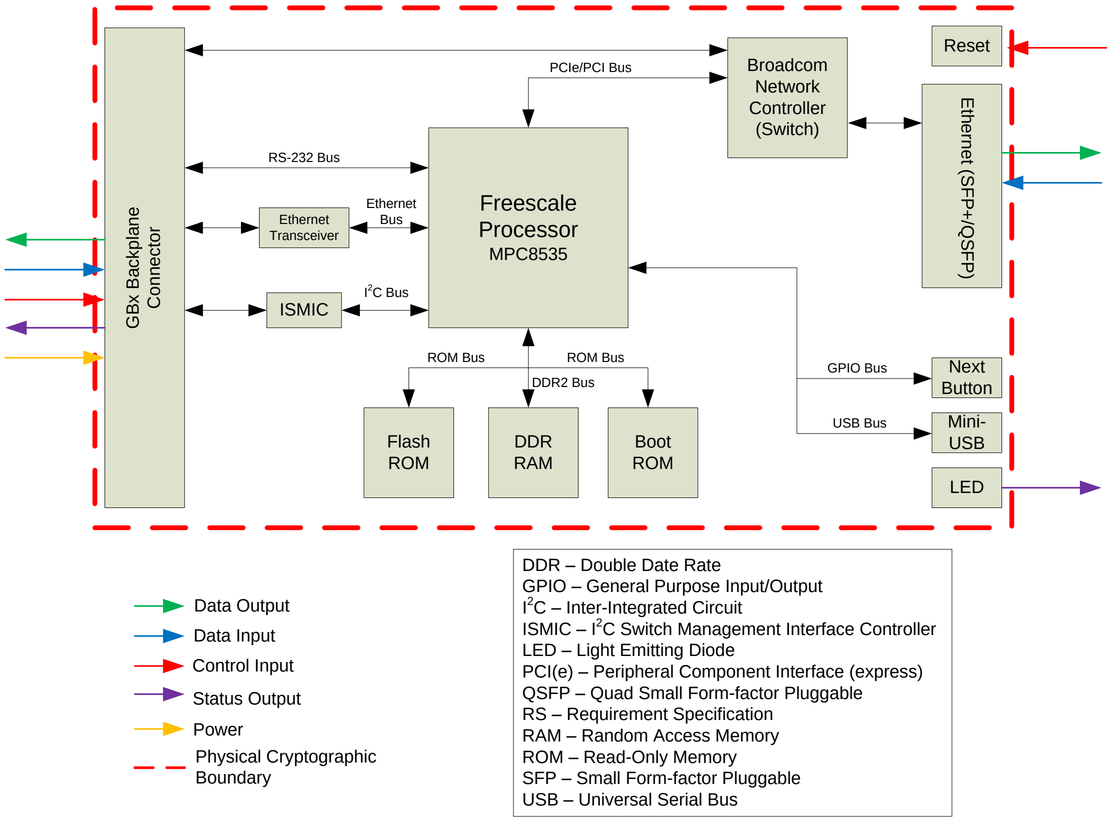

Figure 2 – HPE BladeSystem c-Class Virtual Connect Hardware Platform Block Diagram

2.3 Module Interfaces

As a firmware cryptographic module, the module's physical ports and interfaces are those of the HPE BladeSystem c-Class Virtual Connect hardware platform on which the VC Firmware runs.

The module's hardware platforms connect to the BladeSystem Enclosure through the backplane connector that plugs into the enclosure, providing connection pathways to all of the enclosure components and subsystems in order to provide administration. The backplane connector provides serial, Ethernet, and I²C connectivity. In addition, the backplane connector also provides Virtual Connect management via both the Web GUI and the CLI. Information flowing through the Ethernet interface is general, non-security relevant data.

The following is a list of physical interfaces implemented by these platforms:

- GBx backplane connector
- Ethernet SFP+ connector
- Ethernet QSFP connector

- Reset button
- LED indicators
- USB 2.0 (Mini) Type B connector (not used by the module)
- Next button (not used by the module)

The physical ports are separated into the logical interfaces defined by FIPS 140-2: data input, data output, control input, status output, and power. The module provides this same set of logical interfaces through its user interfaces (Web GUI and CLI), which allow it to receive and respond to calls for cryptographic and administrative services.

A mapping of the FIPS 140-2 logical interfaces to the module's physical and logical interfaces is shown in Table 5.

Table 5 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Module Physical Interface	Module Logical Interface
Data Input	• Ethernet Interfaces (SFP+, QSFP) • Backplane connector	Application inputs via user interfaces
Data Output	• Ethernet Interfaces (SFP+, QSFP) • Backplane connector	Application outputs via user interfaces
Control Input	• Backplane connector • Reset button	Application management commands and command parameters via user interfaces
Status Output	• Backplane connector • LED[40] indicators	Application command return statuses via user interfaces
Power Interface	Power interface	Not applicable

2.4 Roles, Services, and Authentication

The sections below describe the module's roles and services and define the authentication methods employed.

2.4.1 Authorized Roles

There are two authorized FIPS roles supported by the module: the Crypto-Officer (CO) role and the User role. The module is capable of supporting multiple CO and User secure sessions at a time. Operators of the module assume the role of CO or User through role-based authentication mechanisms implemented by the HPE Virtual Connect application. The module supports both local and remote authentication methods. An operator accesses the module by providing credentials that match those stored locally or on a remote LDAP server.

Operators of the module are assigned to an HPE-defined administrative role, each of which maps to one of the authorized FIPS roles. An operator's role is explicitly assumed based on their username or credentials stored on a CAC[41] card.

[40] LED – Light Emitting Diode
[41] CAC – Common Access Card

An operator assigned to the "Domain" HPE administrative role assumes the CO role. Table 6 maps all of the HPE administrative roles to their FIPS-defined role and provides a description of the services available to each role. Table 7 lists the Approved security services for both the CO and User roles. The CO has access to all the services of the User.

Table 6 – Mapping of HPE Administrative Roles to FIPS-Defined Roles

FIPS-Defined Role	HPE Administrative Role	Description
CO	Domain	Define local user accounts, set passwords, define roles; configure role-based user authentication; Import enclosures
User	Network	Configure network default settings; select the MAC[42] address range to be used by the Virtual Connect domain; create, delete, and edit networks
	Server	Create, delete, and edit server Virtual Connect profiles; assign and unassign profiles to device bays; select and use available networks
	Storage	Select the WWNs[43] to be used by the domain; set up the connections to the external FC[44] Fabrics; configure FC SNMP settings

2.4.2 Operator Services

Descriptions of the services available to an operator with the CO and User role are provided in Table 7. Please note that the keys and CSPs listed in Table 7 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 7 – Module Services by Role

Service	Role		Description	CSP and Type of Access
	CO	User		
Create/Modify Users	✓		Create, edit, and delete users; define user accounts and assign permissions	User password – W
Change CO Password	✓		Change the CO password	CO password – W
Change User Password	✓	✓	Change the User password	User password – W

[42] MAC – Media Access Control
[43] WWN – World Wide Name
[44] FC – Fibre Channel

Service	Role		Description	CSP and Type of Access
	CO	User		
Access the CLI	✓	✓	Manage the module using the CLI, accessed via SSH protocol over Ethernet or directly via serial console	Crypto Officer password – X User password – X SSH session key – W/X FFC DH public/private key components – W/X SSH integrity key – W/X SSH encryption key – W/X RSA SSH public/private keys – X
Access the Web GUI	✓	✓	Access the Web GUI via HTTPS connection through web browser	Crypto Officer password – X User password – X Crypto Officer LDAP password – X User LDAP password – X TLS session Key – W/X FFC DH public/private key components – W/X RSA TLS public/private keys – X TLS integrity key – W/X TLS encryption key – W/X AES GCM IV[45] – W/X
Access the Module using CAC cards	✓	✓	Log in to the module using CAC cards	TLS session Key – W/X FFC DH public/private key components – W/X RSA TLS public/private keys – X TLS integrity key – W/X TLS encryption key – W/X AES GCM IV – W/X Operator CAC credential – X
Zeroize Keys	✓		Zeroize all keys[46] and certificates; resets default CO password to factory settings	All keys – W
Show Status	✓	✓	Indicate whether the module is in FIPS mode	None
Initialize Module (Enter FIPS mode)	✓		Initialize the module in FIPS mode	Module key – W Module key password – W Utility key – W Utility key password – W RSA TLS private key – W RSA SSH private key – W
Backup Module	✓		Backup the domain configuration file to be loaded for future use	Backup encryption key password – W/X Backup encryption key – W/X
Restore Module	✓		Restore the module with an encrypted domain configuration file	Backup encryption key password – W/X Backup encryption key – W/X
Create Support Dump	✓		Generate a support log, which can be used for technical assistance	Support encryption key password – W/X Support encryption key – W/X
Connect to HPE OA	✓		Communicate with HPE OA to obtain status	TLS session key – W/X TLS integrity key – W/X TLS encryption key – W/X

[45] IV – Initialization Vector

[46] Please see Table 10 for the list of keys that can be zeroized using the "Zeroize Keys" service. More specifically, if a key listed in Table 10 has the text "Zeroized via Web GUI or CLI zeroization command" in the "Zeroization" column, then it can be zeroized with the "Zeroize Keys" service.

Service	Role		Description	CSP and Type of Access
	CO	User		
Configure SNMPv3 Settings	✓	✓	Enable and disable SNMPv3; configure SNMPv3 access types	SNMPv3 privacy key – W SNMPv3 authentication key – W
Connect via SNMPv3	✓	✓	Connect to the module via SNMPv3	SNMPv3 privacy key – RX SNMPv3 authentication key – RX
Generate TLS Certificate	✓		Generate a TLS certificate to be used for new TLS sessions	RSA TLS public/private keys – W
Import TLS Certificate	✓		Import a TLS certificate generated by a Certificate Authority	RSA TLS public key – W
Import Asymmetric Keys	✓	✓	Import a trusted key pair to be used for services such as SSH and SFTP[47]	RSA SSH public/private Keys – W
Update Firmware	✓		Update module firmware with newer version; verify module firmware with public key	Firmware Update Key – X
Perform Self-Tests	✓	✓	Initiate power-up self-tests on demand via reboot or power cycle	None
Configure CAC Authentication	✓		Enable, disable, and configure CAC authentication. Requires LDAP to be enabled and configured, including LDAP Service Account details.	None

2.4.3 General Operator Services

The module provides additional services for which an operator is not required to assume an authorized role.

Modules that are part of a single or multi-enclosure Virtual Connect domain may communicate to synchronize configuration data and exchange encrypted support files. This allows a module to be a back-up in case the primary module for the Virtual Connect domain becomes disabled. These services allow external Virtual Connect modules to access status information from the module. A request for a configuration data file does not require an operator to assume an authorized role as it does not require operator interaction.

The additional services are listed in Table 8. These services do not affect the overall security of the module, nor do they modify any private/secret keys or CSPs.

Table 8 – Services Not Requiring an Authorized Role

Service	Description	CSP and Type of Access
Synchronize with back-up module	Synchronize configuration data with the back-up module	Backup module password – X SSH encryption key – X SSH integrity key – X
Support file extraction	Extract encrypted support file with an external Virtual Connect appliance	Virtual Connect dump password – X SSH encryption key – X SSH integrity key – X

[47] SFTP – Secure File Transfer Protocol

Service	Description	CSP and Type of Access
Module management	Provide configuration data to HPE OA	Virtual Connect management password – X SSH encryption key – X SSH integrity key – X
Send/receive SOAP messages	Establish a connection with a server and communicate via SOAP	TLS encryption key – X TLS integrity key – X

2.4.4 Non-Security Relevant Services

The module offers additional services to all operators; these services are not relevant to the secure operation of the module. All services provided by the module are listed in the *HPE Virtual Connect for c-Class BladeSystem User Guide Version 4.65; Part Number: P01611-001, Dated: January 2018*, which is available from HPE customer support.

2.4.5 Authentication

The module supports role-based authentication. Roles are explicitly assumed based on the credential provided by the operator. The following authentication methods are supported:

- Local Authentication (Username/Password)

  Local authentication employs a locally-stored username/password combination that is unique to each supported role. To assume the CO role, operators must authenticate using the username and password associated with the “Domain” HPE administrative role. To assume the User role, operators must authenticate using the username and password associated with the “Network”, “Server”, or “Storage” HPE administrative role.

  CO and User passwords that are created by the CO or User must be at least 8 characters in length and can contain uppercase and lowercase letters [A-z, a-z]; numbers [0-9]; and special characters.

- Remote Authentication (LDAP Credential Certificate)

  Module operator accounts that are stored on a remote LDAP server are assigned to one or more groups. Each group is assigned an HPE administrative role. Thus, when logging via LDAP, the operator explicitly assumes the role designated by the LDAP group to which they are assigned. If they are assigned to multiple LDAP groups, the operator will assume multiple HPE administrative roles. To assume the CO role, operators must authenticate using the username and password associated with the “Domain” LDAP groups. To assume the User role, operators must authenticate using the username and password associated with the “Network”, “Server”, or “Storage” LDAP groups. If the user is assigned to a group that falls into both the CO and User roles, the user assumes the role with the highest privileges, the CO.

  CO and User passwords used for LDAP authentication follow the same complexity rules as those noted above for passwords used for local authentication.

In order to access the remote LDAP server, authentication is made to the server using the server's 2048-bit RSA public key located on the server's certificate. Once a connection to the LDAP server is established, authentication data is wrapped with the server's RSA public key.

- Remote Authentication (CAC Card Certificate)

  CAC authentication is based on the certificate presented by the operator via CAC card. The operator selects the appropriate certificate from those read by a web browser from the CAC card. The certificate is checked for its validity, chain of trust, and revocation status. If it is a valid certificate, LDAP service account details set in the module are used to log in to LDAP and authenticate the *subject* or *subjectAltName* data obtained from the certificate.

  The LDAP service account details are used to establish a session between the module and the LDAP server to validate the *subject* or *subjectAltName*. Therefore, LDAP authentication must be enabled and LDAP service account details must be properly configured. Based on the LDAP server response to the authentication request from the module, the operator will get appropriate access privilege as configured in the LDAP server for the corresponding *subject* or *subjectAltName*.

  In order to access the remote LDAP server, authentication is made to the server using the server's 2048-bit RSA public key located on the server's certificate. Once a connection to the LDAP server is established, authentication data is wrapped with the server's RSA public key.

Note that CAC user authentication is supported only on the Web GUI. When CAC is enabled, the following will be disabled:

- CLI access
- Web GUI login with username and password
- Local user accounts

For all supported authentication methods, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1:100,000 as required by FIPS 140-2. Table 9 provides the strength of the authentication mechanisms used by the module.

Table 9 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Username/Password (local)	Once properly configured, the minimum length of the password is 8 characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. Assuming a minimum password length of 8 characters, the chance of a random attempt falsely succeeding is: 1: (94^8), or 1: 6,095,689,385,410,816 Which is less than 1:1,000,000 as required by FIPS 140-2. The fastest network connection supported by the module (for management) is 100 Mbps. Hence at most (100×1024^2 bits × 60 seconds=) 6.29×10^9 bits of data can be transmitted to the module in one minute (assuming no overhead). Each password attempt is (8 bits x 8 characters =) 64 bits in length, meaning ($6.29 \times 10^9/64$=) 9.83×10^7 password attempts can be made in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1: (94^8 possible passwords / 9.83×10^7 passwords per minute) 1: 62,011,082 Which is less than 1:100,000 within one minute as required by FIPS 140-2.
RSA Public Key (LDAP authentication of username and password)	The RSA public key used for LDAP authentication of username and password is 2048 bits, yielding an equivalent 112 bits of strength. The chance of a random authentication attempt falsely succeeding is: 1: (2^{112}), or 1: 5.1922968585348276285304963292201e+33 Which is less than 1:1,000,000 as required by FIPS 140-2. The fastest network connection supported by the module (for management) is 100 Mbps. Hence at most (100×1024^2 bits × 60 seconds=) 6.29×10^9 bits of data can be transmitted to the module in one minute (assuming no overhead). Each attempt is 112 bits in length, meaning ($6.29 \times 10^9/112$=) 5.62×10^7 attempts can be made in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1: (2^{112} possible keys / 5.62×10^7 keys per minute) 1: 9.24×10^{25} Which is less than 1:100,000 within one minute as required by FIPS 140-2.

Authentication Type	Strength
RSA Public Key (LDAP authentication of *subject* or *subjectAltName* from CAC certificate)	The RSA public key used for LDAP authentication of *subject* or *subjectAltName* is 2048 bits, yielding an equivalent 112 bits of strength. The chance of a random authentication attempt falsely succeeding is: 1: (2^{112}), or 1: 5.1922968585348276285304963292201e+33 Which is less than 1:1,000,000 as required by FIPS 140-2. The fastest network connection supported by the module (for management) is 100 Mbps. Hence at most (100×1024^2 bits × 60 seconds=) 6.29×10^9 bits of data can be transmitted to the module in one minute (assuming no overhead). Each attempt is 112 bits in length, meaning ($6.29 \times 10^9/112$=) 5.62×10^7 attempts can be made in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1: (2^{112} possible keys / 5.62×10^7 keys per minute) 1: 9.24×10^{25} Which is less than 1:100,000 within one minute as required by FIPS 140-2.

Upon successful login to the CLI, the operator is presented with a banner displaying the Virtual Connect version, the copyright notice, and a “Getting Started” message followed by the CLI command prompt, “FIPS->”. Upon successful login to the Web GUI, the operator is presented with the Virtual Connect Manager home page.

2.5 Physical Security

As a multi-chip embedded firmware module, the module relies on the HPE BladeSystem c-Class Virtual Connect hardware platform to provide the mechanisms necessary to meet FIPS 140-2 level 1 physical security requirements. All components of the hardware are made of production-grade materials, and all integrated circuits are coated with commercial standard passivation.

Additionally, the hardware has been tested for and meets applicable Federal Communications Commission (FCC) Electromagnetic Interference and Electromagnetic Compatibility requirements for business use as defined in Subpart B of FCC Part 15.

2.6 Operational Environment

The module does not provide a general-purpose OS to the user. The module runs a proprietary OS (HPE OS 2.6.32.60), which provides a limited operational environment, and only the module’s custom-written image can be run on the system. Access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the firmware module is executing/operational is prohibited. Processes that are spawned by the firmware module are owned by the module and are not owned by external processes. The module provides a method to update its firmware to a newer version. This method involves downloading a digitally-signed firmware update to the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 10.

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Module Key Password	Random data (32 Bytes)	Internally generated via Approved DRBG	Not output from the module	Stored in plaintext in NOR[48] flash memory	Zeroized via Web GUI or CLI zeroization command	Used as PBKDF2 input to generate Module Key
Module Key	32-byte Data Protection Key (AES 256-bit key)	Internally generated via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Key used to encrypt all CSPs stored in NAND[49] flash memory
Utility Key Password	Random data (20 Bytes)	Internally generated via Approved DRBG	Output encrypted via SSH to the backup module	Stored in plaintext in NOR Flash memory; stored encrypted via Module Key in NAND flash memory	Zeroized via Web GUI or CLI zeroization command	Used as PBKDF2 input to generate Utility Key
Utility Key	32-byte Data Protection Key (AES 256-bit key)	Internally generated via PBKDF2	Output encrypted via SSH protocol	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Key used to obfuscate Backup Module Password
Backup Encryption Key Password	8-byte Password	Externally generated; input electronically via TLS or SSH	Not output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Password input to PBKDF2 function to derive Backup Encryption Key
Backup Encryption Key	32-byte Data Protection Key (AES 256-bit key)	Internally generated via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Key used to encrypt Virtual Connect configuration file

[48] NOR – Not OR
[49] NAND – Not AND

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Support Encryption Key Password	8-byte Password	Externally generated; input electronically via TLS or SSH	Not output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Password input to PBKDF2 function to derive Support Encryption Key
Support Encryption Key	32-byte Data Protection Key (AES 256-bit key)	Internally generated via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Key used to encrypt Virtual Connect support file
RSA SSH Public Key	RSA 2048-bit public key	Internally generated via Approved RSA Key Generation method; input via configuration file restore	Output in plaintext; output encrypted by Backup Encryption Key	Stored encrypted via Module Key in NAND flash memory	N/A	SSH Protocol; SFTP; Signature verification; Key unwrapping
RSA SSH Private Key	RSA 2048-bit private key	Internally generated via Approved RSA Key Generation method; input via configuration file restore	Output encrypted by Backup Encryption Key	Stored encrypted via Module Key in NAND Flash memory	N/A	SSH Protocol; SFTP; Signature generation; Key wrapping
RSA TLS Public Key	RSA 2048-bit public key	Internally generated via Approved RSA Key Generation method; input via configuration file restore	Output in plaintext; output encrypted by Backup Encryption Key	Stored encrypted via Module Key in NAND flash memory	N/A	TLS protocol; Signature verification; Key unwrapping
RSA TLS Private Key	RSA 2048-bit private key	Internally generated via Approved RSA Key Generation method; input via configuration file restore	Output encrypted by Backup Encryption Key	Stored encrypted via Module Key in NAND Flash memory	N/A	TLS protocol; Signature generation; Key wrapping
SSH Session Key	SSH shared secret	Agreed using Diffie-Hellman	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Shared session key used to derive SSH Integrity Key and SSH Encryption Key
SSH Integrity Key	HMAC SHA-256 HMAC SHA-512	Internally generated via SP800-135rev1 SSH KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used to generate SSH payload integrity message; used to verify integrity of SSH payload

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Encryption Key	AES 128, 192, 256 (CBC, CTR)	Internally generated via SP800-135rev1 SSH KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used to encrypt and decrypt SSH payload
TLS Pre-Master Secret	Pre-master secret for TLS	Established using RSA transport	Never output from module	Plaintext in volatile RAM	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Derivation of TLS Master Secret
TLS Master Secret	TLS master secret AES 128, 256 (CBC, GCM) Triple-DES 168-bit	Internally generated via SP800-135rev1 TLS KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Shared master secret used to derive TLS Integrity Key and TLS Session Encryption Key
TLS Integrity Key	HMAC SHA-256 HMAC SHA-512	Internally generated via SP800-135rev1 TLS KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used to generate TLS payload integrity message; used to verify integrity of TLS payload
TLS Session Encryption Key	AES 128, 256 (CBC, GCM) Triple-DES 168-bit	Internally generated via SP800-135rev1 TLS KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used to encrypt and decrypt TLS payload
AES GCM IV	96 bit IV length	Internally Generated deterministically in compliance with TLS 1.2 GCM Cipher Suites for TLS and Section 8.2.1 of NIST SP 800-38D	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	IV input to AES GCM function
FFC DH Public Key Component	Public components of FFC DH protocol 2048-bit	Internally generated via Approved DRBG	Output in plaintext	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used for SSH session establishment and initial key exchange

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
FFC DH Private Key Component	Private exponent of FFC DH protocol 2048-bit	Internally generated via Approved DRBG	Never output from module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Used for SSH session establishment and initial key exchange
Crypto Officer Password	ASCII string (minimum 8 characters)	Externally generated; input electronically via TLS or SSH; input via configuration file restore	Output encrypted by Backup Encryption Key	Stored obfuscated via SHA-512 hash in NAND Flash memory and encrypted via Module Key	Zeroized via Web GUI or CLI zeroization command	Used for CO authentication to the module
User Password	ASCII string (minimum 8 characters)	Externally generated; input electronically via TLS or SSH; input via configuration file restore	Output encrypted by Backup Encryption Key	Stored obfuscated via SHA-512 hash in NAND Flash memory and encrypted via Module Key	Zeroized via Web GUI or CLI zeroization command	Used for User authentication to the module
Operator CAC Credential	Public key associated with module operator’s certificate	Input by CO via TLS	Never output from the module	Stored in Flash memory and in RAM in plaintext	Zeroized when the certificate validation and user authentication is complete	Authenticating the Operator
Crypto Officer LDAP Password	ASCII string (minimum 8 characters)	Externally generated; input electronically via TLS	Never output from module	Not stored on the module	N/A	Used for CO authentication to the module via LDAP
User LDAP Password	ASCII string (minimum 8 characters)	Externally generated; input electronically via TLS	Never output from module	Not stored on the module	N/A	Used for User authentication to the module via LDAP
Backup Module Password	ASCII string (16 characters, excludes special characters)	Internally generated via Approved DRBG	Output encrypted via the Utility Key	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command	Used by the backup Virtual Connect unit in order to synchronize configuration data
Virtual Connect Dump Password	ASCII string (12 characters, excludes special characters)	Internally generated via Approved DRBG	Output encrypted over SSH session	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command	Password used by external Virtual Connect units to authenticate SSH session in order to extract a support file

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Privacy Key	AES 128-bit key	Internally generated via SNMP KDF	Output encrypted by Backup Encryption Key	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command	Encrypt packets being transferred via SNMP
SNMPv3 Authentication Key	HMAC SHA-1 Key	Internally generated via SNMP KDF	Output encrypted by Backup Encryption Key	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command	Authenticate packets being transferred via SNMP
Firmware Update Key	RSA 2048-bit Public Key	Externally generated; hardcoded	Never output from module	Stored unencrypted in NAND Flash memory	N/A	Verify the RSA signature of new firmware prior to installation
DRBG Seed	Random data – (384 bits)	Internally generated using nonce along with DRBG entropy input	Never output from module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Seeding material for SP 800-90A DRBG
DRBG Entropy	256-bit value	Internally generated	Never output from module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Entropy material for SP 800-90A DRBG
DRBG ‘V’ Value	Internal state value	Internally generated	Never output from module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Internal state value for SP 800-90A DRBG
DRBG ‘Key’ Value	Internal state value	Internally generated	Never output from module	Stored in plaintext in volatile memory	Zeroized via Web GUI or CLI zeroization command or by module shutdown or reboot	Internal value for SP 800-90A DRBG

2.8 Self-Tests

Cryptographic self-tests are performed by the module when the module begins operation in the FIPS mode and when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, expected error status, and error resolution.

2.8.1 Power-Up Self-Tests

Power-up self-tests are automatically performed by the module when power is supplied to the HPE BladeSystem c-Class Virtual Connect hardware platform and the module is loaded into memory. The power-up self-tests in the list that follows may also be run on-demand when the CO or User reboots the HPE BladeSystem c-Class Virtual Connect hardware platform. The module will perform the listed power-up self-tests to successful completion. During the execution of self-tests, data output from the module is inhibited.

If the module fails a power-up self-test, the module's self-test error counter will increment and the module will reboot in order to recover from the failure. After rebooting, the module will attempt to perform the power-up self-tests again. After 10 failed self-test attempts throughout the lifetime of the module (including conditional self-tests), the module will enter a critical error state and no longer function, requiring the HPE BladeSystem c-Class Virtual Connect hardware platform to be returned to HPE. The module indicates the critical error to the operator through the Web GUI and via LEDs. Error messages for a KAT failure will indicate the algorithm that failed along with the text "selftest failed".

The module performs the following self-tests at power-up:

- Firmware integrity check (HMAC SHA-256)
- Known Answer Tests (KATs)
  - AES Encrypt KAT (CBC mode)
  - AES Decrypt KAT (CBC mode)
  - AES Encrypt KAT (GCM mode)
  - AES Decrypt KAT (GCM mode)
  - Triple-DES Encrypt KAT (CBC mode)
  - Triple-DES Decrypt KAT (CBC mode)
  - RSA 186-4 Signature Generation KAT
  - RSA 186-4 Signature Verification KAT
  - RSA Encrypt KAT
  - RSA Decrypt KAT
  - SHA-1 KAT
  - HMAC SHA-256 KAT
  - HMAC SHA-384 KAT
  - HMAC SHA-512 KAT
  - CTR_DRBG KAT

2.8.2 Conditional Self-Tests

Conditional self-tests are performed by the module whenever a new random number is generated or when a new RSA key pair is generated. If the module fails a conditional self-test, the module's self-test error counter will increment and the module will reboot in order to recover from the failure. After 10 failed self-test attempts throughout the lifetime of the module (including power-up self-tests), the module enters into a critical error state and will no longer function, requiring the HPE BladeSystem c-Class Virtual Connect hardware platform to be returned to HPE. The module indicates the critical error to the operator through the Web GUI and via LEDs. Error messages for a conditional test failure will indicate the algorithm that failed along with the reason, which may be one of the following: “selftest failed”, “internal error”, “drgb not initialized”, or “pairwise test failed”.

The module performs the following conditional self-tests:

- CTR_DRBG Continuous Random Number Generator Test (CRNGT)
- NDRNG CRNGT
- RSA Pairwise Consistency Test for sign/verify
- Firmware Load Test

For the Firmware Load Test, the module verifies that the image is properly signed using a 2048-bit RSA public key (Firmware Update Key in Table 10) with SHA-256 digest.

2.8.3 Critical Functions Self-Tests

The module performs four critical function tests for each of the four SP 800-90A DRBGs: DRBG Instantiate, DRBG Reseed, DRBG Generate, and DRBG Uninstantiate. The purpose of the DRBG Instantiation Test is to prepare each SP 800-90A DRBG with initial state values and a reseed counter value. The purpose of the DRBG Reseeding Test in each of the SP 800-90A DRBGs is to ensure that the DRBG does not repeat a previously generated random number. The purpose of the DRBG Generate Test is to verify that both the instantiation and reseed algorithms are tested during power-up. The purpose of the DRBG Uninstantiate test is to verify that the DRBG uninstantiates properly and no secret values created by the DRBG are accessible.

Critical functions tests are performed during power-up and conditionally. If the module fails a critical functions test, the module will cease operation and enter a critical error state. In the critical error state, the module will indicate the error to the operator through the Web GUI and automatically reboot. After 10 failed self-test attempts throughout the lifetime of the module, the module will no longer function, requiring the HPE BladeSystem c-Class Virtual Connect hardware platform to be returned to HPE.

The module performs the following critical functions tests:

- SP 800-90A DRBG Instantiate Test
- SP 800-90A DRBG Generate Test
- SP 800-90A DRBG Reseed Test
- SP 800-90A DRBG Uninstantiate Test

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any other attacks.

3. Secure Operation

The module meets Level 1 for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved mode of operation.

HPE recommends that module operators read the specific *HPE Virtual Connect for c-Class BladeSystem User Guide* for enclosure-specific information before proceeding with the VC Firmware setup. The User Guide provides information on the initial setup and operation of the VC Firmware.

3.1 Initial Setup

Prior to operating the module for the first time, the CO must configure a 4-pin DIP[50] switch located on the motherboard of the HPE BladeSystem c-Class Virtual Connect hardware platform. The switch is located at the front of the platform, on the opposite end of the backplane connector. In order to place the module in the FIPS mode, the pins of the switch shall be placed in the following positions (from switch 1 to switch 4) : OFF, OFF, ON, OFF. The CO must remove the cover of the platform in order to access the DIP switch.

After configuring the DIP switch, the CO shall replace the cover on the platform, reinsert the platform into the BladeSystem enclosure, and power-up the module for the first time. The CO can confirm that the module is operating in the FIPS mode via the Web GUI or the CLI. Additional information on confirming the FIPS mode of operation is provided in Section 3.2.2.

3.2 Crypto Officer Guidance

The Crypto Officer is responsible for ensuring that the module has been properly configured as described in Section 3.1 and is therefore operating in its FIPS-Approved mode of operation. When configured according to the Crypto Officer guidance in this Security Policy, the module only runs in its FIPS-Approved mode of operation.

3.2.1 Secure Management

The module can be managed remotely via a Web GUI or CLI. Through these management interfaces, a CO can view the status of the FIPS mode of operation, manage the module's operations, and back-up and restore module configuration files. Access to the module is controlled by role-based authentication, described in Section 2.4. Access to the module via the Web GUI is provided by HPE VCM. Access to the module via the CLI is provided by an SSH client running on a networked machine.

While the module is operating in the FIPS-Approved mode, additional modules not configured to operate in an Approved mode cannot communicate with the module. In order for additional modules to communicate with one another, they too must be operating in the FIPS-Approved mode. When initialized and configured per the CO guidance in this Security Policy, the module does not support a non-Approved mode of operation.

[50] DIP – Dual In-line Package

3.2.2 Verifying the Approved Mode

The CO shall be responsible for regularly monitoring the modules' status for FIPS-Approved mode of operation.

The module provides its current operational status via the Web GUI and CLI. When connecting to the module via the Web GUI, the CO or User can confirm the current mode of operation by locating the FIPS icon in the top HPE VCM banner. If the FIPS icon is present, the module is operating in the FIPS-Approved mode.

When accessing the module via the CLI, the CO or User can determine the current mode of operation with the "show domain" command. The CLI will output "FIPS Mode: true" if the module is operating in the FIPS-Approved mode.

3.2.3 Save Domain and Export Dump

The CO is capable of saving an encrypted version of the module's configuration file or support file. The generation of the key used for the encryption of these files is performed by an SP800-132 PBKDF2. When the CO is prompted to enter a new "Encryption key" (password), the CO shall enter a password no less than 8 characters in length. The password shall consist of upper-case and lower-case letters and numbers. The probability of guessing the password will be equal to $1:62^8$, or $1:2.18 \times 10^{11}$. The key derived by the PBKDF2 is used solely for storage purposes.

3.2.4 Zeroization

Ephemeral keys can be zeroized by power-cycling the Virtual Connect hardware platform. Keys stored in NOR flash and the ISMIC[51] (refer to Table 10) can be zeroized via the Destroy Domain screen in the "Configuration" tab of the Web GUI or with the "delete domain –zeroize" command in the CLI. Keys stored in NAND flash are encrypted with the Module Key; therefore, they are not required to meet zeroization requirements. The keys stored in NAND flash will not be accessible after a zeroization service has been performed and the Module Key is zeroized.

3.2.5 Password Complexity

Passwords that are created by module operators shall be at least 8 characters in length and may contain any combination of uppercase and lowercase letters [A-z, a-z]; numbers [0-9]; and special characters (not including space).

3.2.6 TLS Version Configuration

The TLS v1.0 and TLS v1.1 protocol should not be used in the FIPS-Approved mode of operation. By default the TLS v1.2 protocol is enabled in the FIPS-Approved mode. An administrator with the CO role can use the Web SSL Configuration screen of the HPE VCM to be certain the TLS version is 1.2. It must remain "TLSv1.2 only". The "TLSv1, TLSv1.1, and TLSv1.2" option must not be selected.

[51] ISMIC – I2c Switch Management Interface Controller

3.3 User Guidance

An operator with the User role is neither authorized nor able to modify the configuration of the module. Users may only use the services listed in Table 7. Although Users do not have any ability to modify the configuration of the module, they should report to the CO if any irregular activity is observed.

3.4 Non-Approved Mode of Operation

When configured according to the Crypto Officer's guidance found herein, the module does not support a non-Approved mode of operation.

4. Acronyms

Table 11 provides definitions for the acronyms used in this document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DDR	Double Data Rate
DES	Data Encryption Standard
DH	Diffie-Hellman
DIP	Dual In-line Package
DRBG	Deterministic Random Bit Generator
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FC	Fibre Channel
FCC	Federal Communications Commission
FFC	Finite Field Cryptography

Acronym	Definition
FIPS	Federal Information Processing Standard
Gb	Gigabit
Gbps	Gigabits per second
GCM	Galois Counter Mode
GPIO	General Purpose Input/Output
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
HP	Hewlett Packard
HPSIM	HP Systems Insight Manager
HTTP	Hypertext Transport Protocol
HTTPS	Secure Hypertext Transport Protocol
I^2C	Inter-Integrated Circuit
I/O	Input/Output
IP	Internet Protocol
iSCSI	Internet Small Computer Systems Interface
ISMIC	I2c Switch Management Interface Controller
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KO	Keying Option
KPW	Key Wrap with Padding
KW	Key Wrap
LAN	Local Area Network
LANIO	Local Area Network I/O
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per Second
N/A	Not Applicable
NAND	Not AND
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
NOR	Not OR

Acronym	Definition
NVLAP	National Voluntary Laboratory Accreditation Program
NVRAM	Non-Volatile Random Access Memory
OA	Onboard Administrator
OFB	Output Feedback
OS	Operating System
PBKDF	Password-Based Key Derivation Function
PCI(e)	Peripheral Component Interface (express)
PKCS	Public Key Cryptography Standards
PKG	Public Key (Q) Generation
QSFP	Quad Small Form-factor Pluggable
RAM	Random Access Memory
RFC	Request for Comments
ROM	Read-Only Memory
RS	Requirement Specification
RSA	Rivest Shamir and Adleman
SAN	Storage Area Network
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-factor Pluggable
SFPT	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
U.S.	United States
USB	Universal Serial Bus
VC	Virtual Connect
VCEM	Virtual Connect Enterprise Manager
VCM	Virtual Connect Manager
VLAN	Virtual Local Area Network
WWN	World Wide Name

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com