Hewlett Packard Enterprise Development LP

HP BladeSystem c-Class Virtual Connect Module

Firmware Version: 4.41

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.6

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 if America
Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

1 INTRODUCTION 4
- 1.1 PURPOSE 4
- 1.2 REFERENCES 4
- 1.3 DOCUMENT ORGANIZATION 4
- 1.4 DOCUMENT TERMINOLOGY 4

2 BLADESYSTEM VIRTUAL CONNECT 6
- 2.1 OVERVIEW 6
  - *2.1.1 HP BladeSystem c-Class Virtual Connect Module 6*
- 2.2 MODULE SPECIFICATION 8
  - *2.2.1 Logical Cryptographic Boundary 8*
  - *2.2.2 Physical Cryptographic Boundary 8*
- 2.3 MODULE INTERFACES 10
- 2.4 ROLES AND SERVICES 12
  - *2.4.1 Crypto-Officer and User Services 12*
  - *2.4.2 General Operator Services 14*
  - *2.4.3 Non-Security Relevant Services 15*
  - *2.4.4 Authentication Security 15*
- 2.5 PHYSICAL SECURITY 16
- 2.6 OPERATIONAL ENVIRONMENT 17
- 2.7 CRYPTOGRAPHIC KEY MANAGEMENT 17
- 2.8 SELF-TESTS 26
  - *2.8.1 Power-Up Self-Tests 26*
  - *2.8.2 Conditional Self-Tests 26*
  - *2.8.3 Critical Functions Tests 27*
- 2.9 MITIGATION OF OTHER ATTACKS 27

3 SECURE OPERATION 28
- 3.1 INITIAL MODULE SETUP 28
- 3.2 SECURE MANAGEMENT 28
  - *3.2.1 Verifying the Approved Mode 28*
  - *3.2.2 Save Domain and Export Dump 29*
  - *3.2.3 Zeroization 29*
- 3.3 USER GUIDANCE 29

4 ACRONYMS 30

Table of Figures

FIGURE 1 – HP BLADESYSTEM C-CLASS VIRTUAL CONNECT MODULE LOGICAL BLOCK DIAGRAM 8
FIGURE 2 – HP VIRTUAL CONNECT HARDWARE BLOCK DIAGRAM 9
FIGURE 3 – HP VIRTUAL CONNECT FLEX 10/10D BLADE (FRONT VIEW) 10
FIGURE 4 – HP VIRTUAL CONNECT FLEX-10 10GB ETHERNET BLADE (FRONT VIEW) 10
FIGURE 5 – HP VIRTUAL CONNECT FLEXFABRIC 10GB/24-PORT BLADE (FRONT VIEW) 11
FIGURE 6 – HP VIRTUAL CONNECT FLEXFABRIC 20/40 F8 BLADE (FRONT VIEW) 11
FIGURE 7 – FIPS ICON LOCATION 29

List of Tables

TABLE 1 – FIPS 140-2 TERMINOLOGY COMPARISON 5
TABLE 2 – SECURITY LEVEL PER FIPS 140-2 SECTION 7
TABLE 3 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS 11
TABLE 4 – MAPPING HP ADMINISTRATIVE ROLES TO FIPS-DEFINED ROLES 12

TABLE 5 – CRYPTO OFFICER AND USER SERVICES 13
TABLE 6 – SERVICES NOT REQUIRING AN AUTHORIZED ROLE 15
TABLE 7 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 17
TABLE 8 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 19
TABLE 9 – ACRONYMS 30

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HP BladeSystem c-Class Virtual Connect Module from Hewlett Packard Enterprise Development LP This Security Policy describes how the HP BladeSystem c-Class Virtual Connect Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. 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. The HP BladeSystem c-Class Virtual Connect Module is referred to in this document as the HP Virtual Connect module, the crypto-module, or 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 HP website (http://www.hpe.com) contains information on the full line of products from HP.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

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

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to HP. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to HP and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact HP.

1.4 Document Terminology

This document uses terminology that slightly differs from terminology used in the HP Networking product documentation. Please use Table 1 as a reference to avoid confusion.

Table 1 – FIPS 140-2 Terminology Comparison

Security Policy Terminology	HP Development Company Equivalent
Cryptographic Module / Module	Refers to the logical cryptographic boundary of the FIPS 140-2 evaluated cryptographic module, as defined in Section 2.2. Example: HP BladeSystem c-Class Virtual Connect Module
BladeSystem Blade / Blade	Representative of all of the HP BladeSystem c-class modules that can be embedded into an HP BladeSystem c3000 or HP BladeSystem c7000 enclosure. The Virtual Connect FlexFabric and Virtual Connect Ethernet modules represent the physical cryptographic boundary of the FIPS 140-2 evaluated cryptographic module. Example: HP Virtual Connect Flex-10/10D Blade
BladeSystem Enclosure / Enclosure	Refers to either the HP BladeSystem c3000 or HP BladeSystem c7000 Enclosure. These enclosures host the embedded c-Class Virtual Connect modules. Example: HP BladeSystem c7000 enclosure

2 BladeSystem Virtual Connect

2.1 Overview

The HP BladeSystem is a rack-mount enterprise-class computing infrastructure designed to maximize power while minimizing costs, saving up to 56% of the total cost of ownership compared to traditional infrastructures. An example HP BladeSystem environment may consist of an HP BladeSystem c3000 or HP BladeSystem c7000 enclosure, one or two Onboard Administrator (OA) blades for enclosure management, one or more Virtual Connect (VC) blades to provide Ethernet and Fiber Channel (FC) network connectivity, and one or more of a range of blades designed to provide flexible computation or storage services.

HP Virtual Connect technology virtualizes the connections between the server and the network infrastructure (server-edge virtualization) so networks can communicate with pools of HP BladeSystem servers. This allows you to change servers in minutes instead of days or weeks. VC provides the following:

- Cleanly separates server enclosure administration from Local Area Network (LAN) and Storage Area Network (SAN) administration
- Allows you to add, move, or replace servers without impacting production LAN and SAN availability
- Enables HP 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

VC takes the existing LAN and SAN management interfaces and adds an abstraction layer, or virtualization layer, between the edge of the server and the edge of the network. As a result, the external networks connect to a shared resource pool of servers rather than to individual servers. The VC modules interact with the server blades through the enclosure mid-plane.

Administrators use VC management tools (VC Enterprise Manager (VCEM) or VC Manager (VCM)) to create an I/O[1] connection profile for each server after physically making the LAN and SAN connections to the VC modules. The VCM provides management capabilities that run on a processor in the VC Ethernet blade. This means each BladeSystem enclosure must have at least one VC Ethernet blade. The I/O connection profile, or server profile, provides the linkage between the server and the connections defined in VC. Server profiles contain information about server addresses, connections, and boot parameters.

2.1.1 HP BladeSystem c-Class Virtual Connect Module

The HP BladeSystem c-Class Virtual Connect Module is a firmware module made up of four separate elements (subsystems) which function together to provide a virtualized network fabric that connects servers to networking and storage. Each subsystem contributes to a separate operational function of the module such as administration, networking, authentication, and cryptography. The module's subsystems are explained below:

- VC Administration Subsystem – This subsystem consists of the Apache Web Server software, OpenSSH server, the HTTP[2] interface logic, I/O drivers, and circuitry logic API[3]. It exposes logical interfaces accessible via HTTPS[4], SOAP[5], and SSH[6] that allow management of the VC.

[1] I/O – Input/Output
[2] HTTP – HyperText Transport Protocol
[3] API – Application Programming Interface
[4] HTTPS – Secure HyperText Transport Protocol
[5] SOAP – Simple Object Access Protocol
[6] SSH – Secure Shell

There are interfaces with HPSIM[7] and VCEM over SOAP. HPSIM is a management application that communicates with the HP Onboard Administrator (OA), HP Integrated Lights-Out (iLO), and HP Virtual Connect blades in the c-Class enclosure. VCEM is an application that administers network address assignments, performs group-based configuration management and provides failover server connections for Virtual Connect domains.

- VC Security Manager Subsystem – This subsystem performs user authentication and account management, and also provides integration into existing LDAP[8] directories.

- VC Crypto Engine – This subsystem includes all the cryptographic libraries for handling the activation of FIPS mode, as well as the memory registers and non-volatile storage used for managing cryptographic keys. Used in key generation, authentication, certificate self-signing, validation, and encryption.

- VC Network/Storage Management Subsystem – This subsystem encompasses the internal management Ethernet interface connected to the enclosure management LAN, the TCP/IP[9] stack, and the data link and physical layer interface drivers used by the Operating System (OS) to communicate with other BladeSystem blades over the management network. This subsystem performs port aggregation and bridging logic for the server downlinks as well as the external uplinks. It also provides VLAN[10] port security.

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 HP website (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA4-8174ENW&cc=us&lc=en).

The HP BladeSystem c-Class Virtual Connect Module is validated at the following FIPS 140-2 Section levels:

Table 2 – 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[11]
7	Cryptographic Key Management	1
8	EMI/EMC[12]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

[7] HPSIM – HP Systems Insight Manager
[8] LDAP – Lightweight Directory Access Protocol
[9] TCP/IP – Transmission Control Protocol/Internet Protocol
[10] VLAN – Virtual Local Area Network
[11] N/A – Not Applicable
[12] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The HP BladeSystem c-Class Virtual Connect Module is a firmware module with a multi-chip embedded embodiment. The overall security level of the module is 1. The logical cryptographic boundary of the HP Virtual Connect module is defined as the firmware. The firmware image (vcfwall441.bin) is executing on one of four HP BladeSystem c-Class Virtual Connect blades, which act at the module's physical cryptographic boundary. The blades are designed to be embedded within either the HP BladeSystem c3000 enclosure or HP BladeSystem c7000 enclosure.

2.2.1 Logical Cryptographic Boundary

As a firmware module, the HP Virtual Connect module has a logical cryptographic boundary. The logical cryptographic boundary is the border in which information such as cryptographic keys and encrypted data get passed to and from the module. The information is passed from and passed to the physical components of the blade on which the module is operating on. There are four main components which make up the HP Virtual Connect firmware image. Those components are shown in Figure 1, within the red, dotted box.

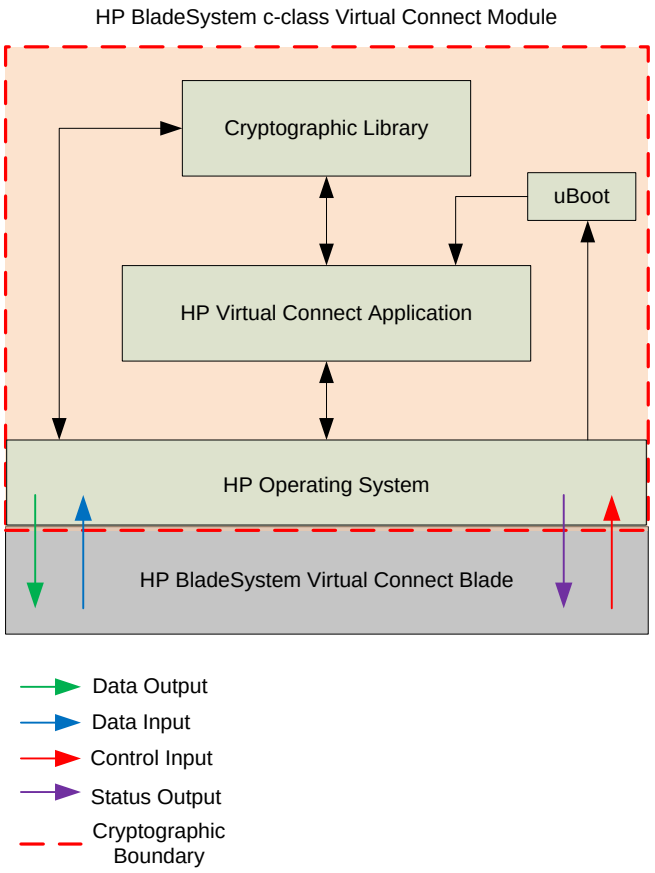

Figure 1 – HP BladeSystem c-Class Virtual Connect Module Logical Block Diagram

2.2.2 Physical Cryptographic Boundary

The HP Virtual Connect firmware module is designed to operate on one of four Virtual Connect embedded BladeSystem blades:

- HP Virtual Connect Flex-10/10D Blade
- HP Virtual Connect Flex-10 10Gb Ethernet Blade

- HP Virtual Connect FlexFabric 10Gb/24-Port Blade
- HP Virtual Connect FlexFabric 20/40 F8 Blade

These blades serve as the module's physical cryptographic boundary and are designed to be embedded within either the HP BladeSystem c3000 enclosure or HP BladeSystem c7000 enclosure. The processor located on each of the blades executes the module.

Figure 2 shows the hardware block diagram for the Virtual Connect BladeSystem blades. The block diagram demonstrates the major physical components and connections of each of the BladeSystem blades.

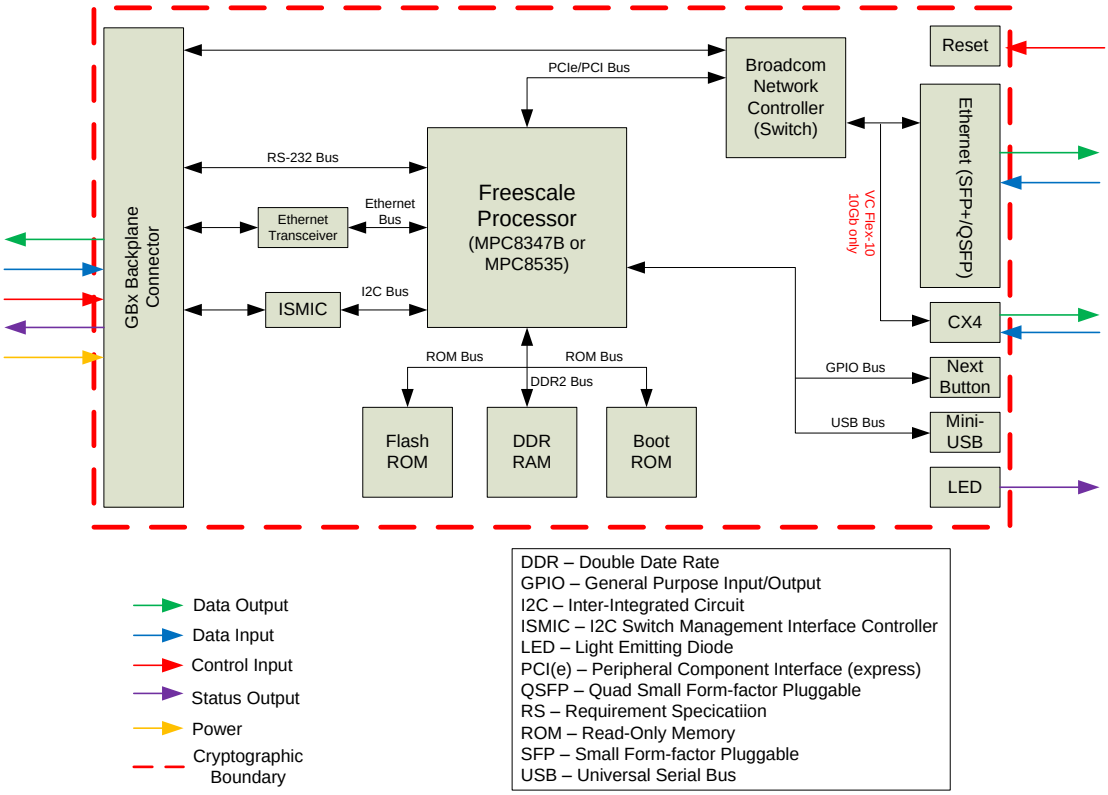

Figure 2 – HP Virtual Connect Hardware Block Diagram

2.3 Module Interfaces

The HP Virtual Connect module implements distinct interfaces in its firmware design. As a firmware cryptographic module, the HP Virtual Connect module features the physical ports of the HP BladeSystem blades. Both the firmware interfaces and the physical interfaces can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

These logical interfaces (as defined by FIPS 140-2) map to the blades' physical interfaces, as described in Table 3.

Figure 3 shows the front view of the HP Virtual Connect Flex-10/10D blade.

Figure 3 – HP Virtual Connect Flex-10/10D Blade (Front View)

Figure 4 shows the front view of the HP Virtual Connect Flex-10 10Gb Ethernet blade.

Figure 4 – HP Virtual Connect Flex-10 10Gb Ethernet Blade (Front View)

Figure 5 shows the front view of the HP Virtual Connect FlexFabric 10Gb/24-port blade.

Figure 5 – HP Virtual Connect FlexFabric 10Gb/24-Port Blade (Front View)

Figure 6 shows the front view of the HP Virtual Connect FlexFabric 20/40 F8 blade.

Figure 6 – HP Virtual Connect FlexFabric 20/40 F8 Blade (Front View)

During FIPS operation, the USB port is disabled. The Next button does not alter the operation of the HP BladeSystem c-Class Virtual Connect Module. The HP Virtual Connect module connects 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. This physical interface is called the "backplane connector" in the table below. It provides Serial, Ethernet, and I2C connectivity. VC management via the web GUI[13] and the CLI is provided by the backplane connector. Information flowing through the Ethernet interface is general, non-security relevant data.

Table 3 maps the module's logical and physical interfaces to the FIPS 140-2 logical interfaces.

Table 3 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	HP BladeSystem c-Class Virtual Connect Module Logical Port/Interface	HP BladeSystem c-Class Virtual Connect Module Firmware Port/Interface
Data Input	TLS[14], SSH, and plaintext sessions (CLI[15], Web)	Ethernet Interfaces (SFP+, CX4[16], QSFP[17]), backplane connector
Data Output	TLS, SSH, and plaintext sessions (CLI, Web)	Ethernet Interfaces (SFP+, CX4, QSFP), backplane connector
Control Input	CLI commands, Web GUI	Backplane connector, Reset button

[13] GUI – Graphical User Interface
[14] TLS – Transport Layer Security
[15] CLI – Command Line Interface
[16] Virtual Connect Flex-10 10Gb Ethernet Blade only
[17] Virtual Connect FlexFabric 20/40 F8 Blade only

FIPS 140-2 Logical Interface	HP BladeSystem c-Class Virtual Connect Module Logical Port/Interface	HP BladeSystem c-Class Virtual Connect Module Firmware Port/Interface
Status Output	CLI, Web, SOAP	Backplane connector, LEDs[18]
Power Interface	Not applicable	Backplane connector

2.4 Roles and Services

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 multiple User secure sessions at a time. Operators of the module assume the role of CO and User through role-based authentication mechanisms, which is implemented by the HP Virtual Connect Application. The module supports local and remote authentication methods. A CO or User can access the module by providing credentials stored on a remote LDAP server or stored locally by the HP Virtual Connect module.

Operators of the HP Virtual Connect module are assigned to a HP-defined administrative role. Each HP administrative role maps to a FIPS-defined role. FIPS-defined roles are explicitly selected based on the username provided by the operator. Each username is associated with one or more HP administrative roles and the FIPS role that they assume is based on the HP administrative role(s) that they are assigned. Any user assigned to the "Domain" HP Administrative role assumes the CO role. Table 4 maps the HP administrative roles to their FIPS-defined role. Example services for each role are provided in the table. Table 5 in Section 2.4.1 lists the Approved security services for both the CO and User.

Table 4 – Mapping HP Administrative Roles to FIPS-Defined Roles

HP Administrative Role	Description	FIPS-defined Role
Domain	Define local user accounts, set passwords, define roles; Configure role-based user authentication; Import enclosures	CO
Network	Configure network default settings; Select the MAC address range to be used by the VC domain; Create, delete, and edit networks	User
Server	Create, delete, and edit server Virtual Connect profiles; Assign and unassign profiles to device bays; Select and use available networks	User
Storage	Select the WWNs[19] to be used by the domain; Set up the connections to the external FC Fabrics; Configure FC SNMP[20] settings	User

2.4.1 Crypto-Officer and User Services

Descriptions of the services available to the Crypto-Officer and User roles are provided in Table 5 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table 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.

[18] LED – Light Emitting Diode
[19] WWN – World Wide Name
[20] SNMP – Simple Network Management Protocol

- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 5 lists the services that the Crypto-Officer and User have access to.

Table 5 – Crypto Officer and User Services

Service	Description	Role Access	CSP and Type of Access
Create/modify users	Create, edit; and delete users; define user accounts and assign permissions.	CO	User Password –W
Change CO Password	Change the Crypto-Officer password	CO	Crypto-Officer Password – W
Change User Password	Change the User Password	CO, User	User Password – W
Access the CLI	Manage the module using the CLI, accessed via SSH protocol over Ethernet or via serial console Configure network default settings, manage server Virtual Connect profiles, and device profiles; Select and use available networks; Select the WWNs[21] to be used by the domain; Set up the connections to the external FC Fabrics; Configure FC SNMP[22] settings	CO, User User only	Crypto-Officer Password – X User Password – X SSH Session Key – W/X DH[23] Public/Private Key Components – W/X SSH Integrity Key – W/X SSH Encryption Key – W/X RSA[24] SSH Public/Private Keys – X
Access the GUI	Access the GUI via HTTPS connection through web browser Configure network default settings, manage server Virtual Connect profiles, and device profiles; Select and use available networks; Select the WWNs to be used by the domain; Set up the connections to the external FC Fabrics; Configure FC SNMP settings	CO, User User only	Crypto-Officer Password – X User Password – X Crypto-Officer LDAP Password – X User LDAP Password – X TLS Session Key – W/X DH Public/Private Key Components – W/X RSA TLS Public/Private Keys – X TLS Integrity Key – W/X TLS Encryption Key – W/X
Zeroize Keys	Zeroize all keys[25], certificates, and users. Resets default CO password to factory settings	CO	All Keys – W
Check FIPS Mode Status	Display FIPS status of module	CO, User	None

[21] WWN – World Wide Name
[22] SNMP – Simple Network Management Protocol
[23] DH – Diffie-Hellman
[24] RSA – Rivest, Shamir, Adleman
[25] Please see Table 8 for the list of keys that can be zeroized using the "Zeroize Keys" service. More specifically, if a key listed in Table 8 has the text "Zeroized via GUI or CLI zeroization command" in the "Zeroization" column, then it can be zeroized with the "Zeroize Keys" service.

Service	Description	Role Access	CSP and Type of Access
Initialize module (Enter FIPS Mode)	Initializes the module in FIPS mode	CO	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	CO	Backup Encryption Key Password – W/X Backup Encryption Key – W/X
Restore module	Restore the module with an encrypted domain configuration file	CO	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	CO	Support Encryption Key Password – W/X Support Encryption Key – W/X
Connect to Onboard Administrator	Communicate with HP Onboard Administrator to obtain status	CO	TLS Session Key – W/X TLS Integrity Key – W/X TLS Encryption Key – W/X
Configure SNMP settings	Enable and disable SNMP; Configure SNMP access types	CO, User	SNMP Privacy Key – W SNMP Authentication Key – W
Connect via SNMP	Connect to the module via SNMP	CO, User	SNMP Privacy Key – RX SNMP Authentication Key – RX
Generate TLS Certificate	Generate a TLS certificate to be used for new TLS sessions	CO	RSA TLS Public/Private Keys – W
Import TLS Certificate	Import a TLS certificate generated by a Certificate Authority	CO	RSA TLS Public Key – W
Import Asymmetric Keys	Import a trusted key pair to be used for services such as SSH and SFTP[26]	CO, User	RSA SSH Public/Private Keys – W
Update Firmware	Update module firmware with newer version; Verify module firmware with public key	CO	Firmware Update Key – X
Self-tests	Initiate power-up self-tests on demand via reboot or power cycle	CO User	None

2.4.2 General Operator Services

The module provides additional services to operators not requiring to assume an authorized role (listed in Table 6). The module will communicate with HP Virtual Connect modules running on other blades in order to synchronize configuration data and export encrypted support files. This allows other HP Virtual

[26] SFTP – Secure File Transfer Protocol

Connect modules to be a back-up in case the primary HP Virtual Connect module becomes disabled. These services allow external VC modules to access status information from the module. The request for the configuration file does not require an operator to assume an authorized role as it does not require operator interaction. The services listed in Table 6 do not affect the overall security of the module nor do they modify any secret keys or CSPs.

Table 6 – Services Not Requiring an Authorized Role

Service	Description	CSP and Type of Access
Synchronize with Back-up VC	Synchronize configuration data with the back-up VC module	Back-up Module Password – X SSH Encryption Key – X SSH Integrity Key – X
Support File Extraction	Extract encrypted support file with an external VC unit	VC Dump Password – X SSH Encryption Key – X SSH Integrity Key – X
VC Management	Provide configuration data to HP Onboard Administrator	VC 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

2.4.3 Non-Security Relevant Services

The module offers additional services to all operators, which are not relevant to the secure operation of the module. All services provided by the modules are listed in the *HP Virtual Connect for c-Class BladeSystem Version 4.40/4.41 User Guide; Part Number: 798322-002, Dated: March 2015*. The product guide is supplied with the shipment of the HP c-Class BladeSytem Blades which host the module; or may be freely obtained at http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04562188&lang=en-us&cc=us.

2.4.4 Authentication Security

The module supports role-based authentication. Authentication credentials can be stored locally or on a remote LDAP server. Roles are explicitly selected based on the username provided by the operator. In order to log in as the CO, an operator will provide the username associated with the "Domain" HP administrative role, in addition to the correct password. In order to log in as the User, an operator will provide the unique username associated with the "Network", "Server", or "Storage" HP administrative role in addition to the correct password.

Users that are stored on a remote LDAP server are assigned to one or multiple groups. Each group is given an HP administrative role. When logging in with an LDAP credential, the user is given the role designated by the LDAP group they are assigned. If they are assigned to multiple LDAP groups, then they will obtain multiple HP administrative roles. In order to log in as the CO, an operator will provide the username

associated with the "Domain" LDAP groups. In order to log in as the User, an operator will provide the unique username associated with the "Network", "Server", or "Storage" LDAP groups.

Crypto-Officer and User passwords that are created by the CO or user must be at least 8 characters in length and can contain upper- and lower-case letters [A-z, a-z], numbers [0-9], and special characters (ie. !,@,#,$); not including space. Each character of the 8 character password could be 1 of 94 printable ASCII[27] characters, providing for a password strength of (1:94^8 =) 1 in 6,095,689,385,410,816.

In order to access the remote LDAP server, authentication is made with the server using the server's public RSA key located on the server's certificate. Once a connection to the LDAP server is established, authentication data is wrapped with the server's public key. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is 1:2^{112}

The fastest network connection supported by the module (for management) is 100 Mbps[28]. Hence at most (100 x 1024^2 bits × 60 seconds=) 6.29 x 10^9 bits of data can be transmitted to the module in one minute (assuming no overhead).

For both local password and RSA public key authentication, 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. The calculations are presented below for each authentication type.

For local password authentication, each password attempt is (8 bits x 8 characters =) 64 bits in length, meaning (6.29 x 10^9/64=) 9.83 x 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 x 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.

For RSA public key authentication, (6.29 x 10^9/112=) 5.62 x 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 x 10^7 keys per minute)
1: 9.24 x 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 and copyright notice and a getting started message followed by the CLI command prompt "->".
Upon successful login to the Web GUI, the operator is presented with the Virtual Connect Manager home page.

2.5 Physical Security

Since this is a firmware module, the module relies on the host platform to provide the mechanisms necessary to meet FIPS 140-2 physical security requirements. The host platform is one of four HP BladeSystem c-Class Virtual Connect Module BladeSystem blades, enclosed by an HP BladeSystem c-Class enclosure. All components of the target platform are made of production-grade materials, and all integrated circuits are coated with commercial standard passivation.

The host platforms have been tested for and meet applicable Federal Communications Commission (FCC) Electromagnetic Interference and Electromagnetic Compatibility requirements for business use as defined in Subpart B of FCC Part 15.

[27] ASCII – American Standard Code for Information Interchange
[28] Mbps – Megabits per second

2.6 Operational Environment

The HP BladeSystem c-Class Virtual Connect Module does not provide a general-purpose operating system (OS) to the user. The module runs a proprietary OS (HP OS 2.6.17), 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 the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update to the module.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 7 below.

Table 7 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[29] CBC[30], CTR[31], ECB[32] encryption/decryption and wrap/unwrap with 128-,192-, and 256-bit keys	3334
AES GCM[33] encryption/decryption and message authentication with 128- and 256-bit keys[34]	3334
Triple-DES[35] CBC mode encryption/decryption; KO[36] 1, 2	1904
RSA (FIPS 186-4) Key-pair Generation of 2048-bit keys	1713
RSA (FIPS 186-4) Signature Generation and Verification (PKCS[37] #1 v1.5) with 2048-bit keys	1713
SHA[38]-1, SHA-256, SHA-384, and SHA-512	2769
HMAC[39] with SHA-256. SHA-384, and SHA-512	2125
SP[40]800-90A CTR_DRBG[41]	776
TLS KDF[42]	488
SSH KDF	488
SNMP KDF	488

[29] AES – Advance Encryption Service
[30] CBC – Cipher Block Chaining
[31] CTR - Counter
[32] ECB – Electronic Code Book
[33] GCM – Galois Counter Mode
[34] In the event Module power is lost and restored the calling application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed as required by IG A.5.
[35] DES – Data Encryption Standard
[36] KO – Keying Option
[37] PKCS – Public Key Cryptography Standard
[38] SHA – Secure Hash Algorithm
[39] HMAC – (keyed-) Hashed Message Authentication Code
[40] SP – Special Publication
[41] DBRG – Deterministic Random Bit Generator
[42] KDF – Key Derivation Function

Algorithm	Certificate Number
PBKDF2[43]	Vendor affirmed

The module employs the following key establishment methodologies, which are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key encapsulation; key establishment methodology provides between 112 and 256 bits of encryption strength)

Additionally, the module utilizes the following non-FIPS-approved algorithm implementations allowed for use in FIPS-mode:

- Linux NDRNG[44] (/dev/random) – for seeding the FIPS-approved DRBG
- OpenSSL *md_rand* – provides Salt as input to the PBKDF2 function

Hewlett Packard Development Company, L.P. affirms compliance with SP 800-132 for the full implementation of PBKDF2. The HP BladeSystem c-Class Virtual Connect Module implements option 1(a) from section 5.4 of the Special Publication. Please refer to Section 3.2.2 for Crypto-Officer guidance specific to this function.

[43] PBKDF2 – Password-Based Key Derivation Function 2. (PBKDF2 is published in Internet Engineering Task Force Request for Comments (RFC) 2898 and maps to PBKDF defined in NIST SP 800-132.)
[44] NDRNG – Non-Deterministic Random Number Generator

The module supports the critical security parameters (CSPs) listed below in Table 8.

Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key 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[45] Flash memory	Zeroized via GUI or CLI zeroization command	Used as PBKDF2 input to generate Module Key
Module Key	32-byte Data Protection Key (AES 256-bit key)	Generated internally via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Key used to encrypt all CSPs stored in NAND[46] flash memory
Utility Key Password	Random data (20 Bytes)	Generated internally via Approved DRBG	Output encrypted via SSH to the back-up module	Stored in plaintext in NOR Flash memory; Stored encrypted via Module Key in NAND Flash memory	Zeroized via GUI or CLI zeroization command	Used as PBKDF2 input to generate Utility Key
Utility Key	32-byte Data Protection Key (AES 256-bit key)	Generated internally via PBKDF2	Output encrypted via SSH protocol	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Key used to obfuscate Back-up Module Password
Backup Encryption Key Password	8-byte Password	Generated externally; Input electronically via TLS or SSH	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Password input to PBKDF2 function to derive Backup Encryption Key

[45] NOR – Not OR
[46] NAND – Not AND

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Back-Up Encryption Key	32-byte Data Protection Key (AES 256-bit key)	Generated internally via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Key used to encrypt VC configuration file
Support Encryption Key Password	8-byte Password	Generated externally; Input electronically via TLS or SSH	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; 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)	Generated internally via PBKDF2	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Key used to encrypt VC support file
AES GCM Key	AES 128- and 256-bit key	Internally Generated via approved DRBG	Not output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Encrypt and decrypt blocks of data; TLS Encryption Key
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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA SSH Public Key	RSA 2048-bit public key	Generated internally via Approved RSA Key Generation method; Input via configuration file restore	Output in plaintext; Output encrypted by Back-up Encryption Key	Stored encrypted via Module Key in NAND Flash memory	N/A[47]	SSH Protocol; SFTP; Signature verification; Key unwrapping
RSA TLS Public Key	RSA 2048-bit public key	Generated internally via Approved RSA Key Generation method; Input via configuration file restore	Output in plaintext; Output encrypted by Back-up Encryption Key	Stored encrypted via Module Key in NAND Flash memory	N/A	TLS protocol; Signature verification; Key unwrapping
RSA SSH Private Key	RSA 2048-bit private key	Generated internally via Approved RSA Key Generation method; Input via configuration file restore	Output encrypted by Back-up Encryption Key	Stored encrypted via Module Key in NAND Flash memory	N/A	SSH Protocol; SFTP; Signature generation; Key wrapping
RSA TLS Private Key	RSA 2048-bit private key	Generated internally via Approved RSA Key Generation method; Input via configuration file restore	Output encrypted by Back-up 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	Generated internally via SP800-135rev1 SSH KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Shared session key used to derive SSH Integrity Key and SSH Encryption Key

[47] N/A – Not Applicable

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Integrity Key	HMAC SHA-1 key	Generated internally via SP800-135rev1 SSH KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used to generate SSH payload integrity message; Used to verify integrity of SSH payload
SSH Encryption Key	Triple-DES key	Generated internally via SP800-135rev1 SSH KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used to encrypt/decrypt SSH payload
TLS Session Key	TLS master secret	Generated internally via SP800-135rev1 TLS KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Shared master secret used to derive TLS Integrity Key and TLS Encryption Key
TLS Integrity Key	HMAC SHA-1 key	Generated internally via SP800-135rev1 TLS KDF	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used to generate TLS payload integrity message; Used to verify integrity of TLS payload
TLS Encryption Key	AES 128- or 256-bit key	Generated internally via Approved DRBG	Never output from the module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used to encrypt/decrypt TLS payload
DH Public Key Components	Public components of DH protocol	Generated internally via Approved DRBG	Output in plaintext	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used for SSH session establishment and initial key exchange

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DH Private Key Components	Private exponent of DH protocol	Generated internally via Approved DRBG	Never output from module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; Module shutdown or reboot	Used for SSH session establishment and initial key exchange
Crypto-Officer Password	ASCII string (minimum 8 characters)	Generated externally; Input electronically via TLS or SSH; Input via configuration file restore	Output encrypted by Back-up Encryption Key	Stored obfuscated via SHA-512 hash in NAND Flash memory and encrypted via Module Key	Zeroized via GUI or CLI zeroization command	Used for Crypto-Officer authentication to the module
User Password	ASCII string (minimum 8 characters)	Generated externally; Input electronically via TLS or SSH; Input via configuration file restore	Output encrypted by Back-up Encryption Key	Stored obfuscated via SHA-512 hash in NAND Flash memory and encrypted via Module Key	Zeroized via GUI or CLI zeroization command	Used for User authentication to the module
Crypto-Officer LDAP Password	ASCII string (minimum 8 characters)	Generated externally; Input electronically via TLS	Never output from module	Not stored on the module	N/A	Used for Crypto-Officer authentication to the module via LDAP
User LDAP Password	ASCII string (minimum 8 characters)	Generated externally; Input electronically via TLS	Never output from module	Not stored on the module	N/A	Used for User authentication to the module via LDAP
Back-up Module Password	ASCII string (16 characters; excludes special characters)	Generated internally via Approved DRBG	Output encrypted via the Utility Key	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command	Used by the back-up VC unit in order to synchronize configuration data

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
VC Dump Password	ASCII string (12 characters; excludes special characters)	Generated internally via Approved DRBG	Output encrypted over TLS session via SANIO[48]	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command	Password used by external VC units to authenticate SSH session in order to extract a support file
SNMP Privacy Key	AES 128-bit key	Generated internally via SNMP KDF	Output encrypted by Back-up Encryption Key	Stored in plaintext in NOR Flash memory	Zeroized via GUI or CLI zeroization command	Encrypt packets being transferred via SNMP
SNMP Authentication Key	HMAC SHA-1 Key	Generated internally via SNMP KDF	Output encrypted by Back-up Encryption Key	Stored in plaintext in NOR Flash memory	Zeroized via GUI or CLI zeroization command	Authenticate packets being transferred via SNMP
Firmware Update Key	RSA 2048-bit Public Key	Generated externally; 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	Generated internally using nonce along with DRBG entropy input	Never output from module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; 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 GUI or CLI zeroization command; Module shutdown or reboot	Entropy material for SP 800-90A DRBG

[48] SANIO – Storage Area Network Input/Output

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG 'V' Value	Internal state value	Internally Generated	Never output from module	Stored in plaintext in volatile memory	Zeroized via GUI or CLI zeroization command; 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 GUI or CLI zeroization command; 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-Approved mode as well as 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 host blade and the module is loaded into memory. The list of power-up self-tests that follows may also be run on-demand when the CO or User reboots the BladeSystem blade. 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 BladeSystem blade to be returned to HP. The module indicates the critical error to the operator through the WebUI and via LED's.

The HP BladeSystem c-Class Virtual Connect Module performs the following self-tests at power-up:

- Firmware integrity check (HMAC SHA-256 checksum)
- Known Answer Tests (KATs)
    - Encrypt AES KAT (ECB mode)
    - Decrypt AES KAT (ECB mode)
    - Encrypt AES KAT (GCM mode)
    - Decrypt AES KAT (GCM mode)
    - Encrypt Triple-DES KAT
    - Decrypt Triple-DES KAT
    - RSA 186-4 Signature Generation KAT
    - RSA 186-4 Signature Verification KAT
    - SHA-1 KAT
    - HMAC SHA-256 KAT
    - HMAC SHA-384 KAT
    - HMAC SHA-512 KAT
    - SP800-90A 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 BladeSystem blade to be returned to HP. The module indicates the critical error to the operator through the WebUI and via LED's.

The HP BladeSystem c-Class Virtual Connect Module performs the following conditional self-tests:

- SP 800-90A CTR_DRBG Continuous Random Number Generator Test (CRNGT)
- Pairwise Consistency Test for RSA Key Generation
- NDRNG CRNGT
- Firmware Load Test using RSA Signature Verification

2.8.3 Critical Functions 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 Uninstatiate. 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 Unstinatiate 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 WebUI and automatically reboot. After 10 failed self-test attempts throughout the lifetime of the module, the module will no longer function; requiring the BladeSystem blade to be returned to HP.

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 modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The HP BladeSystem c-Class Virtual Connect Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

HP recommends that a module operator reads the specific *HP Virtual Connect for c-Class BladeSystem User Guide* for enclosure specific information before proceeding with Virtual Connect setup. This user guide provides information on the initial setup and operation of the HP BladeSystem Virtual Connect.

3.1 Initial Module Setup

Prior to operating the module for the first time, the Cryptographic Officer must configure a 4-pin DIP[49] switch located on the motherboard of the Virtual Connect BladeSystem blade. The switch is located at the front of the blade, on the opposite end of the backplane connector. In order to place the module in the FIPS-Approved 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 BladeSystem blade in order to access the DIP switch.

After configuring the DIP switch, the CO shall replace the cover on the blade, reinsert the blade into the Bladesystem enclosure, and power-up the module for the first time. The CO can confirm that the module is operating the FIPS-Approved mode via the WebUI or through the CLI. Additional information is provided in Section 3.2.1 on confirming the current mode of operation.

3.2 Secure Management

The module can be managed remotely via a WebUI or CLI. Through these management interfaces, a Crypto-Officer 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 HP Virtual Connect module is controlled by role-based authentication, described in Section 2.4. Access to the module via the WebUI is provided by HP Virtual Connect Manager. 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 HP Virtual Connect modules not configured to operate in the Approved mode cannot communicate with the module. In order for additional HP Virtual Connect modules to communicate with one another, they too must be operating in the FIPS-Approved mode. When initialized and configured per the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

3.2.1 Verifying the Approved Mode

The module provides its current operational status via the WebUI and via the CLI. When connecting to the module via the WebUI, the CO or User can confirm the current mode of operation by locating the FIPS icon in the top HP Virtual Connect Manager banner (Figure 7). If the 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.

[49] DIP – Dual In-line Package

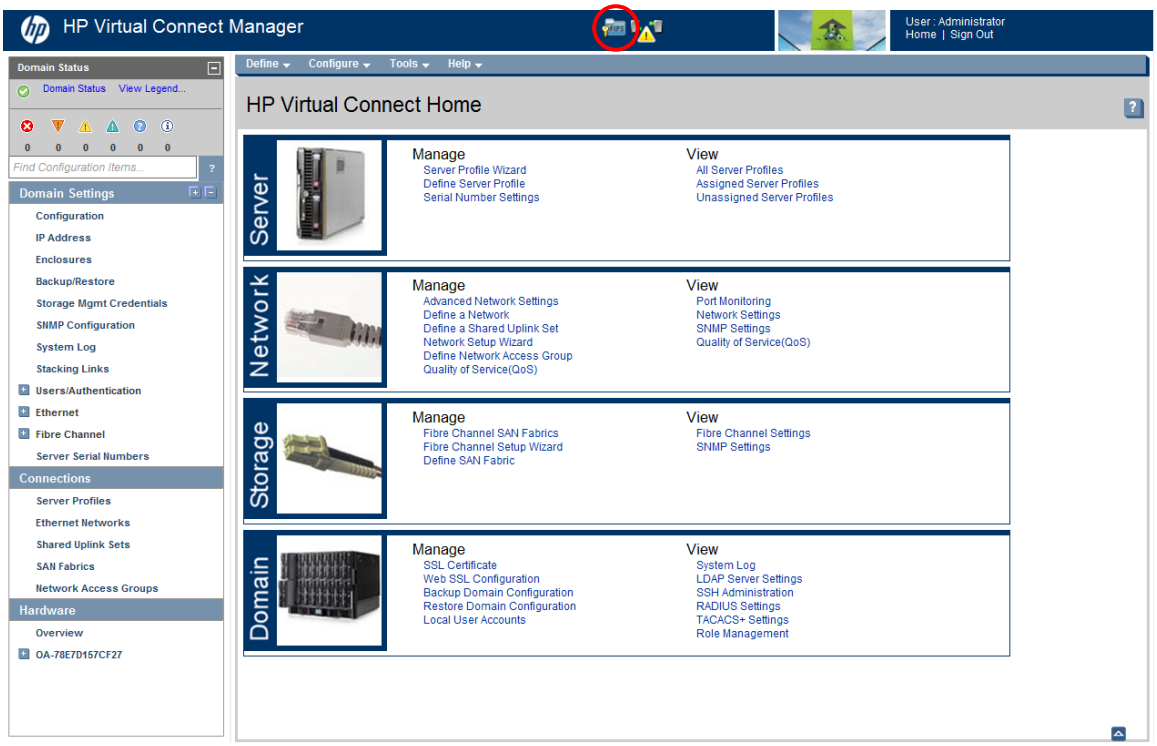

Figure 7 – FIPS Icon Location

3.2.2 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 $1:2.18x10^{11}$. The key derived by the PBKDF2 is used solely for storage purposes.

3.2.3 Zeroization

The Crypto-Officer is able to force zeroization of the module's plaintext CSPs, both stored and ephemeral, via the WebUI and CLI. Ephemeral keys can be zeroized by power-cycling the BladeSystem blade. Keys stored in NOR flash and the ISMIC (refer to Table 8) can be zeroized via the Destroy Domain screen in the "Configuration" tab of the WebUI or with the "delete domain –zeroize" command in the CLI. These services will zeroize all non-encrypted keys stored in NOR Flash. 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.

3.3 User Guidance

The User is neither authorized nor able to modify the FIPS-Approved configuration of the module. Users may only utilize the services listed in Table 5. Although Users do not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is observed.

4 Acronyms

Table 9 lists all of the acronyms used throughout this document.

Table 9 – 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
DDR2	Double Data Rate 2
DES	Data Encryption Standard
DH	Diffie-Hellman
DIP	Dual In-line Package
DRBG	Deterministic Random Bit Generator
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FC	Fibre Channel
FCC	Federal Communications Commission
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GCM	Gallois Counter Mode
GPIO	General Purpose Input/Output

Acronym	Definition
GUI	Graphical User Interface
HP	Hewlett Packard
HPSIM	HP Systems Insight Manager
HMAC	(keyed-) Hash Message Authentication Code
HTTP	Hypertext Transport Protocol
HTTPS	Secure Hypertext Transport Protocol
I2C	Inter-Integrated Circuit
I/O	Input/Output
IP	Internet Protocol
ISMIC	I2c Switch Management Interface Controller
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KO	Keying Option
LAN	Local Area Network
LANIO	Local Area Network I/O
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
N/A	Not Applicable
NAND	Not AND
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NOR	Not OR
NVLAP	National Voluntary Laboratory Accreditation Program
NVRAM	Non-Volatile Random Access Memory
OA	Onboard Administrator
OFB	Output Feedback
PBKDF	Password-Based Key Derivation Function
PCI(e)	Peripheral Component Interface (express)
PKCS	Public Key Cryptography Standards
RAM	Random Access Memory
RFC	Request for Comments
ROM	Read-Only Memory
RS	Requirement Specification

Acronym	Definition
RSA	Rivest Shamir and Adleman
SAN	Storage Area Network
SANIO	Storage Area Network Input/Output
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-factor Pluggable
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
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