

Symantec & CA Technologies, a Division of Broadcom Management Center Virtual Appliance

Software Version: 2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 1

Document Version: 0.8

COPYRIGHT NOTICE

Copyright © 2020 Symantec & CA Technologies, A Division Of Broadcom. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Symantec, and the Symantec logo are trademarks or registered trademarks of Symantec & CA Technologies, A Division of Broadcom. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC & CA TECHNOLOGIES, A DIVISION OF BROADCOM SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC & CA TECHNOLOGIES, A DIVISION OF BROADCOM PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

CONTACT INFORMATION

Symantec & CA Technologies, a division of Broadcom

1320 Ridder Park Dr,

San Jose, CA 95131

www.broadcom.com

This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Contents

1. INTRODUCTION	5
1.1 PURPOSE	5
1.2 REFERENCES	5
1.3 DOCUMENT ORGANIZATION.....	5
2. MANAGEMENT CENTER.....	6
2.1 OVERVIEW	6
2.2 MODULE SPECIFICATION	8
2.2.1 <i>Physical Cryptographic Boundary</i>	8
2.2.2 <i>Logical Cryptographic Boundary</i>	9
2.3 MODULE INTERFACES	10
2.4 ROLES AND SERVICES	11
2.4.1 <i>Crypto-Officer Role</i>	12
2.4.2 <i>User Role</i>	15
2.4.3 <i>Authentication Mechanism</i>	15
2.5 PHYSICAL SECURITY	19
2.6 OPERATIONAL ENVIRONMENT.....	19
2.7 CRYPTOGRAPHIC KEY MANAGEMENT.....	21
2.8 SELF-TESTS.....	31
2.8.1 POWER-UP SELF-TESTS.....	31
2.8.2 <i>Conditional Self-Tests</i>	32
2.8.3 <i>Critical Function Tests</i>	32
2.9 MITIGATION OF OTHER ATTACKS	32
3. SECURE OPERATION.....	33
3.1 INITIALIZATION	33
3.1.1 <i>Management</i>	34
3.1.2 <i>Zeroization</i>	34
3.2 USER GUIDANCE.....	35
4. ACRONYMS.....	36

List of Figures

FIGURE 1 TYPICAL DEPLOYMENT OF A MANAGEMENT CENTER VIRTUAL APPLIANCE.....	7
FIGURE 2 BLOCK DIAGRAM OF THE DELL POWEREDGE R830 SERVER HARDWARE	9

List of Tables

TABLE 1 SECURITY LEVEL PER FIPS 140-2 SECTION	7
TABLE 2 MANAGEMENT CENTER VIRTUAL APPLIANCE CONFIGURATIONS	8
TABLE 3 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE FRONT OF THE MC VA.....	11
TABLE 4 FIPS AND MANAGEMENT CENTER ROLES.....	12
TABLE 5 CRYPTO OFFICER ROLE SERVICES AND CSP ACCESS	12
TABLE 6 USER SERVICES AND CSP ACCESS	15
TABLE 7 AUTHENTICATION MECHANISMS USED BY THE MODULE.....	17
TABLE 8 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR THE MC VA JAVA CRYPTOGRAPHIC LIBRARY V1.0	21
TABLE 9 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR THE MC VA OS CRYPTOGRAPHIC LIBRARY V1.0	23
TABLE 10 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR THE VA MC SSH LIBRARY V1.0.....	24
TABLE 11 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR VA UEFI OS LOADER LIBRARY V4.14	24
TABLE 12 FIPS-ALLOWED ALGORITHMS.....	25
TABLE 13 LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS	26
TABLE 14 ACRONYMS	36

1. Introduction

1.1 Purpose

This is a *Non-Proprietary Cryptographic Module Security Policy* for the Management Center Virtual Appliance (Software Version 2.1) from Symantec & CA Technologies, a Division of Broadcom. This *Non-Proprietary Security Policy* describes how the MC VA 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 Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

This document also describes how to run the appliance in the Approved mode of operation. This policy was prepared as part of the Level 1 validation of the module. The Management Center VA is referred to in this document as MC VA, crypto module, or 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 Symantec website (www.broadcom.com) contains information on the full line of products from Symantec.
- 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 *Non-Proprietary 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
- *Entropy Assessment Report* document
- Other supporting documentation as additional references

With the exception of this *Non-Proprietary Security Policy*, the FIPS 140-2 Submission Package is proprietary to Symantec and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Symantec.

2. Management Center

2.1 Overview

The Symantec Management Center (MC) centrally manages and monitors the Symantec devices in your organization. You can organize devices into hierarchical groups, monitor device health, install policies to ProxySG devices, back up device configurations, and produce consolidated reports.

Management Center can manage up to 1000 individual devices on an enterprise network. Devices can be organized into hierarchies based on location, department, purpose, or other attributes you specify.

Role-based permissions allow greater flexibility, enabling user groups with the same permissions to access and manage policies and devices within their specific organization. User Groups with the same permissions access, manage, and can report on devices within their management area without overlapping job duties and wasting time and resources. Roles can be applied to user groups that you need to have homogenous results (for example user groups that are in specific locations or have a specific job function).

MC facilitates creating and deploying policy to multiple devices simultaneously. It includes Visual Policy Manager and consistency checking between policies and devices to help ensure consistency amongst devices that have the same purpose or require standardized policy. Administrators can manage policy using the Visual Policy Manager on managed devices from within the Management Center web interface.

Administrators can create and edit scripts as well as execute scripts on man-aged devices. Variable replacement is supported, as well as the ability to check versions of a saved script and to import a script from a device.

Management Center provides centralized reporting for managed devices. Statistics Monitoring reports are included by default and include:

- Devices
- WAN Optimization Reports

For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data:

- Security reports
- Web Application reports
- User Behavior reports
- Bandwidth Usage reports

Advanced Reporting provides visibility and a control point between employees of your organization and the cloud services and SaaS applications that users access (e.g., Box, Dropbox, Google Drive, Office 365, Salesforce, Facebook, etc.). Using full Reporter integration enables the discovery of all of the web applications in use, enabling you maximum visibility into all risky users, web sites and potential threats. See how trends of risky users and sites affect your company over time.

See Figure 1 below for a typical deployment scenario for Management Center Virtual Appliance appliances.

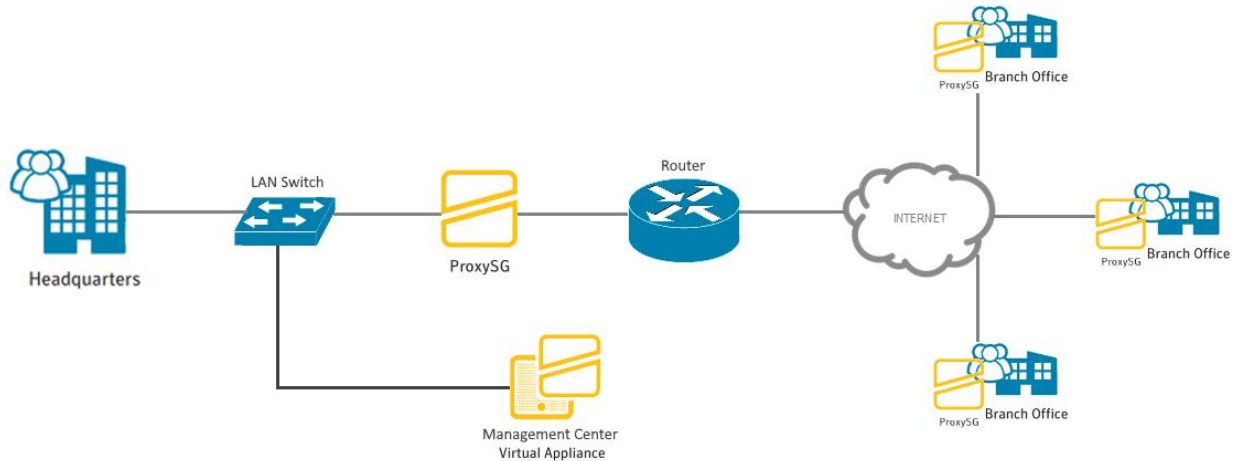


Figure 1 Typical Deployment of a Management Center Virtual Appliance

The Management Center Virtual Appliance is validated at the following FIPS 140-2 Section levels 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	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	Electromagnetic Interference/Electromagnetic Compatibility	1
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

For the FIPS 140-2 validation, the module was tested on the following Symantec virtual appliance configurations listed in Table 2.

Table 2 Management Center Virtual Appliance Configurations

Virtual Appliance Model	Number of Managed Devices
MC-V10-1	1
MC-V10-10	10
MC-V10-25	25
MC-V10-50	50
MC-V10-100	100
MC-V10-250	250
MC-V10-500	500
MC-V10-1000	1000

The different virtual appliances models in Table 2 represent changes in the number of managed devices only. All models are exactly the same from a cryptographic functionality and boundary perspective.

The MC VA is a multi-chip standalone software module that meets overall Level 1 FIPS 140-2 requirements. The module was tested and found compliant on a Dell PowerEdge R830 Server using VMware ESXi v6.0 hypervisor to provide the virtualization layer.

The MC VA software consists of a Linux-based operating system running the MC software. The module software, version 2.1, contains the following cryptographic libraries:

MC VA Java Cryptographic Library v1.0
 MC VA OS Cryptographic Library v1.0
 MC VA SSH Library v1.0
 VA UEFI OS Loader Library v4.14

2.2.1 Physical Cryptographic Boundary

As a software module, the virtual appliance has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hard enclosure around the Dell PowerEdge R830 Server on which it runs. Figure 2 shows the block diagram of the Dell PowerEdge R830 Server (the dashed line surrounding the hardware components represents the module's physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the Dell PowerEdge R830 Server's processor interfaces.

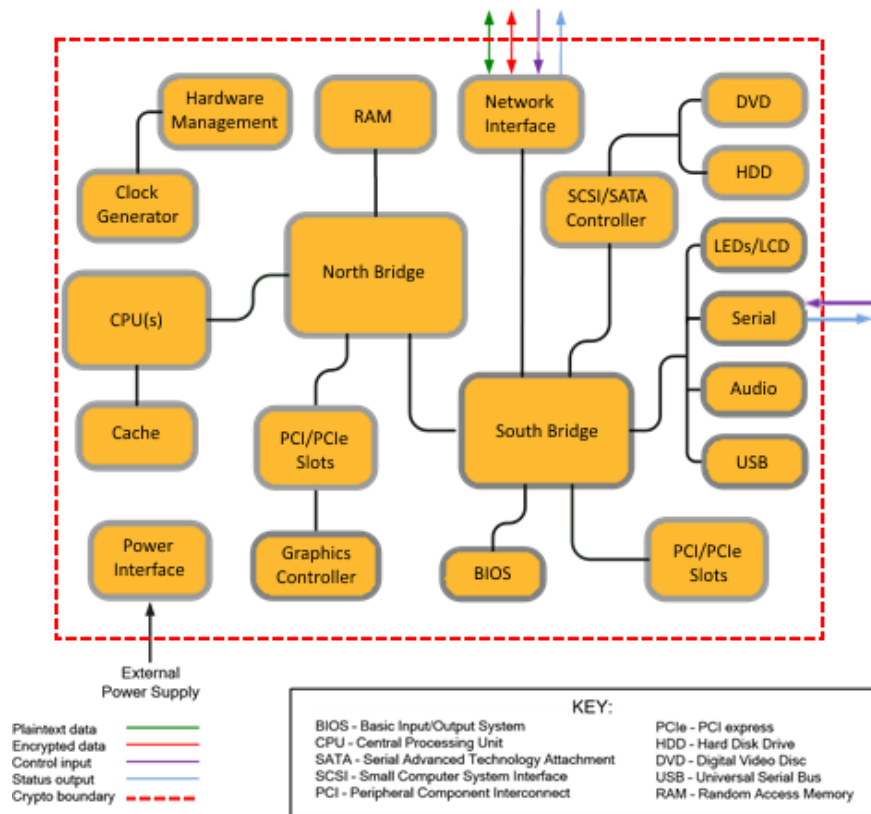


Figure 2 Block Diagram of the Dell PowerEdge R830 Server hardware

The module's physical cryptographic boundary is further illustrated by the black dotted line in Figure 3 below.

The module makes use of the physical interfaces of the tested platform hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the MC VA and the operator, and is responsible for mapping the module's virtual interfaces to the GPC's physical interfaces. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM¹, hard disk, device case, power supply, and fans. Figure 2 shows the block diagram of the Dell PowerEdge R830 Server (the solid black line surrounding the hardware components represents the module's physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the Dell PowerEdge R830 Server's processor interfaces.

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module (shown by the solid yellow line in Figure 3) consists of the OS (RHEL 6.9), which contains the Symantec VA UEFI OS Loader Library v4.14, Symantec MC VA Java Cryptographic Library v1.0, the Symantec MC VA OS Cryptographic Library v1.0, and the MC SSH Library v1.0.

¹ RAM - Random Access Memory

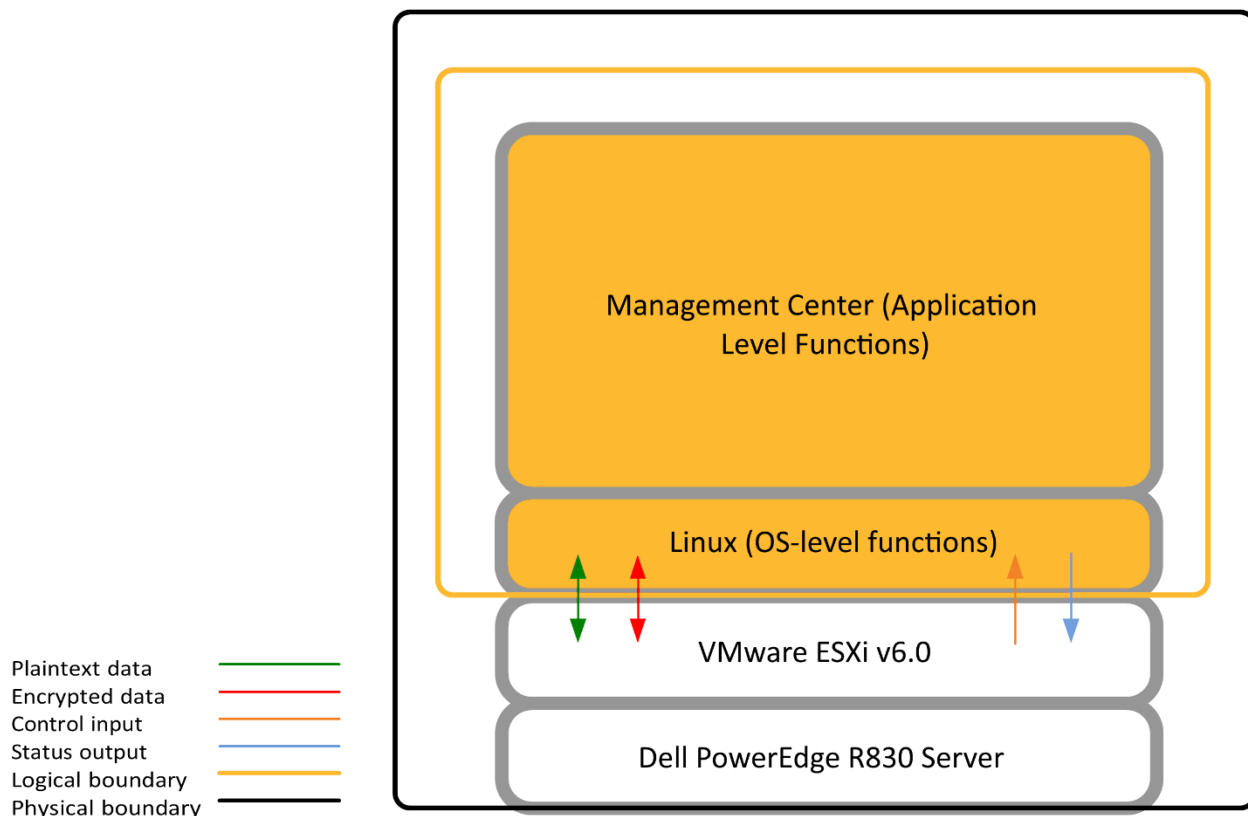


Figure 3 MC VA Cryptographic Boundary

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output

As a software module, the virtual appliance has no physical characteristics. The module's physical and electrical characteristics, manual controls, and physical indicators are those of the host system (Dell PowerEdge R830 Server). The VMware hypervisor provides virtualized ports and interfaces for the module. Interaction with the virtual ports created by the hypervisor occurs through the host system's Ethernet port. Management, data, and status traffic must all flow through the Ethernet port. Direct interaction with the module via the host system is possible over the serial port; however, the Crypto Officer must first map the physical serial port to the MC VA using vSphere Client. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 3 below.

Table 3 FIPS 140-2 Logical Interface Mappings for the front of the MC VA

Physical Port / Interface	Logical Port/Interface	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports Virtual Serial Ports	Data Input Data Output Control Input Status Output
Host System Serial Port	Virtual Serial Port	Control Input Status Output

Data input and output are the packets utilizing the services provided by the modules. These packets enter and exit the module through the Virtual Ethernet ports. Control input consists of Configuration or Administrative data entered into the modules. Control input enters the module via the Virtual Ethernet and Virtual Serial Port interfaces (Management Center Web Interface, SSH CLI, and Serial CLI). Status output consists of the status provided or displayed via the user interfaces (such as Management Center Web Interface, SSH CLI, and Serial CLI) or available log information. Status output exits the module via the user interfaces (such as Management Center Web Interface, SSH CLI, and Serial CLI) over the Virtual Ethernet or Virtual Serial Ports.

2.4 Roles and Services

Before accessing the modules for any administrative services, COs and Users must authenticate to the module according to the methods specified in Table 7. The modules offer the following management interfaces:

- CLI² – This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. When the module has been properly configured, this interface can be accessed via SSH³. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.
- Management Center Web Interface – This interface is used for management of the module. It is accessible remotely with a web browser that supports TLS⁴. Authentication is required before any functionality will be available through the Management Center Web Interface.

When managing the module over the CLI, COs and Users both log into the module with accounts entering the “standard”, or “unprivileged” mode on the MC CLI. Unlike Users, COs have the ability to enter the “enabled” or “privileged” mode after initial authentication to the CLI by supplying the “enabled” mode password. Additionally, COs can only enter the “configuration” mode from the “enabled” mode via the CLI, which grants privileges to make configuration level changes. Going from the “enabled” mode to the “configuration” mode does not require additional credentials. The details of these modes of operation are found below in Table 4.

The CO and User details are found below in Table 4.

² CLI – Command Line Interface

³ SSH – Secure Shell protocol

⁴ TLS – Transport Layer Security

Table 4 FIPS and Management Center Roles

FIPS Roles	Management Center Virtual Appliance Roles and Privileges
CO	<ul style="list-style-type: none"> • The CO is an administrator of the module that has been granted “enabled” mode access while using the CLI and “read/write” access while using the Management Center Web Interface. • When the CO is using the CLI, and while in the “enabled” mode of operation, COs may put the module in its Approved mode, reset to the factory state and query if the module is in Approved mode. In addition, COs may do all the services available to Users while not in “enabled” mode. • Once the CO has entered the “enabled” mode, the CO may then enter the “configuration” mode via the CLI. The “configuration” mode provides the CO management capabilities to perform tasks such as account management and key management. • When the CO is administering the module over the Management Center Web Interface, they can perform all the same services available in CLI (equivalent to being in the “configuration” mode in the CLI) except the module may not be into the Approved mode via the Management Center Web Interface.
User	<ul style="list-style-type: none"> • The User is an administrator of the module that operates only in the “standard” or “unprivileged” mode and has not been granted access to the “enabled” mode in the CLI, and has been given “read-only” privileges when using the Management Center Web Interface. • The User may access the CLI and Management Center Web Interface for management of the module. When the User is administering the module over the Management Center Web Interface, they perform all the same services available in CLI (“standard” mode only services).

Descriptions of the services available to a Crypto Officer (CO) and Users are described below in Table 5 and Table 6 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. There are no additional services that are unauthenticated. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

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

2.4.1 Crypto-Officer Role

Descriptions of the FIPS 140-2 relevant services available to the Crypto-Officer role are provided in the table below. Additional services that do not access CSPs can be found in the *Symantec Management Center Configuration & Management Guide v2.1.1.1*.

Table 5 Crypto Officer Role Services and CSP Access

Service	Description	CSP and access required
Set up the module (serial port only)	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode of operation. For more information, see section 3.1 in this <i>Security Policy</i> .	CO Password: W “Enabled” mode password: W

Service	Description	CSP and access required
Enter the “enabled” mode (CLI)	Manage the module in the “enabled” mode of operation, granting access to higher privileged commands	“Enabled” mode password: R
* Enter the “configuration” mode (CLI)	Manage the module in the “configuration” mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Take the module out of the approved mode of operation and restore it to a factory state	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DH private key: W ECDH private key: W DRBG CSPs: W DPK: W
** Software Load	Loads new external software and performs an integrity test using an RSA digital signature.	Integrity Test public key: WRX
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key: RX RSA private key: RX DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX SSH Session Key: WRX SSH Integrity Key: WRX DRBG CSPs: WRX CO Password: R
Create remote management session (MC)	Manage the module through the Management Center Web Interface (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX TLS Session Key: WRX TLS Integrity Key: WRX TLS Pre-Master Secret: WRX TLS Master Secret: WRX DRBG CSPs: WRX CO Password: R
** Create, edit, and delete User Groups	Create, edit and delete operator groups; define common sets of operator permissions.	None
** Create, edit, and delete operators	Create, edit and delete operators (these may be COs or Users); define operator’s accounts, change password, and assign permissions.	Crypto-Officer Password: W User Password: W DPK: RX
Device Policy and Configuration (MC Web Interface)	Create new policies or import existing policy objects from managed devices. Policy objects can be deployed across data centers	None

Service	Description	CSP and access required
	containing hundreds of hierarchies, device groups, and devices.	
Create and Manage Job and Job Schedules (MC Web Interface)	Create jobs to facilitate device backups, health status monitoring, device configuration compliance, policy import/installation, and system image upgrades.	None
Generate Managed Device Encryption Key	Create the key used to encrypt the managed device credentials.	Managed Device Encryption Key: W
Add device for management	Add a device to be managed from Management Center. An HTTPS session with the device will be established to verify connectivity.	RSA public key: RX ECDH public key: WRX ECDH private key: WRX TLS Session Key: WRX TLS Integrity Key: WRX TLS Pre-Master Secret: WRX TLS Master Secret: WRX DRBG CSPs: WRX MDEK: RX
Show FIPS-mode status (CLI)	The CO logs in to the module using the CLI. Entering the command “show version” will display if the module is configured in Approved mode.	None
Show FIPS-mode status (MC Web Interface)	The CO logs in to the module using the Management Center Web Interface and navigates to the About menu that will display if the module is configured in Approved mode.	None
* Zeroize keys	Zeroize keys by taking the module out of the Approved mode and restoring it to a factory state. This will zeroize all CSPs. The zeroization occurs while the module is still in Approved-mode.	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DH private key: W ECDH private key: W DPK: W
** Change password (CLI)	Change Crypto-Officer password	Crypto-Officer Password: RW
Change password (MC Web Interface)	Change Crypto-Officer password	Crypto-Officer Password: RW
* Perform self-test (CLI)	Perform self-test on demand by rebooting the machine	DH public key: W DH private key: W ECDH public key: W ECDH private key: W SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: W

Service	Description	CSP and access required
* Reboot the module (CLI)	Reboot the module.	DH public key: W DH private key: W ECDH public key: W ECDH private key: W SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: W

* - Indicates services that are only available once the CO has entered the “enabled” mode of operation.

** - Indicates services that are only available once the CO has entered the “enabled” mode followed by the “configuration” mode of operation.

2.4.2 User Role

Descriptions of the FIPS 140-2 relevant services available to the User role are provided in the table below. Additional services are that do not access CSPs can be found in the *Symantec Management Center Configuration & Management Guide v2.0.1.1* located here:

https://support.symantec.com/content/unifiedweb/en_US/article.DOC11011.html.

Table 6 User Services and CSP Access

Service	Description	CSP and access required
Create remote management session	Manage the module through the Management Center Web Interface (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX DH public key: RX DH private key: RX ECDH public key: RX ECDH private key: RX TLS Session Key: WRX TLS Integrity Key: WRX TLS Pre-Master Secret: WRX TLS Master Secret: WRX DRBG CSPs: WRX User Password: R
Show FIPS-mode status	The User logs in to the module using the Management Center Web Interface and navigates to the About menu which will display if the module is configured in Approved mode.	None
Change password	Change User password	User Password: RW

2.4.3 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a user ID and password, or certificates associated with the TLS protocol to set up the secure session. Secure sessions that authenticate Users have

no interface available to access other services (such as Crypto Officer services). Each CO or User SSH session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed. Each CO and User Management Center Web Interface session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

Modules used by the United States Department of Defense (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated Common Access Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV⁵ II card authentication.

When the module is configured to use CAC authentication, it will support TLS mutual authentication. This will validate a client certificate against a chosen certificate authority (CA) list. CAC authentication will take place against a Certificate realm, and CO and User authorization takes place against an LDAP realm.

The authentication procedure leverages 3rd party middleware on the management workstation to facilitate two factor authentication of the user to their CAC using a Personal Identification Number (PIN). This process enables the module to retrieve the X.509 certificate from the microprocessor smart card. The process is as follows:

1. On the management workstation, access the CLI and enter the following command to enable mutual authentication:

```
# security ssl client-authentication set-mandatory
```
2. Import the CA certificates necessary as follows:

```
# security ssl import external-certificate <name> <URL>
# security ssl import server-certificate <URL>
```
3. Verify installation was successful with the following command:

```
# security ssl list external-certificate all
```
4. The TLS handshakes begin. The module requires a certificate to complete the handshake (i.e. the verify-peer setting has been enabled).
5. The browser presents the CO or User with a dialog box prompting which certificate to select.
6. The CO or User selects the X.509 certificate on the CAC.
7. The middleware on the management workstation prompts the CO or User for the PIN to unlock the certificate. The CO or User enters the PIN and the certificate is transmitted to the module.
8. The module authenticates the certificate with the following checks:
 - The certificate must be issued by a CA included in the module's truststore.
 - The appliance confirms that the browser has the certificate's private key by challenging the browser to sign random data. The appliance validates the signature using the browser's certificate.
 - The certificate must have a valid signature and not be expired.
9. The module extracts the subject name (of the CO or User) from the subjectAltNames extension of the X.509 certificate according to configuration of the certificate realms, Within the subjectAltNames extension is the CO or User's userPrincipleName (UPN) (when PIV cards are used in place of CACs, the CommonName (CN) field is extracted from the certificate instead). The UPN/CN is what ties the CAC identity to the Principle Name (PN) field of a CO or User record in Active Directory (AD), the LDAP server.
10. The certificate realm is configured to use an LDAP realm for authorization. The LDAP user is determined by LDAP search using the following filter: (userPrincipleName=\$(user.name)).

The CO or User is granted access to the Management Center Web Interface if the UPN/CN is found in the LDAP directory. The exchanges with the LDAP server are secured using TLS.

The authentication mechanisms used in the module are listed in Table 7.

⁵ PIV – Personal Identity Verification II

Table 7 Authentication Mechanisms Used by the Module

Role	Authentication type	Authentication strength
Crypto-Officer	Password	<p>The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95⁸), or 1:6,634,204,312,890,625 chance of false acceptance. The Crypto-Officer may connect locally using the serial port or remotely after establishing a TLS or SSH session.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 × 10⁶ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95⁸ possible passwords / ((6 × 10¹⁰ bits per minute) / 64 bits per password)] 1: (95⁸ possible passwords / 937,500,000 passwords per minute) This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.</p>
	Password (“Enabled” Mode)	<p>The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95⁸), or 1:6,634,204,312,890,625 chance of false acceptance. This password is entered by the Crypto-Officer to enter the “enabled” mode; this is entered locally through the serial port or remotely after establishing an SSH session.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 × 10⁶ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95⁸ possible passwords / ((6 × 10¹⁰ bits per minute) / 64 bits per password)] 1: (95⁸ possible passwords / 937,500,000 passwords per minute)</p>

Role	Authentication type	Authentication strength
		This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	Public keys	<p>The module supports using RSA keys for authentication of Crypto-Officers during TLS (when CAC authentication is configured with a local Certificate Realm). 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 1:2¹¹² or 1: 5.19 x 10³³.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 × 10⁶ × 60 = 6 × 10¹⁰ ⇒) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2¹¹² / 6 × 10¹⁰), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2.</p>

Role	Authentication type	Authentication strength
User	Password	<p>The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95⁸), or 1: 6,634,204,312,890,625 chance of false acceptance. The User may connect remotely after establishing a TLS or SSH session.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 × 10⁶ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95⁸ possible passwords / ((6 × 10¹⁰ bits per minute) / 64 bits per password)] 1: (95⁸ possible passwords / 937,500,000 passwords per minute) This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.</p>
	Public keys	<p>The module supports using RSA keys for authentication of Users during TLS (when CAC authentication is configured with a local Certificate Realm). 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 1:2¹¹² or 1: 5.19 × 10³³.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 × 10⁶ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2¹¹² / 6 × 10¹⁰), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2.</p>

2.5 Physical Security

The Management Center Virtual Appliance is a software module, which FIPS defines as a multi-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on the following operational environment and hardware:

- Dell PowerEdge R830 Server appliance
- Intel Xeon E5 processor
- VMware ESXi v6.0 with Linux (RHEL 6.9) as the guest OS

All cryptographic keys and CSPs are under the control of the guest operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module does not provide a general-purpose operating system. The operating system is not modifiable by the operator, and only the modules' signed image can be executed. All software upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade.

NOTE: Only FIPS-validated software may be loaded to maintain the module's validation.

2.7 Cryptographic Key Management

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

Table 8 FIPS-Approved Algorithm Implementations for the MC VA Java Cryptographic Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#5906	AES ⁶	SP 800-38A	CBC, CTR	AES 128, 256 CBC AES 128, 192, 256 CTR	Data Encryption / Decryption
#5906, #3887	KTS ⁷	SP 800-38F	AES (CBC, CTR) and HMAC	AES 128, 256 CBC AES 128, 192, 256 CTR	Key Transport
#4663	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest
#3887	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 256, 384, 512	Message Authentication
#3094	RSA	FIPS 186-4	SHA-256, SHA-384 PKCS1 v1.5	2048, 3072	KeyPair Generation ⁸ Digital Signature Generation, Digital Signature Verification,
#2468	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Deterministic Random Bit Generation
Vendor Affirmed	CKG	SP 800-133			Key Generation
Vendor Affirmed	PBKDFv2	SP800-132	Section 5.4, option 1(a)	Iteration Count: 65536 Salt: 256 bits from DRBG Algorithm: HMAC-SHA-1	Storing device credentials

⁶ Not all modes verified through CAVS certificates are used in the module.

⁷ KTS – Key establishment methodology provides between 128 and 256 bits of encryption strength

⁸ RSA KeyPair Generation was tested; however, it is not used by any service.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
Vendor Affirmed	KAS-SSC	SP 800-56A rev 3	ECC	P-256, P-384, P-521 ⁹	Key Agreement - Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #2135).
#2135	CVL TLS 1.2	SP800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation

⁹ While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

The module performs PBKDFv2 as defined in IETF RFC #2898. The vendor affirms compliance with SP 800-132, using option 1(a) in Section 5.4 to derive the Managed Device Encryption Key (MDEK). The PBKDF2 is used for storage applications only. The length of the random salt used in PBKDFv2 is 256 bits. The iteration count used in PBKDFv2 is 65536. The passphrase length used in the PBKDFv2 is 2048-bits and meets the requirements specified in IG D.6.

Table 9 FIPS-Approved Algorithm Implementations for the MC VA OS Cryptographic Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#5904	AES ¹⁰	SP 800-38A	CBC, CTR	AES 128, 256 CBC AES 128, 192, 256 CTR	Data Encryption / Decryption
#5904, #3885	KTS ¹¹	SP 800-38F	AES (CBC, CTR) and HMAC	AES 128, 256 CBC AES 128, 192, 256 CTR	Key Transport
#5904	AES	SP 800-38E	XTS	256	Data Encryption / Decryption
#4661	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest
#3885	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 256, 384, 512	Message Authentication
#3093	RSA	FIPS 186-4	SHA-256, SHA-384; PKCS1 v1.5	2048, 3072	Digital Signature Generation, Digital Signature Verification
#3093	RSA	FIPS 186-4	PKCS1 v1.5	2048	KeyPair Generation
#2466	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Deterministic Random Bit Generation

¹⁰ Not all modes verified through CAVS certificates are used in the module.

¹¹ KTS – Key establishment methodology provides between 128 and 256 bits of encryption strength

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
Vendor Affirmed	CKG	SP 800-133			Key Generation
Vendor Affirmed	KAS-SSC	SP 800-56A rev 3	FFC	(2048, 256)	Shared Secret Computation
Vendor Affirmed	KAS-SSC	SP 800-56A rev 3	ECC	P-256, P-384, P-521 ¹²	Shared Secret Computation
#2133	CVL TLS 1.0, TLS 1.1, TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation

Table 10 FIPS-Approved Algorithm Implementations for the VA MC SSH Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#2134	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-256, SHA-512	Key Derivation

Table 11 FIPS-Approved Algorithm Implementations for VA UEFI OS Loader Library v4.14

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#4660	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest as part of Integrity Check
#3092	RSA	FIPS 186-4	SHA-256; PKCS1 v1.5	2048	Digital Signature Verification as part of Integrity Check
#3884	HMAC	FIPS 198-1	HMAC-SHA-1	128	Integrity Check

¹² While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

Table 12 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA	Provides between 112 and 150 bits of encryption strength	Key Wrapping
RSA Signature Verification	1536, 4096-bits	Signature Verification
RSA KeyPair Generation RSA Digital Signature Generation,	4096 ¹³ bits	KeyPair Generation Digital Signature Generation,
MD5	No security is provided by this algorithm.	In TLS 1.0/1.1 Protocol
Non-Deterministic Random Number generator (NDRNG) ¹⁴		Seeding for the FIPS-Approved DRBG (SP 800-90 CTR_DRBG)

NOTE: No parts of the TLS and SSH protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

¹³ RSA 4096 – When generating primes for the 4096-bit RSA modulus, the p and q primes shall be of 2048 bits each and the auxiliary primes shall be longer than 170 bits

¹⁴ NDRNG is listed on the certificate

The module supports the CSPs listed below in Table 13.

Table 13 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Data Protection Key (DPK)	AES XTS 256-bit key	Internally generated via FIPS-Approved DRBG (per IG A.9)	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, User password, “Enabled mode password, RSA private key, and Managed Device Encryption Key
Managed Device Encryption Key (MDEK)	AES CBC 256-bit	Internally generated by PBKDFv2	Never exits the module	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting DPK	Encrypting credentials used to remotely manage other appliances
PBKDFv2 Passphrase	2048 bits of data	Internally generated via FIPS-Approved DRBG	Can exist the module in encrypted form via a secure TLS session	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting DPK	Input to the PBKDFv2 function.
Integrity Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure TLS or SSH session	Never exits the module	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image	Verifying the integrity of the system image during upgrade or downgrade
RSA Public Keys	2048-, 3072-, and 4096-bits	Modules’ public key is internally generated via FIPS-Approved DRBG	Output during TLS/SSH ¹⁵ negotiation in plaintext.	Stored in encrypted form on non-volatile memory	Module’s public key is deleted by command	Negotiating TLS or SSH sessions Used for authentication when

¹⁵ SSH session negotiation can only use RSA key pairs of 2048-bits. TLS session negotiation can use RSA key pairs of 2048-bits, 3072-bits and 4096-bits.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
			Output during TLS negotiation for CAC authentication			adding managed devices.
Client RSA Public Key	1024, 1536, 2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext Can be sent to the module as part of an X.509 certificate during CAC authentication	Never exits the module	Other entities' public keys reside on volatile memory	Other entities' public keys are cleared by power cycle	Negotiating TLS or SSH sessions Used for client authentication when certificate-based authentication is configured.
RSA Private Keys	2048-, 3072-, and 4096-bits	Internally generated via FIPS-Approved DRBG Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port	Never exits the module	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting DPK	Negotiating TLS or SSH sessions
DH public key	2048-bits	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
DH private key	224-bits	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
ECDH private key	P-256 key ¹⁶	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
ECDH public key	P-256 key ¹⁷	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
TLS Pre-Master Secret	384-bit key	Input in encrypted form from TLS client	Never	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Master Secret
TLS Master Secret	384-bit key	Generated internally during session negotiation	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Session Key
TLS Session key	AES CBC128-, or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting TLS data
SSH Session Key	AES CBC 128 or 256-bit key, AES CTR 128, 192, or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting SSH data

¹⁶ While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

¹⁷ While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Integrity key	HMAC SHA-1-, 256-, 384-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for TLS sessions
SSH Integrity key	HMAC SHA-1-, 256-, 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for SSH sessions
Crypto Officer Password User Password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Externally generated. Enters the module in encrypted form via a secure TLS or SSH session. Enters the module in plaintext via a directly attached cable to the serial port	Exits in encrypted form via a secure TLS session for external authentication	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypted DPK	Locally authenticating a CO or User for Management Console or CLI
“Enabled” mode password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Enters the module in encrypted form via a secure SSH session Enters the module in plaintext via a directly attached cable to the serial port	Exits in encrypted form via a secure TLS session for external authentication	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting DPK	Used by the CO to enter the “privileged” or “enabled” mode when using the CLI
SP 800-90A CTR_DRBG Seed ¹⁸	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Seeding material for the SP800-90A CTR_DRBG

¹⁸ The CTR DRBG Seed requires a 384-bit number and uses 256 bits of entropy with the derivation function to create the 384-bit value. The 256-bits of CTR DRBG Entropy is obtained from an entropy-generating NDRNG inside the module’s cryptographic boundary

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG Entropy ¹⁹	256-bit random number with derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Entropy material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG
SP 800-90A CTR_DRBG V value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG

NOTE: The Approved DRBG is seeded with a minimum of 256- bits of strength (384-bits via the derivation function) from an entropy-generating NDRNG inside the module's cryptographic boundary.

¹⁹ The Entropy required by the FIPS-Approved SP 800-90A CTR_DRBG (with AES-256) is supplied by the NDRNG. The NDRNG provides a full 256 bits of entropy per IG 7.14 Scenario 1B.

2.8 Self-Tests

If the module fails the POST Integrity Test, the following error is printed to the CLI (when being accessed via the serial port):

```
Boot system is not valid. Image data is corrupt.
```

If a self-test fails in the MC VA OS Cryptographic Library, the following error is printed to the CLI (when being accessed via the serial port):

```
Openssl FIPS POST Test failed. Rebooting...
```

If a self-test fails in the MC VA Java Cryptographic Library, the following error is printed to the CLI (when being accessed via the serial port):

```
FIPS-out FIPS operational failure detected: "module in error status: <self-test specific details>".
```

```
The system is going down for a reboot NOW!
```

When either of these errors occurs, the modules halt operation and provide no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the modules. The status output provided below is shown only over the CLI (when being accessed via the serial port).

The sections below describe the self-tests performed by the module.

2.8.1 Power-Up Self-Tests

The module performs the following self-tests using the VA UEFI OS Loader Library:

- Known Answer Tests
 - SHA KAT using SHA-1 and SHA-256;
 - HMAC KAT using SHA-1; and
 - RSA Sign/Verify KAT with SHA-256.
- Software integrity check using HMAC-SHA-1.

The module then performs the following self-tests using the MC VA OS Cryptographic Library at power-up:

- Known Answer Tests
 - AES KAT for encryption and decryption
 - AES XTS KAT for encryption and decryption
 - SHA KAT using SHA-1, SHA-256, SHA-384, SHA-512
 - HMAC KAT using SHA-1, SHA-256, SHA-384, SHA-512
 - RSA Sign/Verify KAT with SHA-256
 - SP800-90A DRBG KAT
 - DH "Primitive Z" KAT*
 - ECDH "Primitive Z" KAT*

The module then performs the following self-tests using the MC VA Java Cryptographic Library at power-up:

- Known Answer Tests
 - AES KAT for encryption and decryption
 - SHA KAT using SHA-1, SHA-256, SHA-384
 - HMAC KAT using SHA-1, SHA-256, SHA-384
 - RSA Sign/Verify KAT with SHA-256
 - SP800-90A DRBG KAT

- ECDH “Primitive Z” KAT*

* These self-tests are performed although not required, since SP800-56A rev 3 is vendor affirmed.

No data output occurs via the data output interface until all power-up self tests have completed.

2.8.2 Conditional Self-Tests

The module performs the conditional self-tests in its MC VA Java Cryptographic Library.

- Continuous RNG test (CRNGT) for the SP800-90A DRBG
- Continuous RNG test (CRNGT) for the Non-Deterministic Random Number Generator (NDRNG)

The module performs the conditional self-tests in its MC OS VA Cryptographic Library.

- RSA pairwise consistency check upon generation of an RSA keypair
- Continuous RNG test (CRNGT) for the SP800-90A DRBG
- Continuous RNG test (CRNGT) for the Non-Deterministic Random Number Generator (NDRNG)
- Software Load Test using RSA Signature Verification

2.8.3 Critical Function Tests

The module performs the following critical function tests in the UEFI OS Loader:

- RSA signature Verification

The Management Center Virtual Appliance performs the following critical function tests on both the MC VA OS and MC VA Java Cryptographic Libraries:

- CTR DRBG Instantiate Critical Function Test
- CTR DRBG Reseed Critical Function Test
- CTR DRBG Generate Critical Function Test
- CTR DRBG Uninstantiate Critical Function Test

Both the MC VA OS and MC VA Java Cryptographic Libraries run health checks on their respective CTR DRBGs every 2^{24} requests, which is less than the CTR DRBG reseed interval of 2^{48} per NIST SP800-90A.

Additionally, per the IG A.9 requirements, the MC OS Cryptographic Library performs the following critical functions test for AES XTS to ensure that the two keys used in this operation are not identical ($Key_1 \neq Key_2$):

- AES XTS Duplicate Key Test

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The Management Center Virtual Appliance can be configured into an explicit FIPS mode of operation as per the instructions provided below in Section 3.1. However, the Management Center Virtual Appliance supports a non-compliant state, the initialization of which requires an explicit separate configuration. When the Management Center Virtual Appliance is operating in non-compliant state, the services have access to non-Approved and non-Allowed algorithms. The logical boundary of the module is defined such that all functionality available in non-compliant state is scoped out from the module boundary. Thus, when the module is operating in FIPS Approved mode of operation, it can access only FIPS Approved or Allowed algorithms as access to non-Approved and non-Allowed algorithms are explicitly inhibited by design of the module.


The Management Center Virtual Appliance Management Center Virtual Appliance meets FIPS-140-2 Level 1 requirements. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

Caveat: This guide assumes that a virtual environment is already setup and ready for accepting a new virtual appliance installation.

3.1 Initialization

Physical access to the module's host hardware shall be limited to the Crypto-Officer, and the CO shall be responsible for putting the module into the Approved mode.

Once the VM has been deployed, the CO must place the module in the Approved mode using the Console Tab which provides access to the virtual serial connection.

1. Download the Virtual Appliance Package (VAP), which consists of the deployment .OVF file, 2 virtual machine disk images (VMDKs), and a .PDF guide.
2. Using the VMware client, deploy the OVF template included in the VAP.
 - a. Provide a name for the VA, click **Next**
 - b. The location (host or cluster), click **Next**,
 - c. The location for the virtual machine file storage, Click **Next**
 - d. Specify thin or thick provision based on the resources available, click **Next**.
 - e. Select a network to map to and click **Next**.
 - f. Click **Finish**
3. Power on the virtual appliance so that this icon is seen: 
4. In the VMware client, right click the VA and select **Open Console**.
5. Enter the serial number of the appliance. The console will prompt you to hit Enter three times.
6. Press **Enter** three times.

```
Welcome to the Symantec Virtual Series Appliance Serial Console
Version: Blue Coat Management Center 2.1.1.1, Release id: 226719 64-bit
```

```
----- MENU -----
1) Command Line Interface
2) Setup Console
-----
Enter option:
```

7. Enter **1** to access the Command Line Interface.

8. Type **enable** and press **Enter**.
9. Enter the following command: **fips-mode enable**.

When prompted for confirmation, select **Y** to confirm.

- **NOTE 1:** The fips-mode enable command causes the device to power cycle, zeroing the appliance and returning the configuration values set in steps 1 and 2 to their factory state.

10. After the system has finished rebooting, press **Enter** three times.

11. Enter the properties for the following:

- a. IP address
- b. IP subnet mask
- c. IP gateway
- d. DNS server parameters

12. The module will prompt for the console account credentials:

DIRECTIONS:

The console username, password and enable password are special administrative credentials which can be used to log into the command line interface or web management interface.

Enter console password:

Verify console password:

Enter enable password:

Verify enable password:

Upon completion of these initialization steps, the module is considered to be operating in its Approved mode of operation. There are no additional non-Approved services while operating in the Approved mode.

3.1.1 Management

The Crypto-Officer is able to monitor and configure the module via the Management Center web interface (HTTPS over TLS) and the CLI (serial port or SSH).

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, customers should consult Symantec's Product Documentation portal and the administrative guidance documents to resolve the issues. If the problems cannot be resolved through these resources, Symantec customer support should be contacted.

The CO password and "enabled" mode password must be at least 8 characters in length.

3.1.2 Zeroization

The CO can return the module to its uninitialized factory state by entering the "enabled" mode on the CLI, followed by the "fips-mode disable" command. This command will automatically reboot the module and zeroize all keys. Zeroization includes all temporary/ephemeral session keys, and also the persistently stored RSA private key, Crypto-Officer password, User password, "Enabled" mode password, and the Managed Device Encryption Key. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

3.2 User Guidance

The User is only able to access the module remotely via SSH (CLI) or HTTPS (Management Console). The User must change his or her password at the initial login. The User must be diligent to pick strong passwords (alphanumeric with minimum 8 characters) that will not be easily guessed and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as TLS or SSH session keys. The User should report to the Crypto-Officer if any irregular activity is noticed.

4. Acronyms

This section describes the acronyms used throughout this document.

Table 14 Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
BMC	Baseboard Management Controller
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
DH	Diffie Hellman
DHE	Diffie Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie Hellman
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NDRNG	Non-deterministic random number generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
USB	Universal Serial Bus