# Symantec & CA Technologies, a division of Broadcom Management Center

Models: MC-S400-20
MC-S400 Hardware Versions: 090-03341, 090-03342, 090-03343
FIPS Security Kit Version: HW-KIT-FIPS-400
Firmware Version: 2.1

## FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 2
Document Version: 0.8

# COPYRIGHT NOTICE



# CONTACT INFORMATION

**Symantec & CA Technologies, a division of Broadcom**
1320 Ridder Park Dr,
San Jose, CA 95131
www.broadcom.com

# Table of Contents



# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Purpose

This is a *Non-Proprietary Cryptographic Module Security Policy* for the Management Center S400 appliances (Firmware Version 2.1; Models: MC-S400-20) from Symantec & CA Technologies, a division of Broadcom. This *Non-Proprietary Security Policy* describes how the MC S400 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 2 validation of the module. The Management Center S400 is referred to in this document as MC, S400, 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 500 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 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 appliances.

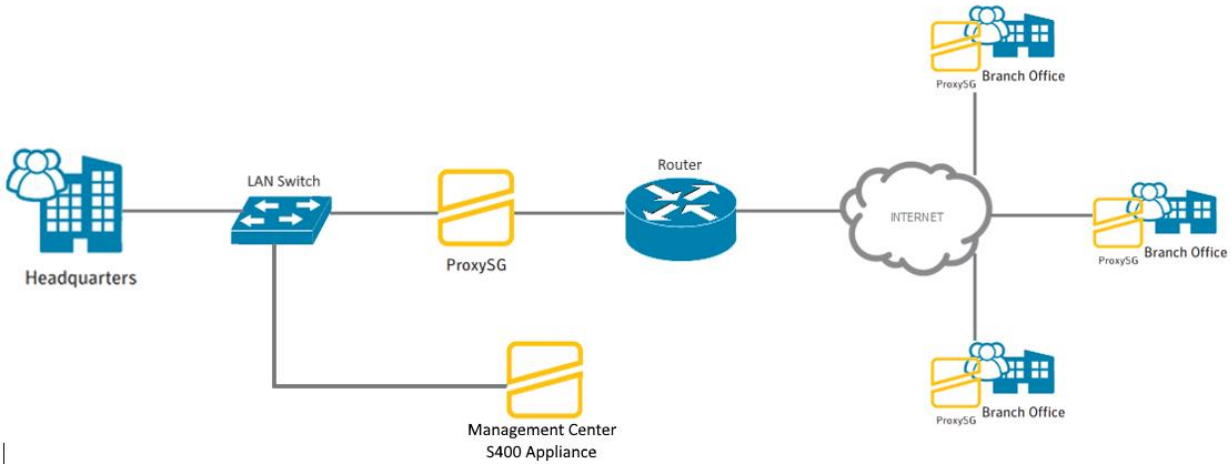


**Figure 1 Typical Deployment of a Management Center appliance (MC-S400)**

Management Center 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 | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 2 |
| 8 | Electromagnetic Interference/Electromagnetic Compatibility | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 3 |
| 11 | Mitigation of Other Attacks | N/A |

## 2.2 Module Specification

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

**Table 2 Management Center Appliance Configurations**

| Appliance Type | Hardware Version | Revision | Model/SKU | SKU / Short Description |
|---|---|---|---|---|
| Management Center S400-20 | 090-03341 | 231-03288 Revision X.0 (Blue Coat branded) | MC-S400-20-100 | 100 Managed Assets |
| | | 231-03288 Revision Y.0 (Symantec branded) | | |
| | 090-03342 | 231-03288 Revision X.0 (Blue Coat branded) | MC-S400-20-250 | 250 Managed Assets |
| | | 231-03288 Revision Y.0 (Symantec branded) | | |
| | 090-03343 | 231-03288 Revision X.0 (Blue Coat branded) | MC-S400-20-500 | 500 Managed Assets |
| | | 231-03288 Revision Y.0 (Symantec branded) | | |

Additionally, the Blue Coat branded appliances will correspond with the 231-03288 Revision X.0 and the Symantec branded appliances correspond to the 231-03288 Revision Y.0.

The hardware version numbers in Table 2 represent the different licensing editions supported. All editions run on the exact same hardware and firmware and are exactly the same from a cryptographic functionality and boundary perspective. The Crypto Officer and User services of the module are identical for all editions.

The MC S400 offers an affordable rack-mountable appliance solution for small enterprises and branch offices that have direct access to the Internet.

The front panel of the MC S400 appliance has 1 Liquid Crystal Display (LCD), two Light Emitting Diodes (LEDs), 6 control buttons, and 1 USB port. (NOTE: the front panel control buttons and the USB port are disabled when configured for Approved mode of operation). ). Please see Figure 2 for the picture of the front of the appliance. Connection ports are at the rear, as shown in Figure 4.

For the FIPS 140-2 validation, the module was tested on the following appliance configurations:
MC S400-20

Symantec Management Center is a module with a Multi-chip Standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the MC S400 is defined by the appliance chassis, which surrounds all the hardware and firmware. The module firmware, version 2.1, contains the following cryptographic libraries:

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

# 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

The front panel of the MC S400 (as shown below in Figure 2) has an Liquid Crystal Display (LCD), interface, 2 Light Emitting Diodes (LEDs), and six control buttons. The control buttons on the front panel are disabled once the module is configured for its Approved mode of operation.

The type and quantity of all ports present in the front panel of the MC S400 are given in Table 3.


**Figure 2 Connection Ports at the Front of the Management Center S400 (Blue Coat logo)**


**Figure 3 Connection Ports at the Front of the Management Center S400 (Symantec logo)**

The type and quantity of all ports present in the front panel of the Management Center S400 are given in Table 3.

**Table 3 FIPS 140-2 Logical Interface Mappings for the front of the Management Center**

| Physical port / interface | Quantity | FIPS 140-2 interface |
|---|---|---|
| LEDs | 2 | Status Output |
| LCD | 1 | Status Output |
| Control Buttons | 6 | N/A (buttons are disabled) |
| USB 2.0 Port | 1 | N/A (port is disabled) |

The status indications provided by the LEDs on the Management Center are described in the graphic above. For the FIPS-validated configuration, the front buttons are all disabled.

The rear of the Management Center is shown in Figure 4.

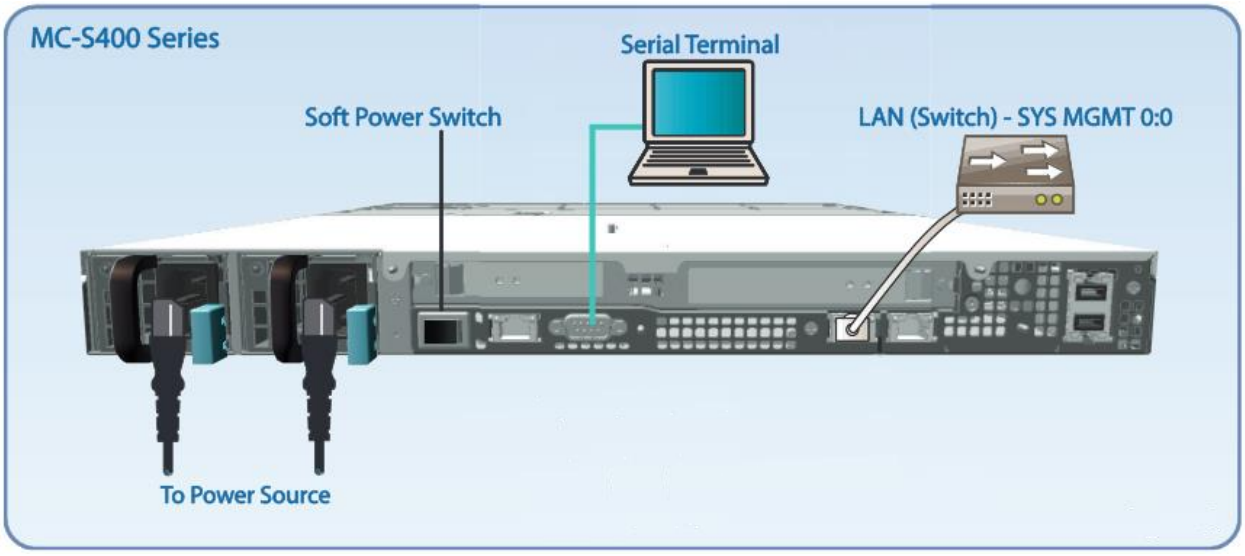


**Figure 4 Connection Ports at the Rear of the Management Center S400**

The rear side of the Management Center (shown in Figure 4) contains all the connecting ports. Those ports are:

- Two AC power connectors.
- A serial port to connect to a Personal Computer (PC) for management.
- One 10/100/1000 Base T Ethernet adapter port for management.

In the FIPS-validated configuration, the additional RJ-45 Ethernet ports are disabled. Only the port indicated in the above diagram is operational. The type and quantity of all ports present in rear panel of the Management Center are given in Table 4.

**Table 4 FIPS 140-2 Logical Interface Mappings for the rear of the Management Center**

| Physical port / interface | Quantity | FIPS 140-2 interface |
|---|---|---|
| Ethernet ports | 3 | N/A (ports are disabled) |

| Physical port / interface | Quantity | FIPS 140-2 interface |
|---|---|---|
| System management port[1] | 1 | Data input<br>Data output<br>Control input<br>Status output |
| BMC[2] management port | 1 | N/A (port is disabled) |
| Serial ports | 1 | Control input<br>Status output |
| Ethernet interface – speed LEDs | 1 | Status output |
| Ethernet interface – activity LEDs | 1 | Status output |
| AC power | 2 | Power input |
| Soft power switch | 1 | Control input |

The status indications provided by the LEDs on the rear of the Management Center are described in Table 5.

**Table 5 Rear Panel LED Status Indications for the Management Center**

| LED | Color | Definition |
|---|---|---|
| Ethernet Interface – Activity LEDs | OFF | No link is present. |
| | GREEN | Link is present. |
| | FLASHING GREEN | Link activity. |
| Ethernet Interface – Activity LEDs | OFF | 10 Mbps speed connection is present. |
| | GREEN | 100 Mbps speed connection is present. |
| | AMBER | 1000 Mbps speed connection is present. |

## 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 9. The modules offer the following management interfaces:

- CLI[3] – 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 SSH[4]. 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 TLS[5]. 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

[1] The port can be used to access all functionality provided by the module. However, it is the preferred port for management.
[2] BMC – Base Management Controller
[3] CLI – Command Line Interface
[4] SSH – Secure Shell protocol
[5] TLS – Transport Layer Security

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 6.

The CO and User details are found below in Table 6.

**Table 6 FIPS and Management Center Roles**

| FIPS Roles | Management Center Roles and Privileges |
|---|---|
| CO | • 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.<br>• 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.<br>• 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.<br>• 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 | • 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.<br>• 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 User are described below in Table 7 and Table 8 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 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 7 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 3.2.1 in this *Security Policy*. | CO Password: W<br>"Enabled" mode password: W |
| Enter the "enabled" mode (CLI) | Manage the module in the "enabled" mode of operation, granting access to higher privileged commands | "Enabled" mode password: RX |
| * 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<br>SSH Integrity Key: W<br>TLS Session Key: W<br>TLS Integrity Key: W<br>TLS Pre-Master Secret: W<br>TLS Master Secret: W<br>DH private key: W<br>ECDH private key: W<br>DRBG CSPs: W<br>DPK: W |
| ** Firmware Load | Loads new external firmware 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<br>RSA private key: RX<br>DH public key: WRX<br>DH private key: WRX<br>ECDH public key: WRX<br>ECDH private key: WRX<br>SSH Session Key: WRX<br>SSH Integrity Key: WRX<br>DRBG CSPs: WRX<br>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<br>RSA private key: RX<br>DH public key: WRX<br>DH private key: WRX<br>ECDH public key: WRX<br>ECDH private key: WRX<br>TLS Session Key: WRX<br>TLS Integrity Key: WRX<br>TLS Pre-Master Secret: WRX<br>TLS Master Secret: WRX<br>DRBG CSPs: WRX<br>CO Password: R |
| ** Create, edit, and delete User Groups | Create, edit and delete operator groups; define common sets of operator permissions. | None |

| Service | Description | CSP and access required |
|---|---|---|
| ** 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<br>User Password: W<br>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 containing hundreds of hierarchies, device groups, and devices. | None |
| 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<br>ECDH public key: WRX<br>ECDH private key: WRX<br>TLS Session Key: WRX<br>TLS Integrity Key: WRX<br>TLS Pre-Master Secret: WRX<br>TLS Master Secret: WRX<br>DRBG CSPs: WRX<br>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<br>SSH Integrity Key: W<br>TLS Session Key: W<br>TLS Integrity Key: W<br>TLS Pre-Master Secret: W<br>TLS Master Secret: W<br>DH private key: W<br>ECDH private key: W<br>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 |

| Service | Description | CSP and access required |
|---|---|---|
| * Perform self-test (CLI) | Perform self-test on demand by rebooting the machine | DH public key: W<br>DH private key: W<br>ECDH public key: W<br>ECDH private key: W<br>SSH Session Key: W<br>SSH Integrity Key: W<br>TLS Session Key: W<br>TLS Integrity Key: W<br>TLS Pre-Master Secret: W<br>TLS Master Secret: W<br>DRBG CSPs: W |
| * Reboot the module (CLI) | Reboot the module. | DH public key: W<br>DH private key: W<br>ECDH public key: W<br>ECDH private key: W<br>SSH Session Key: W<br>SSH Integrity Key: W<br>TLS Session Key: W<br>TLS Integrity Key: W<br>TLS Pre-Master Secret: W<br>TLS Master Secret: W<br>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 v2.1.1.1*.

**Table 8 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<br>RSA private key: RX<br>DH public key: RX<br>DH private key: RX<br>ECDH public key: RX<br>ECDH private key: RX<br>TLS Session Key: WRX<br>TLS Integrity Key: WRX<br>TLS Pre-Master Secret: WRX<br>TLS Master Secret: WRX<br>DRBG CSPs: WRX<br>User Password: R |

| Service | Description | CSP and access required |
|---|---|---|
| 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 PIV[6] 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 browse r 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

[6] PIV – Personal Identity Verification II

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 9.

**Table 9 Authentication Mechanisms Used by Management Center**

| Role | Authentication type | Authentication strength |
|---|---|---|
| Crypto-Officer | Password | 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:($95^8$), 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.<br><br>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 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:<br>1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)]<br>1: (95^8 possible passwords / 937,500,000 passwords per minute)<br>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. |
| | Password (“Enabled” Mode) | 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: ($95^8$), 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.<br><br>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 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:<br>1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)]<br>1: (95^8 possible passwords / 937,500,000 passwords per minute) |

| 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 | 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 $1:2^{112}$ or 1: 5.19 x $10^{33}$.<br><br>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×$10^6$ × 60 = 6 × 10^10 =) 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: (2^112 / 6×10^10), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2. |
| User | Password | 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:($95^8$), or 1: 6,634,204,312,890,625 chance of false acceptance. The User may connect remotely after establishing a TLS or SSH session.<br><br>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 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:<br>1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)]<br>1: (95^8 possible passwords / 937,500,000 passwords per minute)<br>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 | 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 $1:2^{112}$ or 1: 5.19 x $10^{33}$.<br><br>The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×$10^6$ × 60 = 6 × |

| Role | Authentication type | Authentication strength |
|---|---|---|
| | | 10^10 =) 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: (2^112 / 6×10^10), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2. |

## 2.5 Physical Security

The Management Center is a Multi-Chip Standalone cryptographic module. It is enclosed in a hard, opaque metal case that completely encloses all its internal components. There are only a limited set of vent holes provided in the case, and these holes obscure the view of the internal components of the module. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the module. The Crypto-Officer is responsible for the placement of tamper-evident labels and baffles, and guidance and instructions can be found in section 3.1. The labels and baffles are part of the FIPS Security Kit for the S400 models (Part Number: 085-02891; HW-KIT-FIPS-400).

All the module's components are production grade. The Management Center was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

## 2.6 Non-Modifiable Operational Environment

The operational environment requirements do not apply to the Management Center. 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 firmware upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade.

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

## 2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 10 below.

**Table 10 FIPS-Approved Algorithm Implementations for the MC Java Cryptographic Library v1.0**

| CAVP Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| #5908 | AES[7] | SP 800-38A | CBC, CTR | AES 128, 256 CBC<br>AES 128, 192, 256 CTR | Data Encryption / Decryption |
| #5908, #3890 | KTS[8] | SP 800-38F | AES (CBC, CTR) and HMAC | AES 128, 256 CBC<br>AES 128, 192, 256 CTR | Key Transport |
| #4666 | SHS | FIPS 180-4 | SHA-1, SHA-256, SHA-384, SHA-512 | | Message Digest |
| #3890 | HMAC | FIPS 198-1 | HMAC-SHA-1,<br>HMAC-SHA-256,<br>HMAC-SHA-384,<br>HMAC-SHA-512 | 128,<br>256,<br>384,<br>512 | Message Authentication |
| #3097 | RSA | FIPS 186-4 | SHA-256, SHA-384<br>PKCS1 v1.5 | 2048, 3072 | KeyPair Generation[9]<br>Digital Signature Generation,<br>Digital Signature Verification, |
| #2470 | CTR-DRBG | SP 800-90A | CTR-based | AES-256 | Deterministic Random Bit Generation |
| Vendor Affirmed | CKG | SP 800-133 | | | Key Generation |

[7] Not all modes verified through CAVS certificates are used in the module.

[8] KTS – Key establishment methodology provides between 128 and 256 bits of encryption strength

[9] RSA Key Pair 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 | PBKDFv2 | SP800-132 | Section 5.4, option 1(a) | Iteration Count: 65536<br>Salt: 256 bits from DRBG<br>Algorithm: HMAC-SHA-1 | Storing device credentials |
| N/A | KAS-SSC | SP 800-56A rev 3 | ECC | P-256, P-384, P-521[10] | Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #2139). |
| #2139 | CVL TLS 1.2 | SP800-135rev1 | TLS 1.2 SHA Sizes = SHA-256, SHA384 | | Key Derivation |

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 11 FIPS-Approved Algorithm Implementations for the MC OS Cryptographic Library v1.0**

| CAVP Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| #5907 | AES[11] | SP 800-38A | CBC, CTR | AES 128, 256 CBC<br>AES 128, 192, 256 CTR | Data Encryption / Decryption |
| #5907, #3889 | KTS[12] | SP 800-38F | AES (CBC, CTR) and HMAC | AES 128, 256 CBC<br>AES 128, 192, 256 CTR | Key Transport |
| #5907 | AES | SP 800-38E | XTS | 256 | Data Encryption / Decryption |

[10] 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.

[11] Not all modes verified through CAVS certificates are used in the module.

[12] 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 |
|---|---|---|---|---|---|
| #4665 | SHS | FIPS 180-4 | SHA-1, SHA-256, SHA-384, SHA-512 | | Message Digest |
| #3889 | HMAC | FIPS 198-1 | HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 | 128, 256, 384, 512 | Message Authentication |
| #3096 | RSA | FIPS 186-4 | SHA-256, SHA-384 PKCS1 v1.5 | 2048, 3072 | Digital Signature Generation, Digital Signature Verification |
| #3096 | RSA | FIPS 186-4 | PKCS1 v1.5 | 2048 | KeyPair Generation |
| #2469 | CTR-DRBG | SP 800-90A | CTR-based | AES-256 | Deterministic Random Bit Generation |
| Vendor Affirmed | CKG | SP 800-133 | | | Key Generation |
| Vendor Affirmed | KAS-SSC | SP 800-56A rev 3 | FFC | (2048, 256) | Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #2137 and SSH KDF CVL Cert. #2138). |

| 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[13] | Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #2137 and SSH KDF CVL Cert. #2138). |
| #2137 | CVL<br>TLS 1.0, TLS 1.1,<br>TLS 1.2 | SP 800-135rev1 | TLS 1.2 SHA Sizes = SHA-256, SHA384 | | Key Derivation |

**Table 12 FIPS-Approved Algorithm Implementations for the MC SSH Library v1.0**

| CAVP Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| #2138 | CVL<br>SSH | SP 800-135rev1 | AES-128 CBC, AES-256 CBC | SHA-1[14], SHA-256, SHA-512 | Key Derivation |

**Table 13 FIPS-Approved Algorithm Implementations for UEFI OS Loader Library v4.14**

| CAVP Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| #4664 | SHS | FIPS 180-4 | SHA-1, SHA-256 | | Message Digest as part of Integrity Check |
| #3095 | RSA | FIPS 186-4 | SHA-256;<br>PKCS1 v1.5 | 2048 | Digital Signature Verification as part of Integrity Check |

[13] 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.

[14] SSH with HMAC-SHA-1 – While this was CAVP tested, it is not used by any service.

| CAVP Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| #3888 | HMAC | FIPS 198-1 | HMAC-SHA-1 | 128 | Integrity Check |

**Table 14 FIPS-Allowed Algorithms**

| Algorithm | Caveat | Use |
|---|---|---|
| RSA | Key wrapping; key establishment methodology provides 112 or 150 bits of encryption strength | Key Wrapping |
| RSA KeyPair Generation<br>RSA Digital Signature Generation, | 4096[15] bits | KeyPair Generation<br>Digital Signature Generation, |
| RSA Signature Verification | 1536, 4096-bits | Signature Verification |
| MD5 | No security is provided by this algorithm. | In TLS 1.0/1.1 Protocol |
| Non-Deterministic Random Number generator (NDRNG)[16] | | Seeding for the FIPS-Approved DRBG (SP 800-90 CTR_DRBG) |

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

The module supports the CSPs listed below in Table 15.

[15] 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
[16] NDRNG is listed on the certificate

**Table 15 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<br><br>Modules' public key can be imported from a back-up configuration | Output during TLS/SSH[17] negotiation in plaintext.<br><br>Output during TLS negotiation for CAC authentication | Stored in encrypted form on non-volatile memory | Module's public key is deleted by command | Negotiating TLS or SSH sessions<br><br>Used for authentication when adding managed devices. |

[17] 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 |
|---|---|---|---|---|---|---|
| Client RSA Public Key | 1024, 1536, 2048, 3072, and 4096-bits | Other entities' public keys are sent to the module in plaintext<br><br>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<br><br>Used for client authentication when certificate-based authentication is configured. |
| RSA Private Keys | 2048-, 3072-, and 4096-bits | Internally generated via FIPS-Approved DRBG<br><br>Imported in encrypted form via a secure TLS or SSH session<br><br>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<br><br>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<br><br>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<br><br>Removing power | Negotiating TLS or SSH sessions |

| Key | Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|---|---|---|---|---|---|---|
| ECDH private key | P-256 key[18] | Internally generated via FIPS-Approved DRBG | Never exits the module | Stored in plaintext on volatile memory | Rebooting the modules<br><br>Removing power | Negotiating TLS or SSH sessions |
| ECDH public key | P-256 key[19] | Module's public key is internally generated via FIPS-Approved DRBG<br><br>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<br><br>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<br><br>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<br><br>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<br><br>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 | Encrypting SSH data |

[18] 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.

[19] 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-bit, 384-bit key | Internally generated | Never exits the module | Resides in volatile memory in plaintext | Rebooting the modules<br><br>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 | Data authentication for SSH sessions |
| Crypto Officer Password<br><br>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.<br><br>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<br><br>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[20] | 384-bit random number | Internally generated | Never exits the module | Plaintext in volatile memory | Rebooting the modules<br><br>Removing power | Seeding material for the SP800-90A CTR_DRBG |

[20] 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[21] | 256-bit random number with derivation function | Internally generated | Never exits the module | Plaintext in volatile memory | Rebooting the modules<br><br>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<br><br>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<br><br>Removing power | Used for the SP 800-90A CTR_DRBG |

**NOTE:** The Approved DRBG is seeded with a minimum of 384-bits from an entropy-generating NDRNG inside the module's cryptographic boundary.

[21] The CTR DRBG 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 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 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 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.
- Firmware integrity check using HMAC-SHA-1.

The module then performs the following self-tests using the MC 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 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*

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

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

### 2.8.2 Conditional Self-Tests

The module performs the conditional self-tests in its MC 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 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)
- Firmware 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 performs the following critical function tests on both the MC OS and MC 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 OS and MC 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 ≠ 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 Level 2 requirements for this validation.

# 3 Secure Operation

Management Center can be configured into an explicit FIPS mode of operation as per the instructions provided in Section 3.2. However, Management Center supports a non-compliant state, the initialization of which requires an explicit separate configuration. When Management Center 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 meets Level 2 requirements. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

## 3.1 Initial Setup the MC S400 Appliance

Before powering-up the module, the CO must ensure that the required tamper-evident labels (included in the FIPS security kit) are correctly applied to the enclosure. The FIPS security kit (Part Number: HW-KIT-FIPS-400) for the modules consists of the following items as shown below in Figure 5.

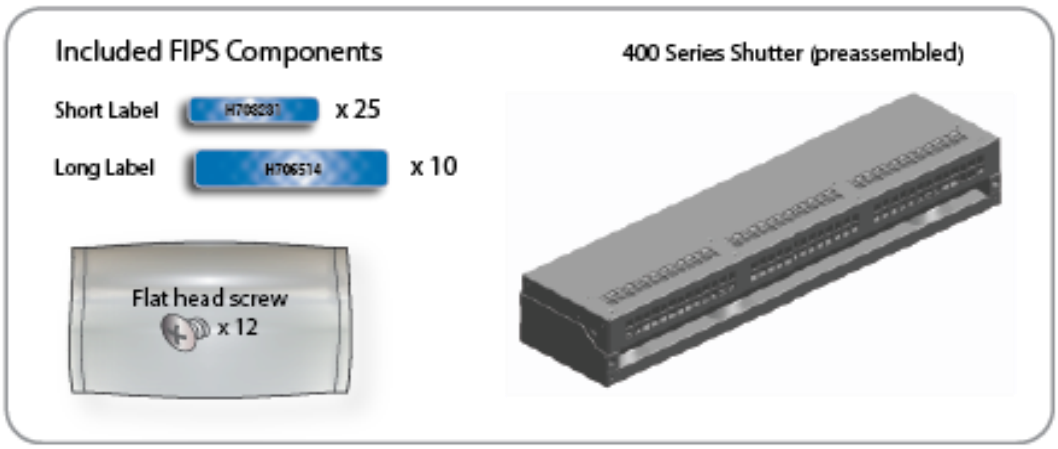


**Figure 5 MC S400 FIPS Security Kit Contents**

Note: Included in the S400 FIPS Kit, there are (25) ‘Short Labels’ and (10) ‘Long labels’; however, only (5) short labels and (2) long labels are required for FIPS compliance. Additional labels are provided for reapplication purposes.

### 3.1.1 MC S400 Label and Baffle Installation Instructions

The Crypto-Officer is responsible for installing the baffle (security panel) and applying the tamper evident labels at the client’s deployment site to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto-Officer is responsible for securing and having control at all times of any unused labels. The Crypto-Officer is responsible for the direct control and observation of any changes to the module such as reconfigurations where the tamper-evident labels or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Crypto-Officers must adhere to the following when applying the tamper-evident labels:

- The minimum temperature of the environment must be 35-degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is -5-degrees to 158-degrees Fahrenheit.
- Do not touch the adhesive side of the label. This disrupts the integrity of the adhesive. If a label is removed from a surface, the image is destroyed and the label shows tamper-evident text as evidence. If you accidently touch the adhesive side, discard that label and apply another one.

Label application tips:

- Apply skin moisturizer on your fingers before handling.
- Use a rubber fingertip to partially remove the label from its backing.
- After applying the labels, allow at least 24 hours for the label adhesive to cure.

### 3.1.1.1 MC S400 Shutter Installation

The two piece rear shutter (S400 Series Shutter as shown in Figure 6) is designed to prevent unauthorized access to key system components by shielding the rear ventilation outlets, option cards, interfaces, and the soft power switch.

1. Remove the top shutter from the bottom shutter by removing two (2) screws and pulling directly rearward. Set the top shutter aside in a safe location.

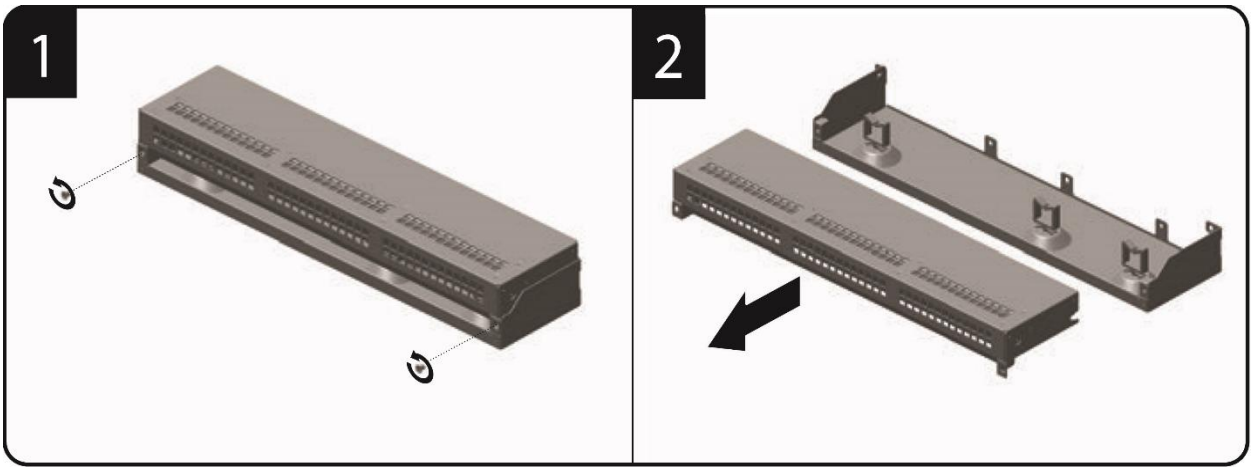


**Figure 6 MC S400 Shutter Disassembly**

2. Align the bottom shutter mounting points against the screw locations and the alignment pins on the chassis and secure with three (3) flat-head screws as shown in Figure 7. Be aware the FIPS kit includes (7) additional screws, in case some are misplaced or lost during installation.

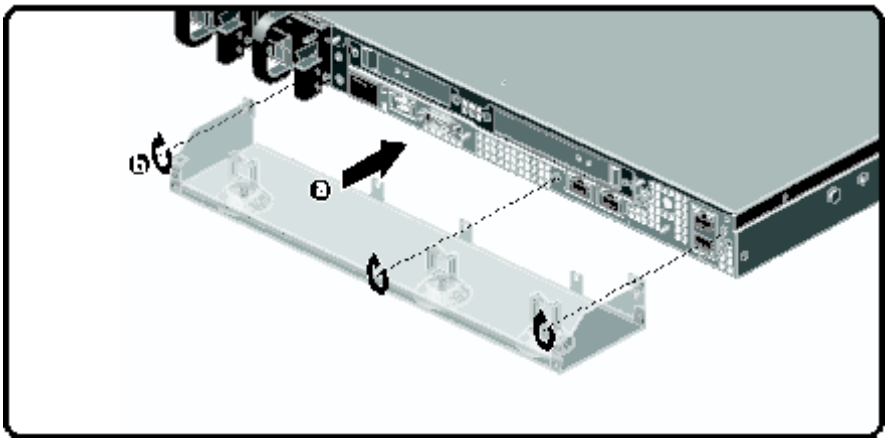

**Figure 7 MC S400 Lower Shutter Installation**

3. Rack mount the appliance.

4. Reinstall the appliance network and other interconnect cables to their respective locations

   **Note**: All network and interconnect cables must installed at this time to prevent reopening of the shutters and subsequent reapplication of the security labels.

5. Route the network cables through the cable management anchors to prevent cables from obstructing airflow.

6. Install the top shutter by aligning the notches with the raised pins on the appliance and secure with two (2) flat-head screws as shown in Figure 8. Be aware the FIPS kit includes (7) additional screws, in case some are misplaced or lost during installation.

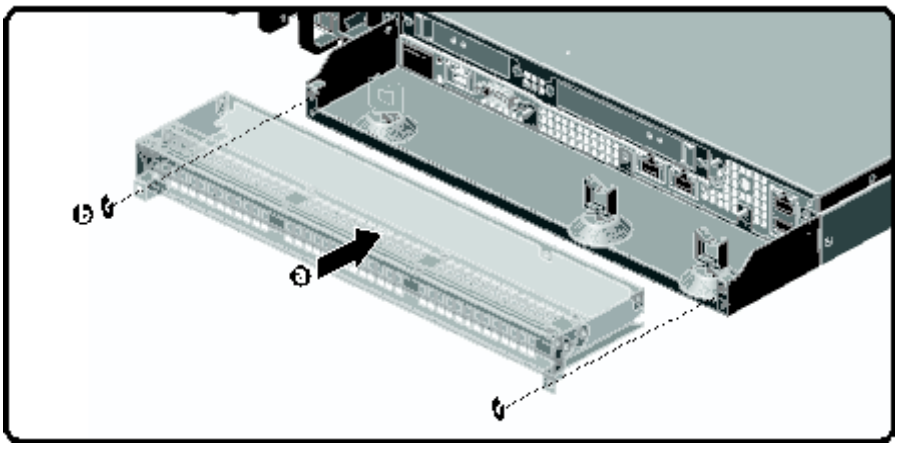

**Figure 8 MC S400 Upper Shutter Installation**

### 3.1.1.2 MC S400 Label Application

The FIPS compliant labels are applied over key areas of the chassis to provide tamper-evident security. If the labels are removed after being affixed to a surface, the image self-destructs and leaves a pattern of VOID markings on the label. The image below illustrates the tamper-evident features of the label. Figure 9 below illustrates the tamper-evident features of the label.


**Figure 9 MC S400 Labels Showing Tamper Evidence**

Use alcohol swabs to clean the label location surface using Isopropyl Alcohol (99%); this ensures complete adhesion. Verify that all the surfaces are dry before applying the labels.

1. Set the appliance on a flat, slip-proof work space and make sure you have access to all sides of the appliance.
2. Apply two (2) short labels (short labels 1 and 2) over the exposed shutter screw heads. These labels extend slightly over the left and right edges of the shutter when properly applied.

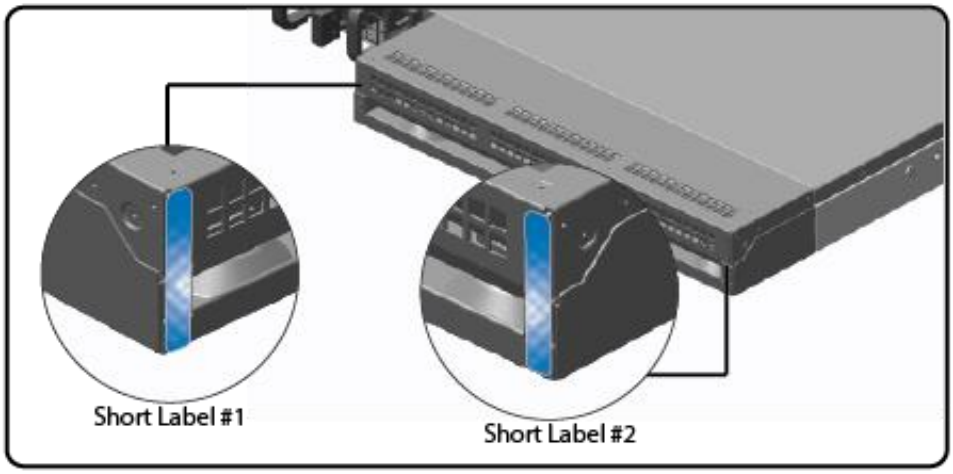


**Figure 10 MC S400 Rear Edge Label Installation**

3. Apply one (1) long label through each power supply unit (long labels 1 and 2) and/or dummy cover in a U-shape, making sure to route the label through the handle and to apply the ends of the label on the chassis top and bottom, as illustrated below. When applying the labels, make sure there is enough material on both ends to properly secure the power supply. When you are applying these labels, it is imperative that you do no cover any of the vent holes.

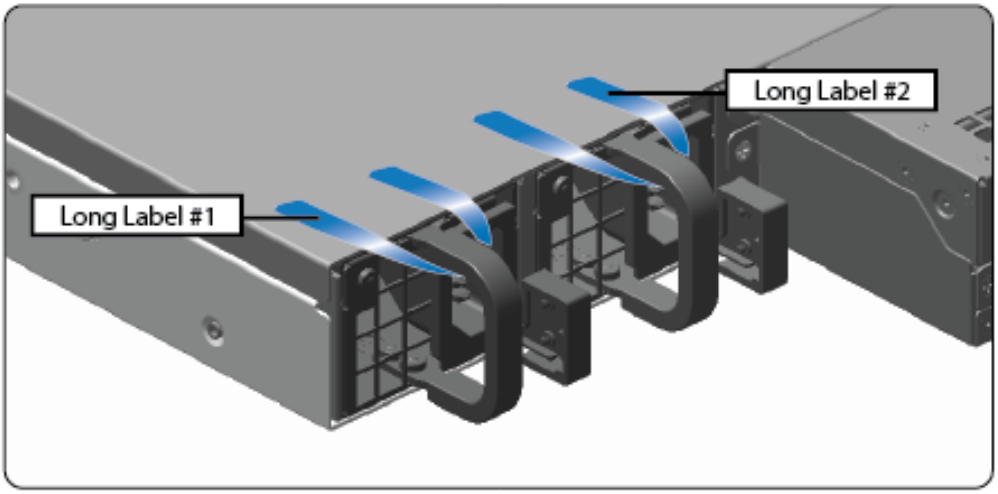


**Figure 11 MC S400 Power Supply Label Installation**

4. Apply two (2) short labels (short labels 3 and 4) over the opposite ends of the bezel and one (1) short label (short label 5) over the center cover panel curvature to prevent unauthorized access to the system components. Each label should be placed on the opposite ends of the appliance, as shown below.

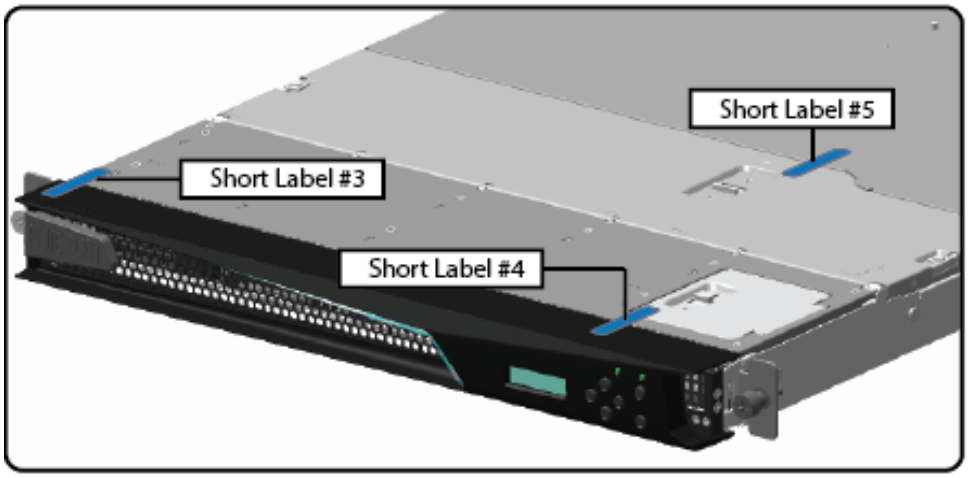


**Figure 12 MC S400 (Blue Coat logo) Top Bezel and Cover Label Installation**

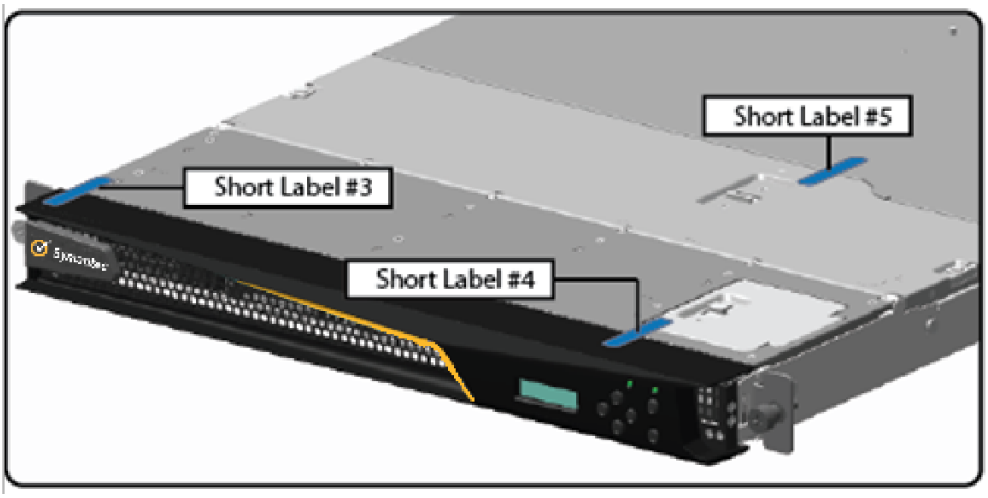


**Figure 13 MC S400 (Symantec logo) Top Bezel and Cover Label Installation**

**Note**: The chassis-center cover labels are destroyed each time the center cover is opened. Be sure to re-secure the appliance after servicing!

5. Power-on the appliance by plugging in the power cords.

# 3.2 Secure Management

## 3.2.1 Initialization

The module is delivered in an uninitialized factory state, and requires minimal first-time configuration to operate in FIPS-Approved mode and be accessed by a web browser. Physical access to the module shall be limited to the Crypto-Officer (CO), and the CO shall be responsible for putting the module into the Approved mode. Note, these same steps in this section shall be followed after the zeroization command is entered.

The process of establishing the initial configuration via a secure serial port is described below.

1. Connect a serial cable to a PC and to the module's serial port. Open a terminal emulator (such as HyperTerminal) on the PC, and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), using the port parameters provided in Table 16.

**Table 16 RS-232 Parameters**

| RS-232C Parameter | Parameter Setting |
|---|---|
| Baud rate | 9600 bps |
| Data bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Flow control | None |

2. Power up the module and wait for the system to finish booting.
3. Press **Enter** three times.

```
Welcome to the Symantec S400 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:
```

4. Enter **1** to access the Command Line Interface.
5. Type **enable** and press **Enter**.
6. 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.

7. After the system has finished rebooting, press **Enter** three times.
8. Enter the properties for the following:
   a. Interface number
   b. IP address

c. IP subnet mask

d. IP gateway

e. DNS server parameters

9. 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.

### 3.2.2 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.

If the CO detects signs of physical tampering, The CO should follow their organizations' defined plan for a security breach.

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

### 3.2.3 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 Managed Device Encryption Key. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

## 3.3 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 17 Acronyms**

| Acronym | Definition |
|---|---|
| AC | Alternating Current |
| AES | Advanced Encryption Standard |
| 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 |
| 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 |