Symantec & CA Technologies, a division of Broadcom
Web Isolation Virtual Appliance

Software Version: 1.10.48-fips+74

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 1
Document Version: 0.3

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 Web Isolation Virtual Appliance, software version 1.10.48-fips+74 from Symantec & CA Technologies, a division of Broadcom. This *Non-Proprietary Security Policy* describes how the Web Isolation Virtual Appliance meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the virtual appliance in the Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Web Isolation Virtual Appliance is referred to in this document as the Web Isolation Virtual Appliance, Web Isolation, 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
- *Submission Summary* 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. Web Isolation Virtual Appliance

2.1 Overview

IT security teams experience a constant barrage of attacks trying to penetrate their defenses and steal their data. Millions of new internet hosts – domains and sub-domains – are born every day. The vast majority of these exist for less than 24-hours, coming up and down quickly. These sites, valid and malicious, are not categorized and analyzed for risk effectively by web filtering and threat intelligence services because they have no meaningful reputational history. Add to this websites that are categorized and have a potentially unsafe risk profile, and security professionals have a real challenge on their hands. Some enterprises set policies that completely block sites that cannot be categorized or are assessed to have a potentially unsafe risk level. This typically results in overblocking their employee's web use since valid sites get caught up in these types of policy rules. Others may choose to roll the dice and permit access to these types of sites in order to not impede their employee's ability to perform their business activities, but this opens the organization up to undo risk. This risk is magnified in the case of privileged users, who are prized targets for cybercriminals because of the significant access rights and sensitive data typically found on their machines.

Web Isolation provides the following benefits:

- Allow protected access to uncategorized or potentially risky sites
- Increase business productivity by giving employees access to a broader set of websites
- Secure web browsing for executives and privileged users whose access to sensitive documents and systems makes them highly prized targets for cybercriminals
- Prevent users from disclosing corporate credentials to malicious websites
- Avoid patient zero by blocking advanced malware and targeted phishing attacks, minimizing alerts, investigations and remediation efforts
- Simplify web access policies and minimize support tickets requesting access to blocked site

See Figure 1 below for a typical deployment scenario for the Web Isolation Virtual Appliance (included in the red-dotted line).

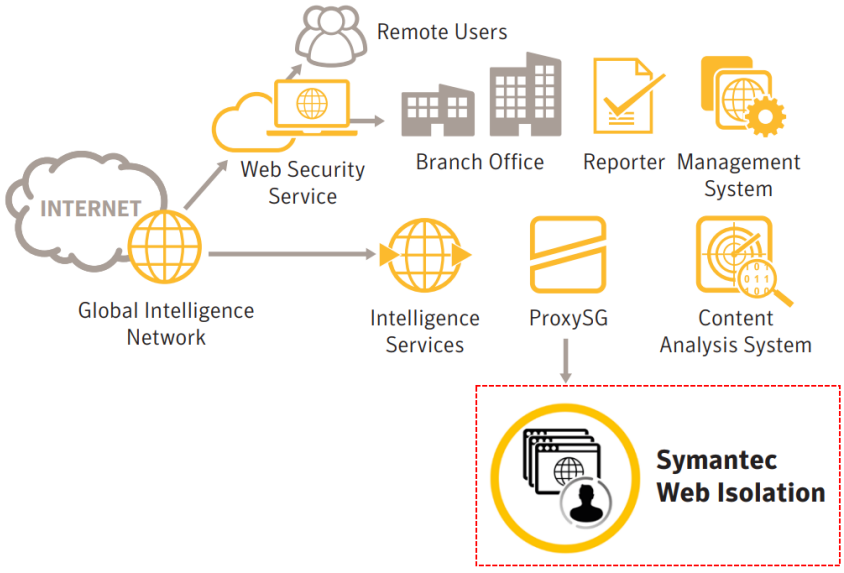


Figure 1 Typical Deployment of a Web Isolation Virtual Appliance

The module 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 Web Isolation Virtual Appliance Configurations

Virtual Appliance Type	SKU
Web Isolation	FWI-VA-NEW-1-100
	FWI-VA-NEW-100-250
	FWI-VA-NEW-250-500
	FWI-VA-NEW-500-1K
	FWI-VA-NEW-1K-2500
Threat Isolation Gateway	TIG-VA-NEW-1-100
	TIG-VA-NEW-100-250
	TIG-VA-NEW-250-500
	TIG-VA-NEW-500-1K
	TIG-VA-NEW-1K-2500

The different SKUs in Table 2 represent changes in the number supported users, and amount of web isolation possible. The module can be licensed as “Web Isolation” or a “Threat Isolation Gateway.” All appliance configurations are exactly the same from a cryptographic functionality and boundary perspective. The Crypto Officer and User services of the module are identical for all SKUs running either license.

The module 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 module software consists of the Web Isolation software with a Linux operating system as the guest OS in a VMware ESXi virtual machine. The module software, version 1.10.48-fips+74, contains the Web Isolation Cryptographic Library v1.0, the Web Isolation Integrity Library v1.0, and the Web Isolation SSH Library v1.0.

2.2.2 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.

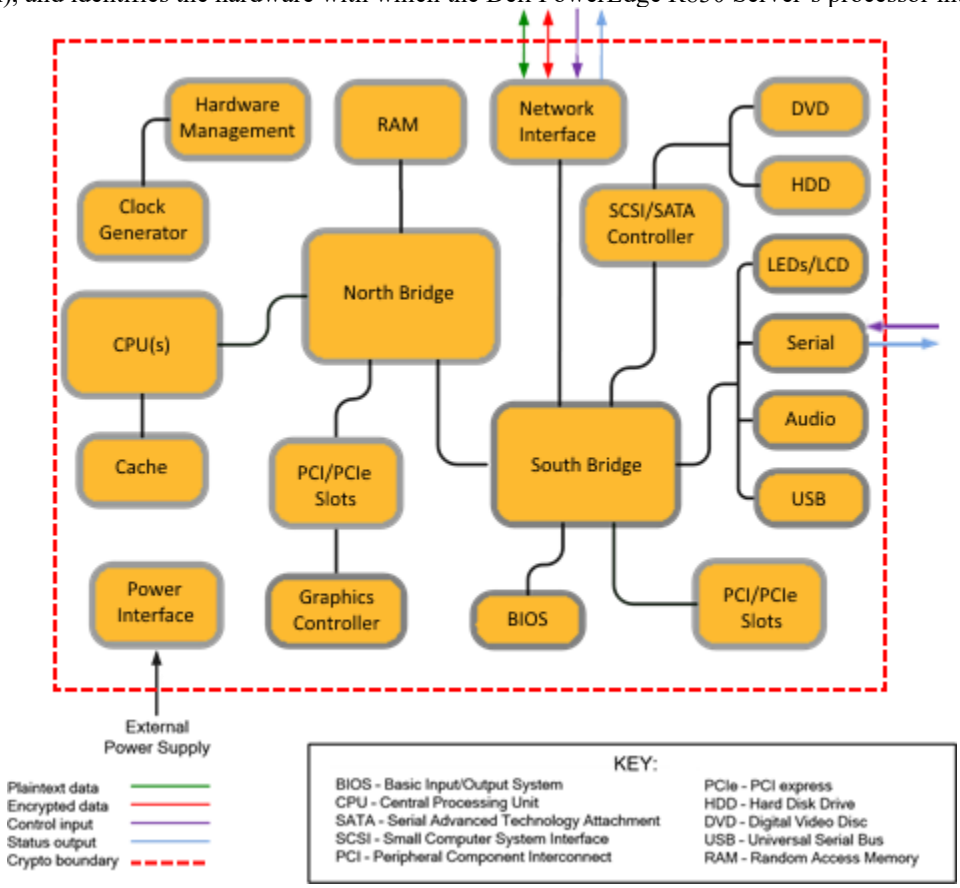


Figure 2 Block Diagram of the Dell PowerEdge R830 Server hardware

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 WI 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, RAM[1], hard disk, device case, power supply, and fans. 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.

[1] RAM – Random Access Memory

2.2.3 Logical Cryptographic Boundary

The logical cryptographic boundary of the module (shown by the red dotted line in Figure 3) consists of the Linux OS, and Web Isolation software, which contains the Web Isolation Cryptographic Library v1.0.

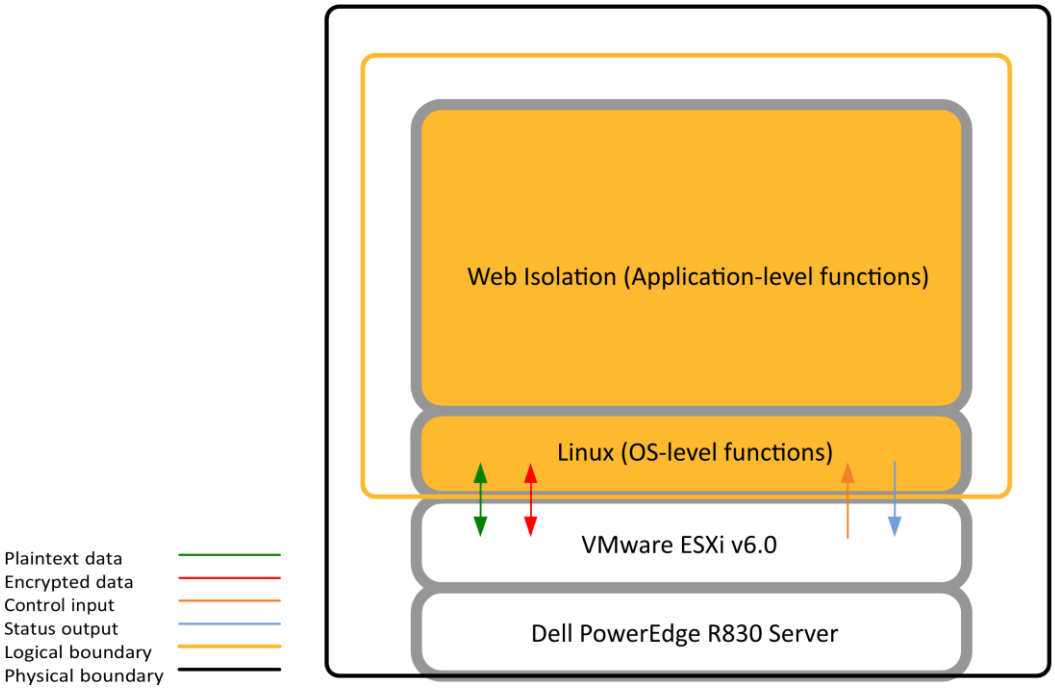


Figure 3 WI VA Cryptographic Boundary

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 WI 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 WI VA

Physical Port / Interface	Logical Port/Interface	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet 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 through the Virtual Ethernet and Virtual Serial Port interfaces (GUI, SSH CLI, and Serial CLI). Status output consists of the status provided or displayed via the user interfaces (such as GUI, SSH CLI, and Serial CLI) or available log information. Status output exits the module via the user interfaces (such as GUI , 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 two management interfaces:

- Command Line Interface (CLI): Accessible locally via the serial interface, or remotely using SSH. This interface is used for management of the modules. This interface must be accessed locally via the serial to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask). When the module has been properly configured, this interface can be accessed via SSH. Management of the module may take place via SSH or via the serial port. Authentication is required before any functionality will be available through the CLI.
- Web User Interface (UI): A graphical user interface accessible remotely with a web browser that supports TLS. This interface is used for management of the modules. Authentication is required before any functionality will be available through the Web UI

The details of these modes of operation are found below in Table 4.

Table 4 FIPS and WI VA Roles

FIPS Roles	Module Roles and Privileges
CO	The CO is an administrator of the module with capabilities to perform tasks such as account management and audit log management.
User	The User is a non-privileged user on the CLI, and has read-only permissions (Viewer) through the Management UI. The User's services are a subset of the CO 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. 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.

The Show Status service of the module is invoked whenever any of the services below in Table 5 or Table 6. As the module only operates in the Approved mode, executing any service of the module provides the status of the module.

2.4.2 Crypto-Officer Role

Descriptions of the FIPS 140-2 relevant services available to the Crypto-Officer role are provided in Table 5 below. Additional services that do not access CSPs can be found in the following documents:

- Symantec Threat Isolation Platform Guide for Administrators, Version 1.10-fips
- Symantec Web Isolation Release Notes, Version 1.10-fips

The link for all documentation can be found here:

- https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/web-isolation/1-0.html
- After navigating to this link, filter the documentation by version, selecting "1.10-fips."

Table 5 Crypto Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module (serial port only)	Initialize the module. For more information, see section 3.1.1 in this *Security Policy*.	CO Password : W
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 Authentication Key: WRX DRBG CSPs: WRX
Create remote management session (Web UI)	Manage the module through the Web UI (TLS) 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 TLS Session Key: WRX TLS Authentication Key: WRX TLS Pre-Master Secret: WRX TLS Master Secret: WRX DRBG CSPs: WRX
CO Authentication	Authenticate to the CO role	CO Password: R
Manage Zone Configuration	Edit Zones	None

Service	Description	CSP and Access Required
Configure Reporting	Configure reports servers, review activity logs, review analytics, and configure log forwarding parameters.	None
Configure Threshold Monitoring	Thresholds can be configured for metrics that will trigger an event log creation/email notification when the threshold is reached (e.g., high CPU load, low disk space).	None
Define Profiles	Define profiles for: • Isolation • Download • Upload • Activity Logging Profile • End-User Data Protection • Application Data Protection	None
Zeroize keys	Zeroize keys by invoking the command "fgcli system reset". This will zeroize all CSPs	All Keys
Change password	Change CO password	CO Password: W
Perform integrity check and power-on self-tests	Perform integrity check and power-on self-tests 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 Authentication Key: W TLS Session Key: W TLS Authentication Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: W HMAC Key: R

2.4.3 User Role

Descriptions of the FIPS 140-2 relevant services available to the User role are provided in Table 6 below. Additional services that do not access CSPs can be found in the following documents:

- Symantec Threat Isolation Platform Guide for Administrators, Version 1.10-fips
- Symantec Web Isolation Release Notes, Version 1.10-fips

The link for all documentation can be found here:

- https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1251137&locale=en_US
- After navigating to this link, filter the documentation by version, selecting "1.10-fips."

Table 6 User Role Services and CSP Access

Service	Description	CSP and Access Required
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 Authentication Key: WRX DRBG CSPs: WRX
Create remote management session (Web UI)	Manage the module through the Web UI (TLS) 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 TLS Session Key: WRX TLS Authentication Key: WRX TLS Pre-Master Secret: WRX TLS Master Secret: WRX DRBG CSPs: WRX
User Authentication	Authenticate to the User role	User Password: R
View Reporting	View reports servers, activity logs, review analytics, and log forwarding parameters.	None
View Threshold Monitoring	Thresholds can be viewed for metrics that will trigger an event log creation/email notification when the threshold is reached (e.g., high CPU load, low disk space).	None
View Profiles	View profiles for: • Isolation • Download • Upload • Activity Logging Profile • End-User Data Protection • Application Data Protection	None
View module configuration parameters and public keys/certificates (CLI)	View non-privileged level information including IP configuration and public keys/certificates.	RSA Public Key: R
Change password	Change User password (CLI Only)	User Password: W

2.4.4 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a user ID and password. Secure sessions that authenticate Users have no interface available to access other services (such as Crypto Officer services). There are no additional timing limitations provided by the module during authentication or between authentication attempts.

Each CO or User SSH session remains active (logged in) and secured until the operator logs out. Each CO and User Web UI session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

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

Table 7 Authentication Mechanisms Used by the Module

Role	Type of Authentication	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.
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 session.

2.5 Physical Security

The Web Isolation 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 4620v4 (single-user mode) processor
- VMware ESXi v6.0 with Ubuntu Linux 14.04 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.

2.7 Cryptographic Key Management

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

Table 8 FIPS-Approved Algorithm Implementations for Web Isolation Cryptographic Library version 1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#5678	AES	SP 800-38A, SP 800-38D	CBC, CTR, GCM[2]	128, 256	Data Encryption / Decryption
#5678 and #3781	KTS	SP 800-38F	AES and HMAC	128, 256	Key Transport
#2847	Triple-DES	SP 800-67	CBC	168 (3 different keys)	Data Encryption[3] / Decryption
#2847 and #3781	KTS	SP 800-38F	Triple-DES and HMAC	112	Key Transport
#4551	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest
#3781	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 HMAC-SHA-512	128, 256, 256, 512	Message Authentication
#3056	RSA	FIPS 186-4	SHA-256 PKCS1 v1.5	2048, 3072	KeyPair Generation Digital Signature Generation, Digital Signature Verification
#2296	DRBG	SP 800-90A	CTR-based		Deterministic Random Bit Generation

[2] AES-GCM was only CAVP tested for 256-bits.

[3] The maximum number of encryption operations for each Triple-DES key is 2^20.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
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. #2066 and SSH KDF CVL Cert. #2067).
Vendor Affirmed	KAS-SSC	SP 800-56A rev 3	ECC	P-256, P-384, P-512	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. #2066 and SSH KDF CVL Cert. #2067).
#2066	CVL TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation
Vendor Affirmed	CKG	SP 800-133			Key Generation

Table 9 FIPS-Approved Algorithm Implementations for Web Isolation Integrity Library version 1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#4548	SHS	FIPS 180-4	SHA-256		Software Integrity Check
#3778	HMAC	FIPS 198-1	HMAC-SHA-256,	256	Software Integrity Check

Table 10 FIPS-Approved Algorithm Implementations for Web Isolation SSH Library version 1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
#2067	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-256, SHA-384	Key Derivation

Table 11 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA Key Wrapping (PKCS#1)	Provides 112 or 150 bits of encryption strength	Key Wrapping
RSA Signature Verification	1536 bits	Signature Verification
Non-Deterministic Random Number generator (NDRNG)		Seeding for the FIPS-Approved DRBG (SP 800-90A 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.

The vendor affirms generated seeds for private keys are generated per SP 800-133 (unmodified output from a DRBG)

The module supports the CSPs listed below in Table 12.

Table 12 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
HMAC Key	HMAC SHA-256	Computed during setup and initialization.	Never output	Stored in plaintext on non-volatile memory.	N/A	Software Integrity Check
RSA Public Keys	2048, 3072-bits	Modules' public key is internally generated via FIPS-Approved DRBG Public key of a peer enters module in plaintext	Output during TLS/SSH[4] negotiation in plaintext.	Stored in plaintext form on non-volatile memory	Zeroize keys service	Negotiating TLS or SSH sessions
RSA Private Keys	2048, 3072-bits	Internally generated via FIPS-Approved DRBG	Never output	Stored in plaintext form on non-volatile memory	Zeroize keys service	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

[4] SSH session negotiation uses only RSA key pairs of 2048-bits. All RSA key pair sizes can be used for TLS session negotiation.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
ECDH public key	P-256 key	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
ECDH private key	P-256 key	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
TLS Session key	AES CBC, CTR, or GCM[5] 128- 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
TLS Session Authentication key	HMAC SHA-1-, 256-, 384- or 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for TLS 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

[5] AES-GCM – The module's use of GCM is specific to TLS and is compatible with TLS 1.2 and supports the acceptable GCM cipher suites from SP800-52 Rev 1, Section 3.3.1.

AES-GCM – The module generates a new AES GCM key in TLS when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key based on the counter size.

AES-GCM – The counter portion of the IV is set by the module within its cryptographic boundary.

AES-GCM – In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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
SSH Session Key	Triple-DES 168-bit, AES CBC, CTR 128- 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
SSH Session Authentication key	HMAC SHA-1-, 256- or 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	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	Zeroize keys service	Authenticating a CO for Web UI or CLI
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.	Exits in encrypted form via a secure TLS session for external authentication	Stored in encrypted form on non-volatile memory	Zeroize keys service	Authenticating User for Web UI or CLI
SP 800-90A CTR_DRBG Seed	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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG Entropy[6]	416-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 384-bits from an entropy-generating NDRNG inside the module's cryptographic boundary.

[6] The Entropy required by the FIPS-Approved SP 800-90A CTR_DRBG (with AES-256) is supplied by the NDRNG

2.8 Self-Tests

If the module fails any power-up self-tests, including the startup integrity test, the corresponding self-test error or modified files for the integrity test is printed to the CLI (when being accessed via the local console):

Integrity Test example:

```
***FILE has changed****
Openssl.c
```

Algorithms KAT example:

```
***********ERROR TO DUE FIPS LOCKDOWN!****************
"ERROR: Self-test failed for AES.
```

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 CO to reboot the modules. The status output provided above is shown only over the CLI (when being accessed via the serial port). The remote CLI via SSH or Web Management interface will be inaccessible when the module is in an error state.

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

2.8.2 Power-Up Self-Tests

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

- Software integrity check (HMAC-SHA-256) by the Web Isolation Integrity Library
- Known Answer Tests for the Web Isolation Cryptographic Library
    - AES-ECB KAT for encryption and decryption
    - AES-GCM KAT for decryption and decryption
    - TDES KAT for encryption and decryption
    - SHA KAT using each of SHA-1, SHA-256, SHA-384, SHA-512
    - HMAC KAT using each of SHA-1, SHA-256, SHA-384, SHA-512
    - RSA Sign/Verify KAT with SHA-256
    - RSA wrap/unwrap KAT
    - SP800-90A DRBG KAT
    - DH "Primitive Z" 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 on all crypto implementations have completed.

2.8.3 Conditional Self-Tests

The module performs the conditional self-tests:

- 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)

2.8.4 Critical Function Tests

The Web Isolation Virtual Appliance performs the following critical function tests:

- DRBG Instantiate Critical Function Test
- DRBG Reseed Critical Function Test
- DRBG Generate Critical Function Test
- DRBG Uninstantiate Critical Function 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 Web Isolation 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 Secure Management

The CO is responsible for initialization and security-relevant configuration and management of the module. Please see the *Symantec Threat Isolation Platform Guide for Administrators, Version 1.10-fips* for more information on configuring and maintaining the module.

Caveat: While the WI VA may hold and boot from multiple software images, only the software image documented in this Security Policy (Software Version: 1.10.48-fips+74) may be used for booting in order to remain compliant. Booting from any other software image will result in a non-compliant module

Per IG 9.7 the loaded software image is a completely replacement of the validated image. Any software version loaded that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

3.1.1 Initialization

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

Download and Extraction

1. Download the installer file from https://support.broadcom.com/security/download-center.
2. Mount the downloaded ISO file to the virtual CD/DVD and boot the VM.
3. When the following screen appears, choose Install Threat Isolation.

4. At the end of the installation, the system automatically reboots.
5. Log into the installed machine using the following default credentials:
   ```
   Username:  fireglass
   Password:  fireglasssecure
   ```
6. At the command line, go to root and type the following:

```
sudo passwd fireglass
```

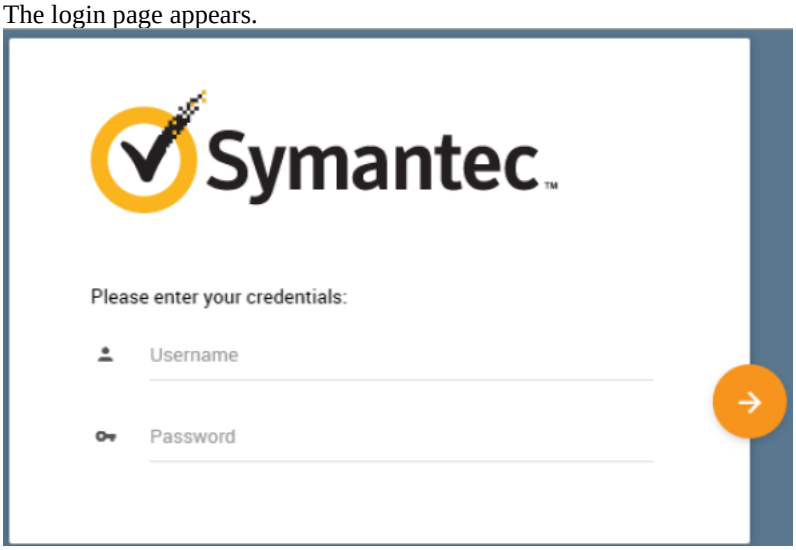
7. Enter your new password.
8. Enter your new password a second time
   Note: the CO must configure the password to be at least 8 characters in length.
9. The following message will be displayed:
   ```
   password updated successfully
   ```
10. To enable the report server, run the following command:
    ```
    cd /opt/fireglass/current/ci_infra/report_server
    sudo ./install.sh
    ```

Initializing the Symantec Threat Isolation Platform

1. Log into the gateway machine through the terminal
2. Run the following command:
   ```
   sudo fgcli setup
   ```
3. The Network Configuration Wizard starts.
4. Follow the instructions of the wizard to perform Initial Setup.
5. The system reinitializes, and the following message is displayed:
   ```
   Done
   ```

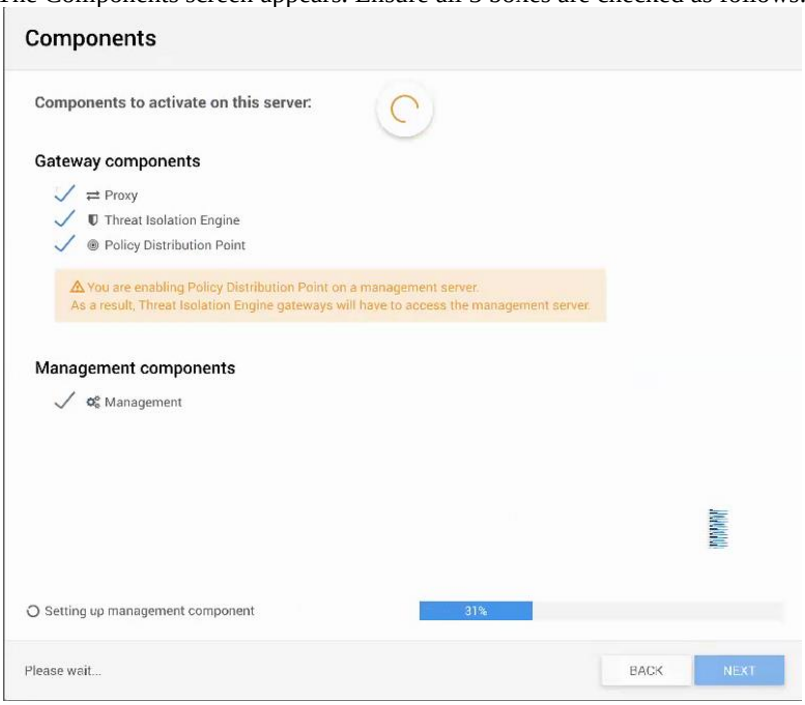
Running the First Time Wizard and Defining Components

1. Open the Symantec Threat Isolation Management UI. From your web browser, open the following URL:
   ```
   https://<management host or IP>:9000
   ```
2. The login page appears.



3. Enter the following default credentials:
   ```
   Username:  admin
   Password:  admin
   ```
4. Click the arrow to log in.
5. The License Agreement window appears.
6. Read the terms of the license agreement and check the checkbox to accept them.
7. Click **Next.**
8. The Initial Settings window appears. Enter the DNS name for the management machine (public DNS host name). Also, enter the appropriate time zone.
9. Click Next.
10. The authentication Settings window appears.
11. Type in a new password for the admin account that is at least 8 characters. Retype in the password for confirmation.
12. Enter an email address for receiving notifications.

13. The Active Directory window appears, leave the settings as unconfigured and click **Next**.
14. The Product Registration window appears.
15. The Components screen appears. Ensure all 3 boxes are checked as follows:



16. The Summary window appears. The message, "The Initial configuration has been successfully completed," should appear. Click **Finish**.

Upon completion of these initialization steps, the module is considered to be operating in its Approved mode of operation. The module only operates in the Approved mode once it has been configured. There is no non-Approved mode of operation.

3.1.2 Management

The CO is able to monitor and configure the module via the Web UI (HTTPS over TLS) and the CLI (serial port or SSH).

The CO 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 Support 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.

Key sizes less than what is specified shall not be used. The CO password must be at least 8 characters in length. The CO must change the CLI password after initial login.

The CO must restrict Web Interface management sessions to be established only using the TLS 1.2 protocol only.

3.1.3 Zeroization

The CO can return the module to its factory state by invoking the command "fgcli system reset". This command will zeroize all persistent keys and CSPs by overwriting the previously stored values with new values. The RSA private key, Crypto-Officer password, and User password are stored persistently and are therefore zeroized as part of this procedure.

In addition, rebooting the module causes all temporary keys stored in volatile memory (SSH Session key, SSH Authentication Key, TLS session key, TLS Authentication key, TLS Pre-Master Secret, TLS Master Secret, DRBG entropy values, and NDRNG entropy values) to be zeroized. 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 (Web UI). 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.

The User must restrict Web Interface management sessions to be established only using the TLS 1.2 protocol only.

4. Acronyms

This section describes the acronyms used throughout this document.

Table 13 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
CSE	Communications Security Establishment
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
GCM	Galois/Counter-Mode
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
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security