IBM® Security QRadar® SIEM

Hardware Version 7.2

Firmware Version 7.2

FIPS 140-2

Non-Proprietary Security Policy

Policy Version 1.2

August 13, 2016

IBM Corporation
80 Bishop Dr. Unit B
Fredericton, NB
E3C 1B2
Canada

Table of Contents

List of Tables

List of Figures

1 Introduction

This document is the non-proprietary Security Policy for the IBM® Security QRadar® SIEM Version 7.2 cryptographic module. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module. The module is referred to in this document as the appliance, cryptographic module, or the module.

This Security Policy describes the features and design of the IBM® Security QRadar® SIEM Version 7.2 using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard and information on the CMVP can be found at http://csrc.nist.gov/groups/STM/cmvp.

This Security Policy contains only non-proprietary information. This document may be freely reproduced and distributed whole and intact. All other documentation submitted for FIPS 140-2 conformance testing and validation is “IBM - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The IBM Security QRadar cryptographic module meets the overall requirements applicable to Level 2 security for FIPS 140-2 as shown in Table 1.

Table 1: Cryptographic Module Security Requirements.

Security Requirements Section	***Level***
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.1 Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CBC	Cipher-Block Chaining
CFB	Cipher Feedback
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hashing for Message Authentication
KAT	Known Answer Test
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PUB	Publication
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm

2 IBM® Security QRadar® SIEM

2.1 Functional Overview

IBM Security QRadar SIEM version 7.2family of products provides a security intelligence platform that integrates critical functions including SIEM, log management, configuration monitoring, network behavior anomaly detection, risk management, vulnerability management, network vulnerability scanning, full packet capture and network forensics into a comprehensive intelligence solution.

IBM Security QRadar version 7.2 delivers these enhanced features:

- QRadar QFlow Collector component provides improved Gbps QFlow collection and processing.
- Enables security information to be retrieved and updated from third-party systems with the Offense API.
- Enhanced threat intelligence feed provides hourly update of threat intelligence with additional context and categorization data.
- Flow burst handling helps ensure that data loss is minimized during very high bursts of network flow data.
- Improved big data integration enables more easily configurable data forwarding profiles.
- IBM Security QRadar Data Node enhancements enable historic data to be stored separately, helping deliver historic searches and analytics without impacting real-time security operations.
- Contains crossover cable high availability user interface configuration designed to simplify high available setup.
- Supports silent installation, enabling full automation of QRadar installs in public and private clouds and enterprise networks.

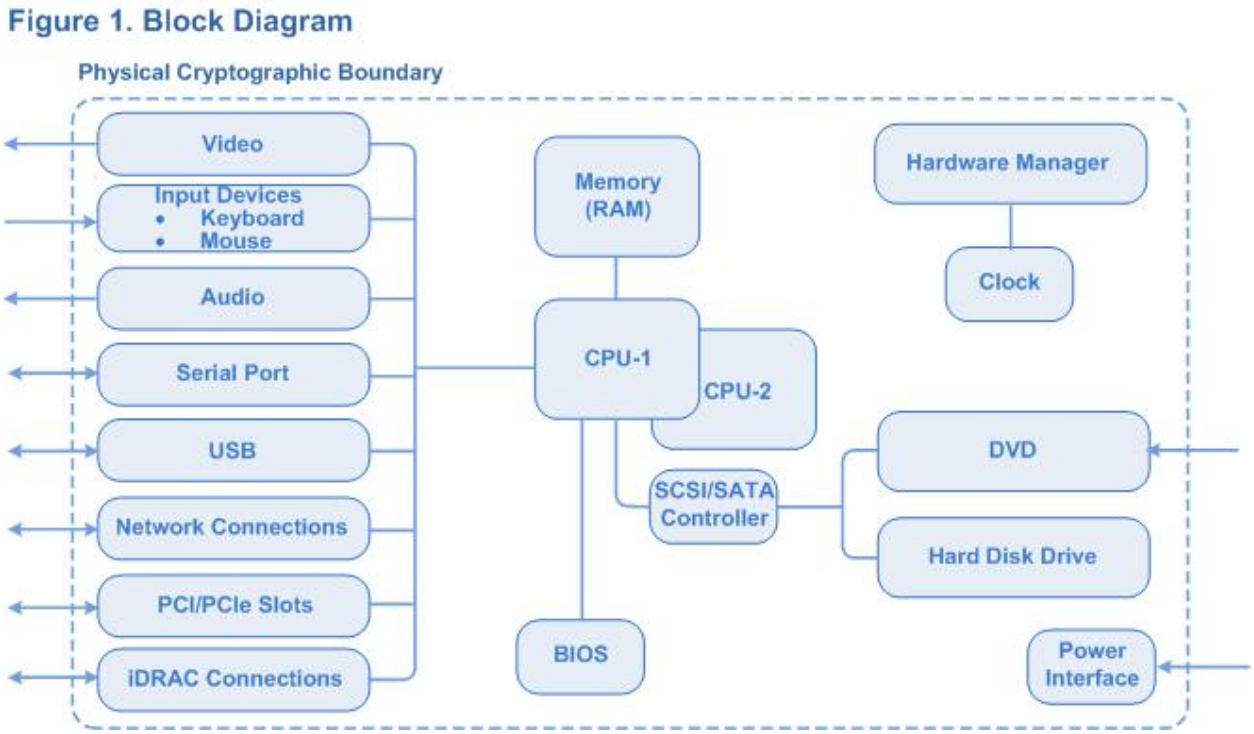
The module provides security functions for encryption, decryption, random number generation, hashing, getting the status of the integrity test, and running the self-tests. The library is used by the application.

2.2 Module Specification

The IBM Security QRadar version 7.2 SIEM is a multi-chip standalone hardware module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the QRadar is defined by the opaque and hard metal appliance chassis, which surrounds all the hardware and software components.

Following is a block diagram of the module.

Figure 1 – Module Block Diagram

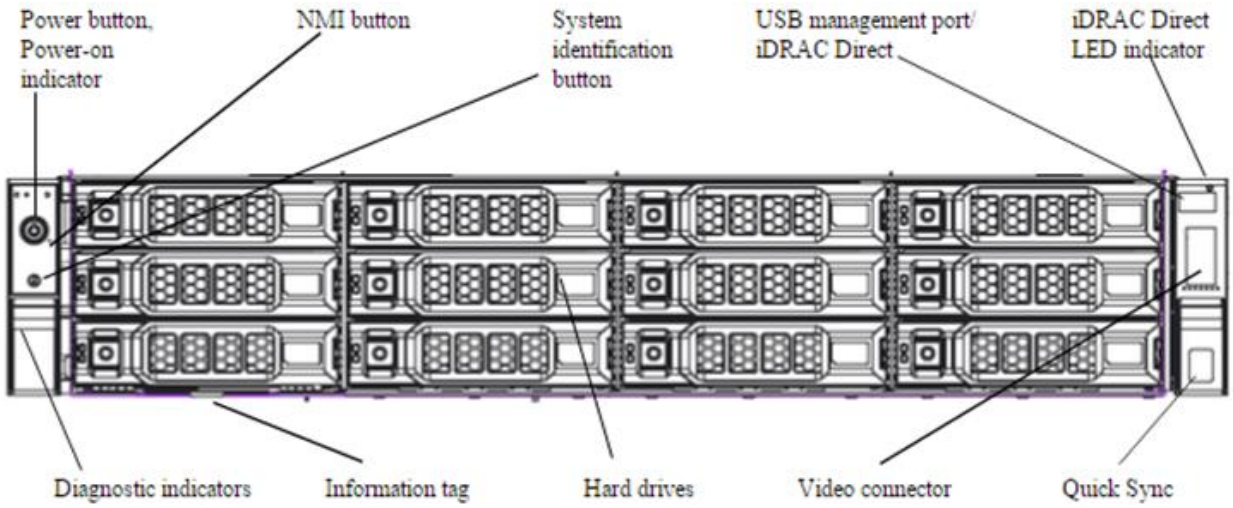


2.3 Module Interfaces

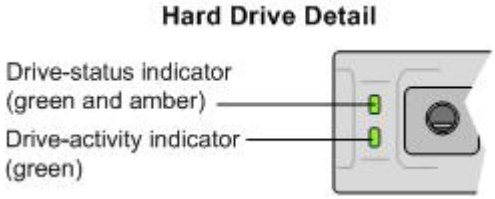
Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

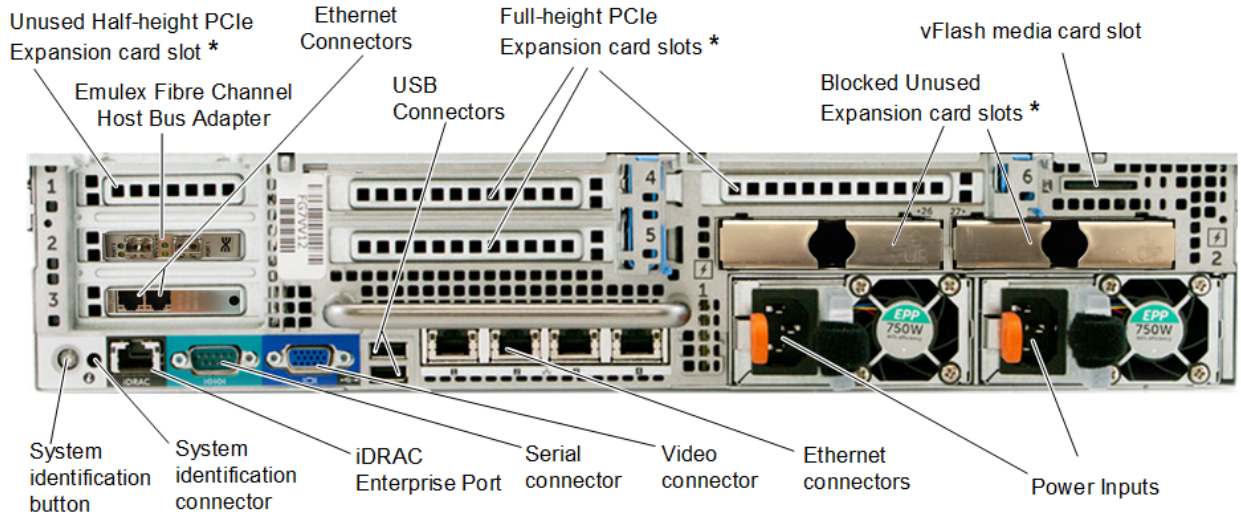
- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

Figure 2 – IBM Security QRadar SIEM Features and Indicators



Front Panel





* Expansion card callouts describe unused card slots that do not map to any module interfaces.

Back Panel

The physical interfaces described in Figure 1 map to logical interfaces defined by FIPS 140-2, as described in Table 2.

Table 2: FIPS 140-2 Logical Interface Mappings

Logical Interface	Physical Ports
Data input	• Ethernet interfaces • vFlash media card slot • Serial connector • USB ports • Emulex FC Host Bus Adapter
Data output	• Ethernet interfaces • vFlash media card slot • Serial connector • Video connectors • USB ports • Emulex FC Host Bus Adapter
Control input	• System management interface • Ethernet interfaces • NMI button • Power button • Serial connector • iDRAC port
Status output	• System management interface • Hard drive status and activity indicators • Ethernet interfaces • Diagnostic indicators • Ethernet interface activity and link indicators • Power supply status indicators • Serial connector • Video connector • iDRAC port • iDRAC Direct LED • Quick Sync interface
Power	• Power inputs

The following features or indicators are not FIPS 140-2 logical interfaces:

- Information tag (documentation only)
- Empty PCIe slots (unused).
- System ID button and connector – outside the scope of evaluation.

2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

2.4.1 Authorized Roles

The module supports role-based authentication, providing three authorized roles that an operator explicitly assumes: a Crypto-Officer (CO) role, a FIPS Admin role, and a User role. The module does not support concurrent operators.

- Crypto-User (cryptographic officer) – The Crypto-Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. Before accessing the module for any administrative service, the operator must authenticate to the module. The module offers 2 management interfaces:
    - Web GUI – Accessible only by User roles
    - QConsole – Accessible only by CO and FIPS Admin roles
- FIPS Admin – The FIPS Admin role has the ability to modify system files, view logs, and reboot the appliance.
- User – The User role has the ability to access module services through Web GUI only.

2.4.2 Services

All services require that operators assume an authorized role. The services associated with each role are listed in Table 3, Table 4, and Table 5. Please note that the keys and Critical Security Parameters (CSPs) listed in these tables use the following indicators to show the type of access required:

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

2.4.3 Crypto Officer Role Services

The Crypto Officer can initialize and configure the module to run in FIPS approved mode and verify FIPS status on an appliance. Crypto users are also allowed all of the commands provided to admin users for QRadar maintenance.

Table 3: Crypto Officer Services

Service	Description	Input	Output	CSP and access type
Install the module	Physically install the IBM Security QRadar SIEM module.	Physical actions	Installed module	None
Perform self-test	Run self-tests on demand via reboot	Command	Status Output	None
Connect via SSH	Establishing an SSH connection uses basic cryptographic services (encryption, decryption, random bit generation, SHA hashing, and HMAC).	Username and password	Connection established	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
commit	Apply any changes made to a system file of your FIPS enabled system.	Command	Command Response	None
deploy	Start a full deploy on the appliance. Restarts all services	Command	Command Response and Status Output	None
disable_verified_mode	Takes the module out of a configured state by allowing 'root' access. The non-configured state is non-compliant and outside the scope of the validation.	Command	Command Response and Status Output	Advanced Encryption Standard (AES) – W Triple Data Encryption Standard (Triple-DES) – W RSA public/private keys – W Diffie-Hellman (DH) – W (keyed) Hash Message Authentication Code (HMAC) – W
fips_self_check	Displays the status of the operating system, required RPM files, log settings, and FIPS mode in the command line.	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
get_logs	Collects system data for your FIPS appliance.	Command	Command Response	None
mod_log4j	Modifies log sources by using the command-line interface of a FIPS enabled appliance.	Command	Command Response	None

Service	Description	Input	Output	CSP and access type
reboot	Restarts a FIPS enabled appliance.	Command	Command Response and Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
service <service name> <start | stop | restart>	Changes the status of a service on your QRadar appliance. For a list of services that can be restarted by the crypto user, type **service --list.**	Command	Command Response and Status Output	None
shell	Accesses a command-line shell for viewing and editing files.	Command	Command Response and Status Output	None
shutdown	Powers off a FIPS enabled appliance.	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
Zeroize	Zeroizes the module to the factory default state. The zeroize service is called by reimaging the module.	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W RADIUS key –W TACACS key – W
help	Displays the help interface for a specific admin or crypto user command. <command> is any crypto user command in this table.	Command	Command Response	None
exit	Log out of the crypto user account.	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

2.4.4 FIPS Admin Role Services

The admin user role maintains and supports the FIPS appliances in your organization. Admin users can use a specific subset set of shell command line options to maintain a FIPS enabled system.

Table 4: FIPS Admin Role Services

Service	Description	Input	Output	CSP and access type
Connect via SSH	Establishing an SSH connection uses basic cryptographic services (encryption, decryption, random bit generation, SHA hashing, and HMAC).	Username and password	Connection established	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
commit	Apply any changes made to a system file of your FIPS enabled system.	Command	Command Response	None
deploy	Start a full deploy on the appliance. Restarts all services	Command	Command Response and Status Output	None
get_logs	Collects system data for your FIPS appliance.	Command	Command Response	None
mod_log4j	Modifies log sources by using the command-line interface of a FIPS enabled appliance.	Command	Command Response	None
reboot	Restarts a FIPS enabled appliance.	Command	Command Response and Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
shell	Accesses a command-line shell for viewing and editing files.	Command	Command Response and Status Output	None
shutdown	Powers off a FIPS enabled appliance.	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
Zeroize	Zeroizes the module to the factory default state. The zeroize service is called by reimaging the module.	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W RADIUS key –W TACACS key – W

Service	Description	Input	Output	CSP and access type
help	Displays the help interface for a specific admin or crypto FIPS command. <command> is any crypto user command in this table.	Command	Command Response	None
exit	Log out of the admin user account.	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

2.4.5 User Services

Users access the module web GUI to access services. Users cannot access shell commands.

Table 5: FIPS User Role Services

Service	Description	Input	Output	CSP and access type
Admin GUI User only				
Connect to the Admin GUI	Establishing an HTTPS connection uses basic cryptographic services (encryption, decryption, random bit generation, and SHA hashing).	Username and password	Connection established	AES – W Triple-DES – W RSA public/private keys – W DH – W
Manage Roles	View, create, edit, and delete operator roles for GUI only.	Command	Command Response	None
Manage Accounts	Create, edit, and disable operator accounts	Command	Command Response	None
Set Authentication Type	Set the module to perform authentication via system, RADIUS[1], TACACS[2], or LDAP[3]/Active Directory	Command	Command Response	RADIUS key – W TACACS key – W LDAP credential – W
Manage License Keys	View, update, and export license keys	Command	Command Response	None
Configure Access Settings	Configure firewall access, update host set-up, configure interface roles, change passwords, and update system time	Command	Command Response	User passwords – W, X

[1] RADIUS – Remote Authentication Dial-In User Service
[2] TACACS – Terminal Access Control Access Control System
[3] LDAP – Lightweight Directory Access Protocol

Service	Description	Input	Output	CSP and access type
Configure System	Set up network hierarchy, system settings, system notifications schedules, and Console settings	Command	Command Response	None
Manage Authorized Services	View, add, and revoke authorized services; configure customer support service	Command	Command Response	None
Manage Backup and Recovery	Manage backup archives and backup/restore data	Command	Command Response	None
Edit Deployment	Create a deployment, assign connections, and configure individual module component	Command	Command Response	AES – R, W, X Triple-DES – R, W, X
Manage Flow Sources	Manage flow sources and flow source aliases	Command	Command Response	None
Configure Remote Networks and Services	Manage QRadar remote networks and services	Command	Command Response	None
Configure Rules	Configure rules to perform tests on events, flows, and offenses	Command	Command Response	None
Discover Servers	Discover servers for creating server-type building blocks	Command	Command Response	None
Forward Syslog Data	Forward raw or normalized syslog data to specified destinations	Command	Command Response	None
Select Data Sources	Provides access to vulnerability scanners, log source management, custom event and flow properties, and flow sources	Command	Command Response	None
Configure Plug-Ins	Provides access to plug-in components, such as the plug-in for the QRadar Risk Manager	Command	Command Response	None
View Audit Logs	Allow User to view audit log files	Command	Command Response	None
All GUI Users				
Manage Dashboard	View, create, edit, and delete a dashboard	Command	Command Response	None
Analyze Events	Analyze records from a network activity log	Command	Command Response	None
Analyze Flows	Monitor network flow data in real-time	Command	Command Response	None
Manage Assets	View and manage asset profiles	Command	Command Response	None
Manage Reports	Create, generate, customize, and view reports	Command	Command Response	None

2.4.6 Authentication Mechanisms

The module supports role-based authentication to control access to services that require access to sensitive keys and CSPs. The CO and FIPS Admin roles are the only roles authorized to access the shell commands. Users can only connect only to the Web GUI.

To access module services, the CO and FIPS Admin role must authenticate using a user ID and password. This can be done locally or using SSH to establishing a secure tunnel to the shell. Secure sessions that authenticate the CO and FIPS Admin only provide the services associated with those roles (i.e., they have no interface available to access other services). Each CO or FIPS Admin SSH session remains active and secured using the tunneling protocol until the operator logs out or an inactivity time is reached.

Users connecting to the module through the Web GUI must first establish a TLS session. These Users then enter a username and password which may be authenticated locally or through the use of external RADIUS, TACACS, or LDAP servers.

The module employs the authentication methods described in Table 6 to authenticate a Crypto-Officer, FIPS Admin, and User.

Table 6: Strength of Authentication Methods

Role	Type of Authentication	Authentication Strength
Crypto-Officer and FIPS Admin	Password	Passwords are required to be at least 6 characters long. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and seven special characters can be used with repetition, which gives a total of 69 characters to choose from. The chance of a random attempt falsely succeeding is 1:69^6, or 1: 107,918,163,081. When a user enters an incorrect password, the module enforces a 2 second delay before issuing the failure and allowing another attempt. Remote connections terminate after 6 consecutive failed attempts. This limits local password attempts to fewer than 30 in a one-minute period (30/69^5) with a probability of far less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

User	Password or Certificate	Passwords are required to be at least 5 characters long. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and 32 special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is 1:94^5 or 1: 689,869,781,056. This would require about 6,898,697 attempts in one minute to raise the random attempt success rate to more than 1:100,000. Since the user is locked out for 30 minutes after every 5 unsuccessful attempts, the most attempts that could be done in one minute would be 5. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.

2.4.6.1 Authentication Data Protection

The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the User role with administrator privileges. The module hashes User's passwords with an SHA-1[4] hash function and stores the hashed password in a password database. CO and FIPS Admin roles passwords are encrypted using Triple-DES and stored in a password database. If a User attempts to access the system multiple times (5 by default) using invalid information, the User must wait the configured amount of time (30 minutes by default) before attempting to access the system again.

2.5 Physical Security

The IBM Security QRadar SIEM is a multi-chip standalone cryptographic module. The module is contained in a hard metal chassis which is defined as the cryptographic boundary of the module. The module's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. The enclosure has a limited set of ventilation holes that, when coupled with factory-installed internal opacity baffles and additional baffles installed by the crypto officer during module initialization, prevent visual inspection of the internal components of the module. Tamper-evident seals are applied to the case and hot-swappable disk drives to provide physical evidence of attempts to remove the chassis

[4] SHA – Secure Hash Algorithm

cover, front bezel or drive assemblies. The tamper evident labels and opacity baffles shall be installed for the module to operate in a FIPS Approved mode of operation.

The IBM Security QRadar SIEM system has been 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 Operational Environment

The module employs a non-modifiable operating environment. Operators are provided with no mechanisms with which to modify the operating system. Also, the module does not provide a mechanism to add additional software or firmware onto the appliance. The module's firmware is executed by the module's Intel Xeon processor.

2.7 Cryptographic Key Management

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

Table 7 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES 128/192/256 in ECB/CBC/CFB/CTR/OFB modes	3509
Triple-DES 192 in TECB/TCBC/TCFB/TOFB modes	1973
RSA (X9.31, PSS, PKCS#1 v1.5) for signing, signature generation and verification, and key generation – 2048 and 3072-bit. The module supports, both FIPS 186-2 and FIPS 186-4.	1804
SHA-1, SHA-256, SHA-512	2894
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512	2242
SP 800-90A Deterministic Random Bit Generator (DRBG) CTR-DRBG AES-256	876
TLS KDF options: TLS 1.0/1.1 using SHA-1, TLS 1.2 using SHA-256 SSH KDF options: SHA-1, SHA-256, SHA-512	577

All cryptographic keys and CSPs are under the control of the OS or calling applications, which is responsible for protection of the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined APIs. The module performs a Software/Firmware Integrity Test using the HMAC-SHA-256 algorithm.

Additionally, the module utilizes the following non FIPS-Approved algorithm implementation:

- Diffie-Hellman keys are from 2048 to 8192 bits (key agreement, key establishment methodology provides between 112 and 202 bits of encryption strength).
- HMAC MD5 and MD5 within TLS only.
- Non-deterministic random number generators for seeding the SP800-90A DRBG.
    - The minimum number of bits of entropy requested per each GET function is 256 bits.
    - The NDRNG is outside the logical boundary but is within the physical boundary.
- RSA provides 2048 and 3072 bit public keys (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength).

The TLS and SSH protocols have not been reviewed or tested by the CAVP and CMVP. Please see NIST document SP800-131A for guidance regarding the use of non FIPS-approved algorithms.

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

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

CSP (Key Type)	Generation / Input	Output	Storage	Zeroization	Use
AES Keys (AES 128, 192, 256 bit keys)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle, host reboot.	TLS or SSH session key. Encryption and decryption.
Triple DES Keys (192 bit keys)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle, host reboot.	TLS or SSH session key. Encryption and decryption.
RSA private key (RSA 2048, 3072 bit key)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle, host reboot	Signature generation, decryption
					Negotiating TLS or SSH sessions
RSA Public Key (RSA 2048, 3072 bit key)	Internally generated	Never API call parameter	Plaintext in volatile memory	By API call, power cycle, host reboot	Signature verification, encryption
					Negotiating TLS or SSH sessions

CSP (Key Type)	Generation / Input	Output	Storage	Zeroization	Use
DH Public Components (Public components of DH protocol are between 2048 and 8192 bits)	Internally generated	API call parameter	Plaintext in volatile memory	By API call, power cycle, host reboot	Negotiating TLS or SSH sessions
DH Private Components (Private components of DH protocol are between 224 and 512 bits)	Internally generated	API call parameter	Plaintext in volatile memory	By API call, power cycle, host reboot	Negotiating TLS or SSH sessions
DRBG entropy input (SP800-90A DRBG (512 bits)	Derived using Non FIPS approved HW RNG	Never	Stored in plaintext in volatile memory.	Zeroized on reboot	DRBG entropy input
CTR_DRBG secret value (128 bits)	Derived internally using counter update function.	Never	Stored in plaintext in volatile memory.	Zeroized on reboot	The value of “V” is the “secret value” of the internal state.
CTR_DRBG secret key (256 bits)	Derived internally using counter update function.	Never	Stored in plaintext in volatile memory.	Zeroized on reboot	The value of “key” is the “secret key” of the internal state.
Crypto-Officer Password, FIPS Admin Password (Passphrase of at least six characters)	Entered by a CO or FIPS Admin locally	Never	Stored on disk in encrypted form	Zeroized when the password is updated with a new password	Used for authenticating all COs and FIPS Admin over CLI[5]

[5] CLI – Command Line Interface

CSP (Key Type)	Generation / Input	Output	Storage	Zeroization	Use
User Password (Passphrase of at least five characters)	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	Used for authenticating all Users over GUI
RADUIS credential (Alpha-numeric string)	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	This password is used by the module to authenticate itself to the RADIUS server. This password is required for the module to validate the credential supplied by the user with the RADIUS server
LDAP credential (Alpha-numeric string)	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	This password is used by the module to authenticate itself to the LDAP server. This password is required for the module to validate the credential supplied by the user with the LDAP server
TACACS Server Encryption Key (Alpha-numeric string)	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	A shared secret to remote TACACS server

CSP (Key Type)	Generation / Input	Output	Storage	Zeroization	Use
HMAC Key (HMAC key SHA-1, 256, or 512)	Internally generated	Never	Plaintext in volatile memory	By command, power cycle, reboot	Message Authentication in TLS, SSH, password hashing.
Software/ firmware Integrity Keys (HMAC SHA-256 key)	Externally generated and hard-coded in the image	Never	Hard-coded in plaintext	By uninstalling the module	Used to perform the software/ firmware integrity test at power-on

2.7.1 Key Generation

The module uses an SP 800-90A DRBG implementation to generate cryptographic keys. This DRBG is FIPS-Approved as shown in Annex C to FIPS PUB 140-2. The module complies with SP 800-133 and IG 7.8.

2.7.2 Key Entry and Output

The cryptographic module itself does not support key entry or key output from its physical boundary in unencrypted form. However, keys are passed to the module as parameters from the applications resident on the host platform via the exposed APIs. Similarly, keys and CSPs exit the module in plaintext via the well-defined exported APIs.

2.7.3 Key/CSP Storage and Zeroization

Symmetric, asymmetric, and HMAC keys are either provided by or delivered to the calling process, and are subsequently destroyed by the module at the completion of the API call. Keys and CSPs stored in RAM can be zeroized by a power cycle or a host system reboot. The SP 800-90A DRBG seed is initialized by the module at power-up and remain stored in RAM until the module is uninitialized by a host system reboot or power cycle. The HMAC key that is used to verify the integrity of the module is stored in a file residing on the host system.

2.8 EMI/EMC

This version of QRadar is hardware running firmware. The IBM QRadar SIEM hardware was tested and found to meet the requirements of the Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15.

2.9 Self-Tests

This section describes the power-up and conditional self-tests performed by the module.

2.9.1 Power-Up Self-Tests

The following self-tests are performed at power-up:

- Software/firmware integrity checks (HMAC SHA-256) over each component of the module.
- Known Answer Tests (KATs):
    - AES Encrypt,
    - AES Decrypt,
    - Triple-DES Encrypt,
    - Triple-DES Decrypt,
    - RSA. The following implementations are tested:
        - X9.31 signature generation, signature verification
        - PKCS#1 1.5 signature generation, signature verification
        - PSS signature generation, signature verification
    - SHA-1, SHA-256, SHA-512
    - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
    - SP 800-90A DRBG. The DRBG performs health checks as per Section 11.3 of SP 800-90A.

The module does not implement CVL KDF self-tests.

If any of the tests listed above fail to complete successfully, the module enters into a critical error state where all cryptographic operations and output of any data is prohibited. An error message is logged for the CO to review and requires action on the CO's part to clear the error state.

2.9.2 Conditional Self-Tests

The cryptographic module performs the following conditional self-tests:

- Continuous DRBG Test
- Continuous NDRNG test for the non-approved NDRNG.
- RSA Pairwise Consistency Check (SIG (gen), SIG (ver), encrypt, decrypt). Implementations tested are PSS, PKCS1, X9.31.

2.10 Design Assurance

Source code and documentation are both managed and stored within SVN an automated configuration management system, and its associated server.

2.11 Mitigation of Other Attacks

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

3 Secure Operation

The IBM QRadar 7.2 module meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

Tamper evident labels and opacity baffles shall be installed for the module to operate in a FIPS Approved mode of operation.

The Crypto-Officer role is responsible for installing the tamper-evident labels, securing and having complete control over any unused labels, and maintaining and observing the labels to ensure that the module stays in a FIPS approved mode.

3.1 Initial Setup

When initialized and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

The following items must be installed to meet FIPS level 2 requirements. The Crypto-Officer must do the following:

- Install 4 formex adhesive material (baffles) over openings in the appliance, to meet opacity requirements.
- Install 24 tamper evident labels to ensure the appliance can show evidence of tampering.

  Note: The Crypto-Officer must record the unique number and location of each tamper evident label applied to the appliance. Refer to this record when inspecting the appliance for signs of tampering.

3.1.1 Obtaining Replacement Baffles and Tamper-Evident Labels

The Crypto-Officer can obtain additional baffles by ordering a FIPS Kit for the Mylar Labels, part number 5YKKK directly from Dell as a spare part.

The Crypto-Officer can obtain additional tamper evident labels by contacting the sales representative at the IBM Support Line and ordering a Serial Tamper Label Pack, part number 00FK877.

3.1.2 Installing Baffles

Use these annotated diagrams to install baffle material (formex adhesive sheeting) over the following four areas of the appliance.

Figure 3 – PCI Cover Install (Baffle 1 of 4)

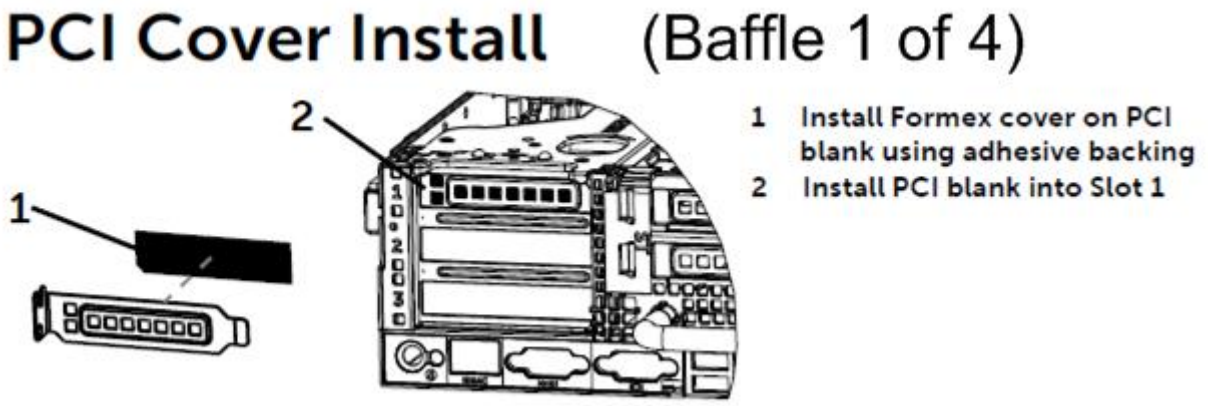


Figure 4 – NDC Cover Install (Baffle 2 of 4)

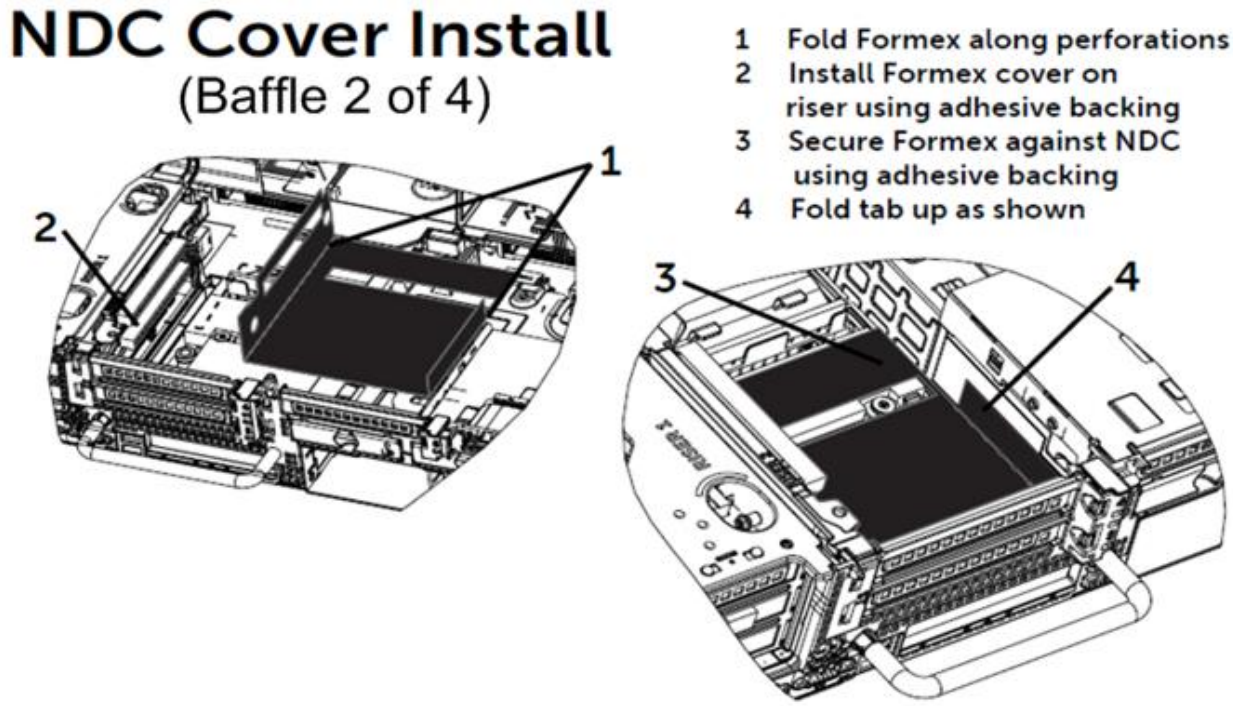


Figure 5 – VFlash Cover Install (Baffle 3 of 4)

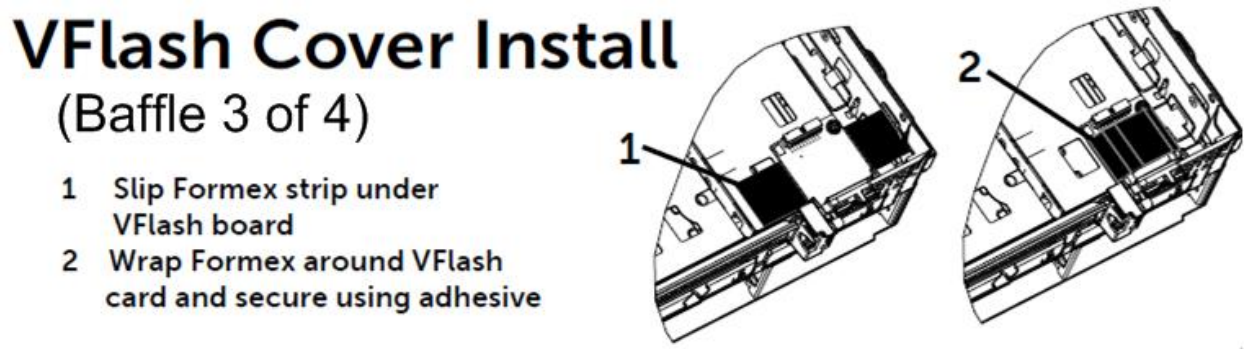
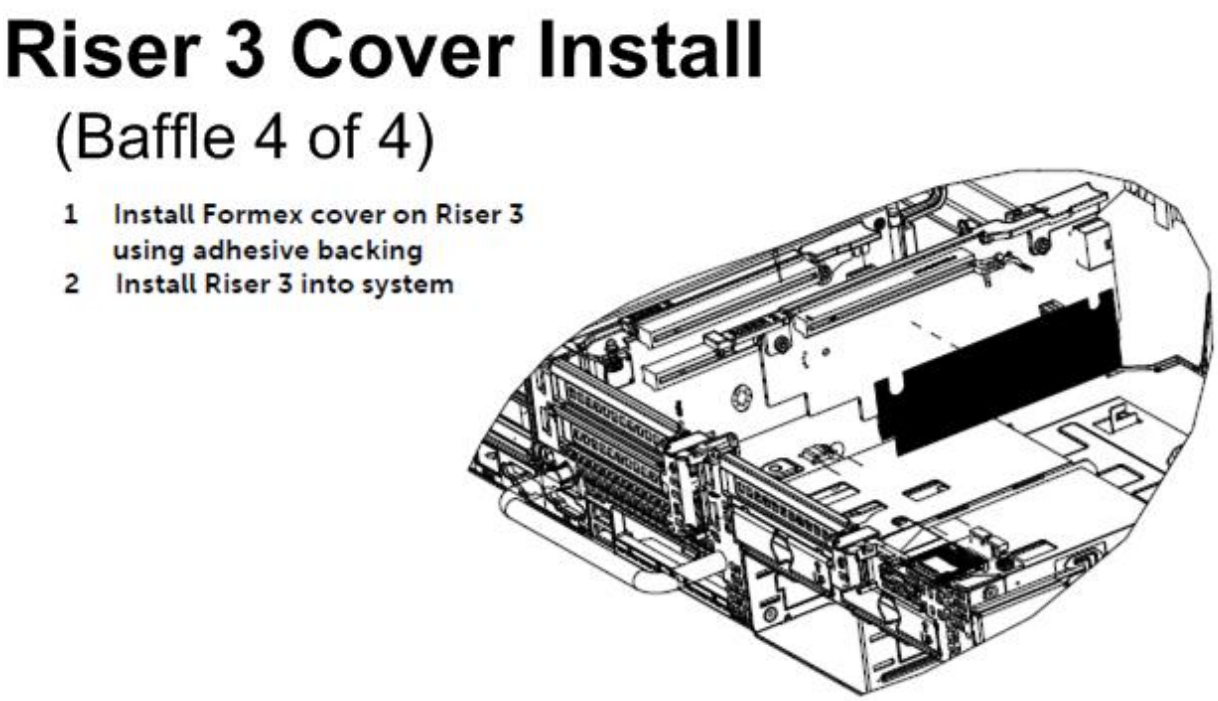


Figure 6 – Riser 3 Cover Install (Baffle 4 of 4)



3.1.3 Installing Tamper Evident Labels

Use these annotated diagrams to install the 24 tamper-evident labels to cover physical access points on the appliance.

Figure 7 – Top Cover Tamper Evident Labels 1 and 2 of 24.

Detail showing label covering the shell and cover.

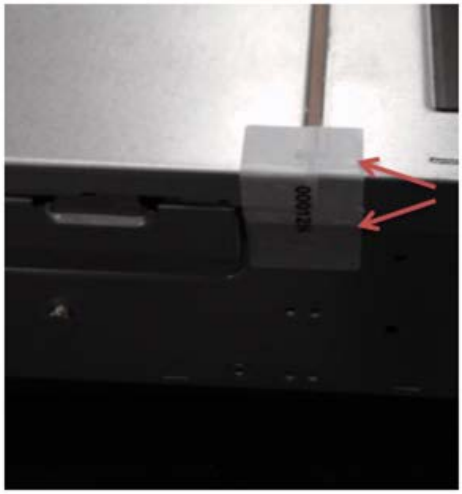


Figure 8 – Top Cover Tamper Evident Labels 3 and 4 of 24.

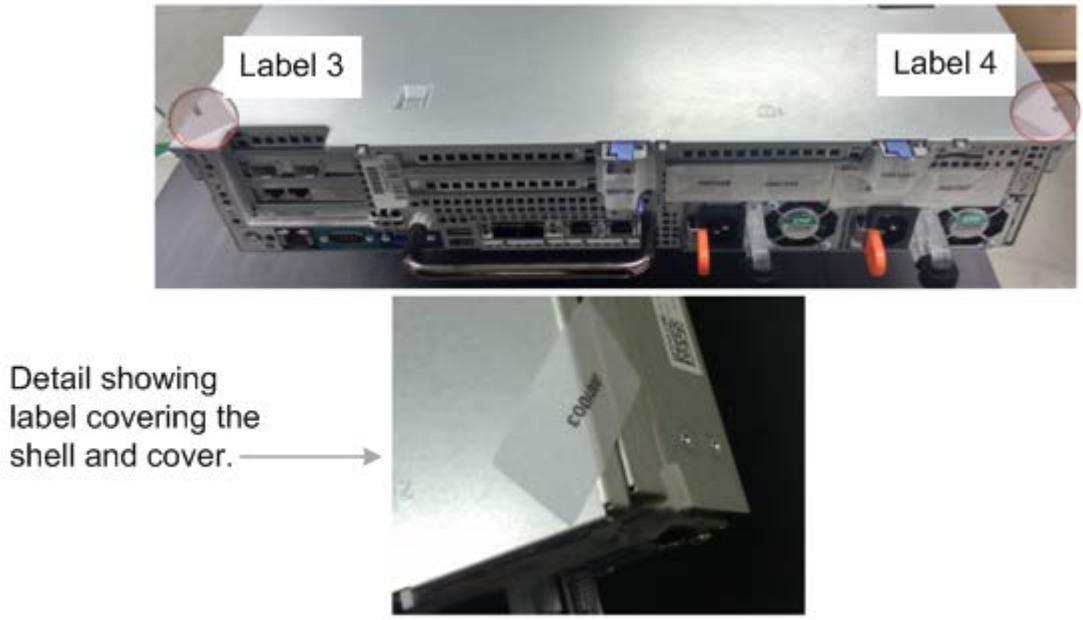


Figure 9 – Hard Disk Drive Tamper Evident Labels 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, and 16, of 24.

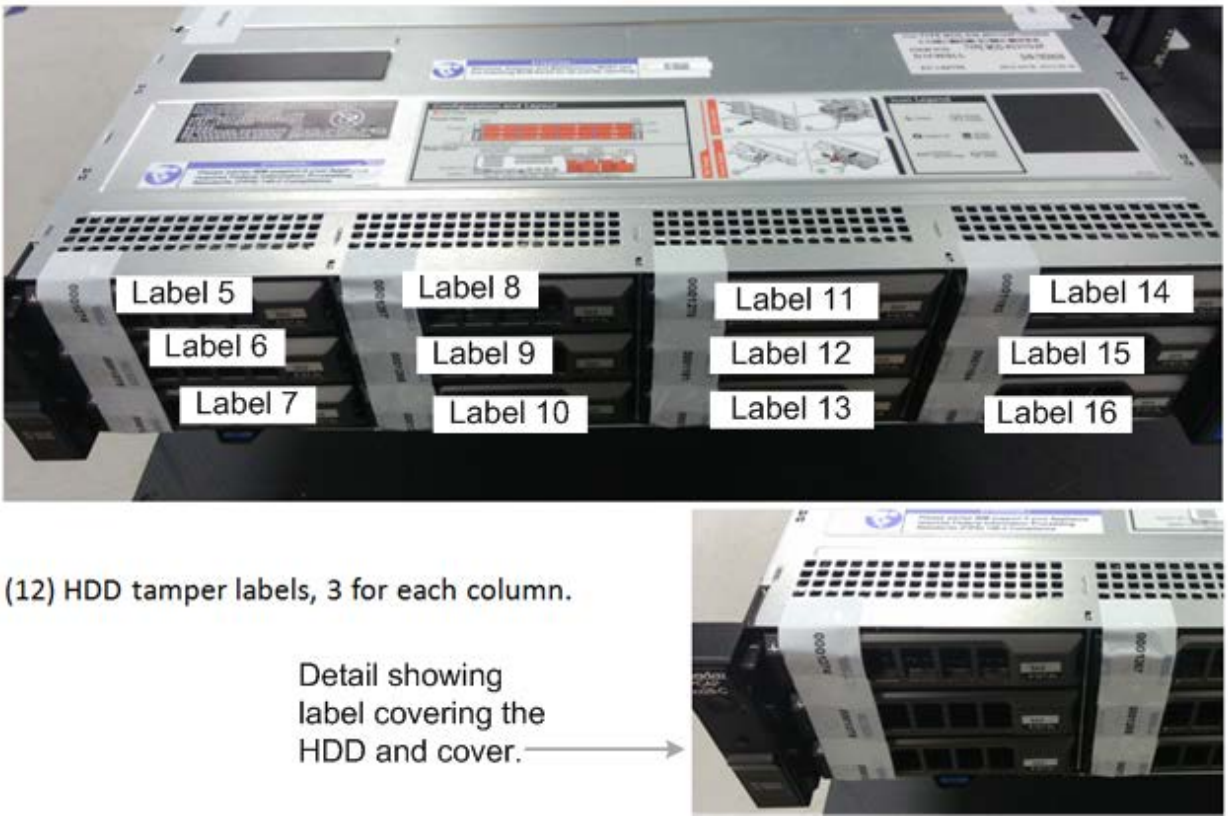


Figure 10 – Bezel Labels 17 and 18 of 24:

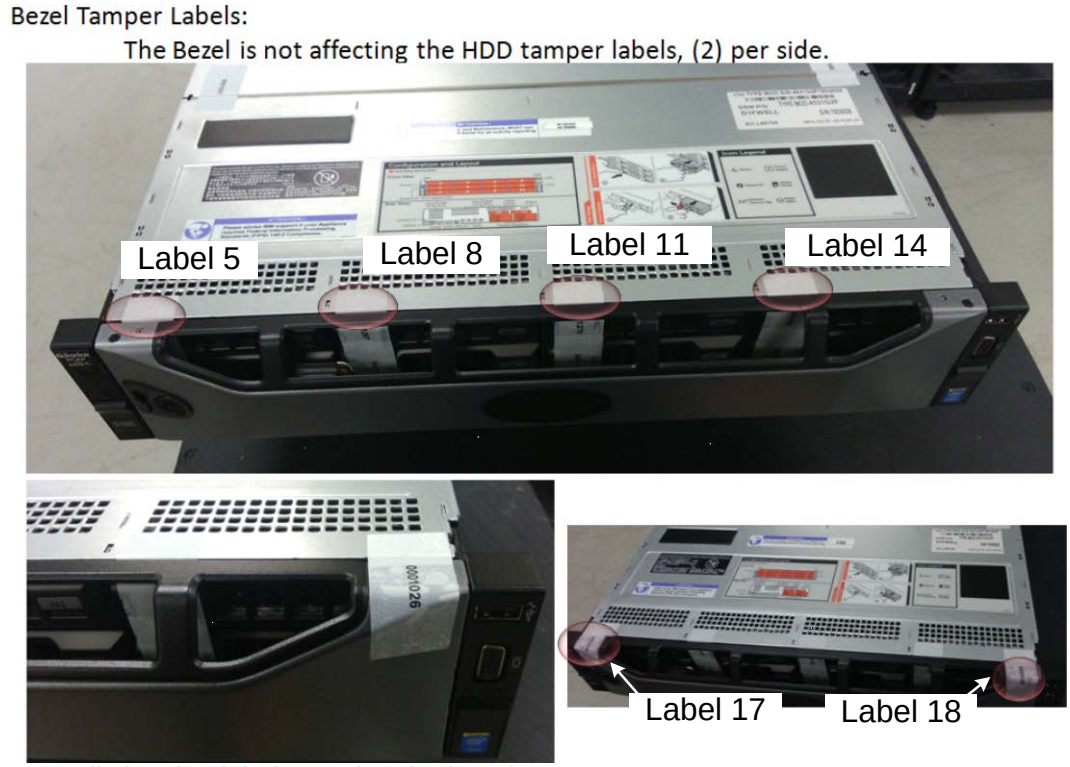
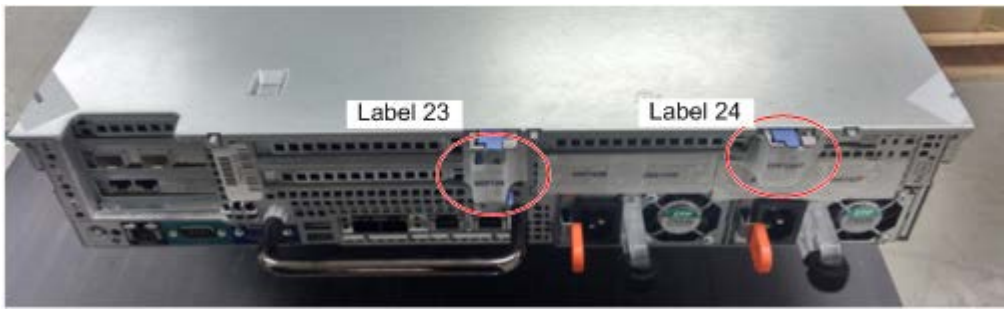


Figure 11 – Filler Labels 19, 20 21, and 22, of 24 (2) per filler:

Figure 12 – Cards Filler Tamper Labels: Labels 23 and 24 of 24:



Review the placement of all tamper-proof labels to ensure that all labels are firmly attached. The procedure is complete. The CO is now ready to continue installing the appliance.

3.2 Secure Management

This section provides guidance which ensures that the module is always operated in a secure configuration.

3.2.1 Initialization

After installing the baffles and tamper evident labels, the Crypto-Officer must use procedures in the IBM Security QRadar Version 7.2 FIPS 140-2 Installation Guide to set up and start the appliance. The procedures in the installation guide are also listed below:

Connect a notebook to the serial port on the rear of the appliance or connect a keyboard and monitor to their respective ports. If you use a notebook to connect to the system, you must use a terminal program, such as HyperTerminal, to connect to the system. Make sure that you set **Connect Using** to the appropriate COM port of the serial connector and **Bits per second** to 9600. You must also set **Stop Bits** (1), **Data bits** (8), and **Parity** (None).

1. Power on the system and login:
    a. Username: **`root`**

    Note: The username is case-sensitive.

    b. Press Enter.
    c. End User License Agreement (EULA) is displayed.
    d. Read the information in The End User License Agreement (EULA) window. Press the Spacebar to advance each window until you reach the end of the document. Type **yes** to accept the agreement, and then press Enter.

e. The activation key window is displayed. The activation key is a 24-digit, four-part, alphanumeric string that you receive with your FIPS appliance. Type the activation key and press enter.

   You can find the activation key printed on a sticker and physically placed on your appliance or it is included with the packing slip; all appliances are listed along with their associated keys.

2. Select normal for the type of setup. Select Next and press Enter
3. Select the Enterprise tuning template. Select Next and press enter
4. Choose one of the following options:
   a. Manual – Select this option to manually input the time and date. Select Next and press Enter. The current Date and Time window is displayed. Go to Step 5.
   b. Server – Select this option to specify your time server. Select Next and press enter. The enter Time Server window is displayed. Go to Step 6.
5. To manually enter the time and date, type the current time and date. Select Next and press Enter. Go to Step 9.
6. To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.
7. Select your time zone continent or area. Select **Next** and press Enter. The Time Zone Region window is displayed.
8. Select your time zone region. Select **Next** and press Enter.
9. Select an Internet Protocol version. Select **Next** and press Enter.
10. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
11. Choose one of the following options:
    a. If you are using IPv4 as your Internet Protocol, go to **Step 14**.
    b. If you are using IPv6 as your Internet Protocol, go to **Step 12**.
12. Choose one of the following options:
    a. To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended amount of time. Go to **Step 14**.
    b. To manually configure for IPv6, select **No** and press Enter. Go to **Step 13**.
13. To enter network information to use for IPv6:

a. In the **Hostname** field, type a fully qualified domain name as the system hostname.
b. In the **IP Address** field, type the IP address of the system.
c. In the **Email Server** field, type the email server. If you do not have an email server, type `localhost` in this field.
d. Select **Next** and press Enter. Go to **Step 15**

14. Configure the QRadar network settings:
15. Configure the QRadar root password:
    a. Type a password. Select **Next** and press Enter.
    b. Retype the password to confirm. Select **Finish** and press Enter. A series of messages are displayed as QRadar continues with the installation. This process typically takes several minutes.
16. Press Enter to select **OK**. The installation is complete. You are now ready to configure any additional appliances that are managed by the QRadar FIPS Console.
17. Install all of your QRadar appliances.
18. Add any managed hosts with the deployment editor from the **Admin** tab of your QRadar Console.
19. Save and deploy your configuration update on your QRadar Console. After you add managed hosts to your QRadar Console, you are ready to enable FIPS mode.
20. Use the command-line interface to enable FIPS mode on the QRadar appliance. When FIPS mode is enabled on a QRadar appliance, command-line interface access is restricted to the admin role or crypto user account. These accounts are created when enable FIPS mode for QRadar. SSH access is restricted to the FIPS admin and crypto user accounts.
    a. **Step 1** Using SSH, log in to QRadar as a root user.
    b. **Step 2** Type the following command:
       ```
       /opt/qradar/fips/setup/fips_setup.py --enable
       ```
       If any required cryptographic files are missing, the output alerts you to the missing files.
    c. **Step 3** Type **Yes** to enable FIPS mode.
    d. **Step 4** Type a password for the crypto user account.
    e. **Step 5** Retype the crypto password to confirm.
    f. **Step 6** Type a password for the admin user account.
    g. **Step 7** Retype the admin password to confirm.

h. **Step 8** Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is enabled.

3.2.2 Management

Check the tamper-evident labels regularly for signs of tampering and ensure the numbered labels are consistent with the record of label numbers and their locations. The record was created when the labels were applied. If any irregular activity is noticed or the module is consistently reporting errors, then IBM customer support should be contacted.

3.2.3 Zeroization

Use the zeroize command to zeroize cryptographic keys and return the module to the factory default configuration.

3.3 User Guidance

Only the module's cryptographic functionalities are available to the User. Users are responsible to use only the services that are listed in Table 5. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is noticed.

The User must not modify the configuration of the module as established by the Crypto-Officer.

4 References

The following National Institute of Standards and Technology publications are available at URL http://csrc.nist.gov/groups/STM/cmvp/index.html:

- *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*
- *FIPS 140-2 Annex A: Approved Security Functions*
- *FIPS 140-2 Annex B: Approved Protection Profiles*
- *FIPS 140-2 Annex C: Approved Random Number Generators*
- *FIPS 140-2 Annex D: Approved Key Establishment Techniques*
- *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* (a joint publication of the National Institute of Standards and Technology and Communications Security Establishment).
- *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197
- *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-3