Bomgar Corporation
Bomgar FIPS Remote Support Appliance
Module Firmware Version 4.4.2FIPS
Instance Firmware Version 16.2.1FIPS
Hardware Version R630

BOMGAR™

FIPS 140-2 Security Level: 2

Non-Proprietary Security Policy

TC:1/14/2019

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Bomgar FIPS Remote Support Appliance from the Bomgar Corporation. This Security Policy describes how the Bomgar FIPS Remote Support Appliance meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 – Security Requirements for Cryptographic Modules details the United States and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSE):https://csrc.nist.gov/projects/cryptographic-module-validation-program.

The Bomgar FIPS Remote Support Appliance is referred to in this document as the Bomgar Appliance, Bomgar FIPS Appliance, cryptographic module, or module.

1.2 References

This document deals with the operations and capabilities of the module only in technical terms of the *FIPS 140-2- Security Requirements for Cryptographic Modules* policy. More information is available about the module from the following sources:

- The Bomgar website at https://www.bomgar.com/fips contains information on the full line of products provided by the Bomgar Corporation.
- The CMVP website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Contacts contains contact information for individuals who can answer questions about the module.

1.3 Document Organization

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

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

This Security Policy and other validation submission documentation are produced by the Bomgar Corporation. Except for this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to the Bomgar Corporation and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact the Bomgar Corporation.

2 Bomgar Appliance

2.1 Overview

The Bomgar Corporation specializes in appliance-based solutions for remote support. The Bomgar FIPS Appliance (*shown in Figure 1*) gives support technicians secure remote control of computers over the internet, LAN, or WAN. The firmware works through firewalls without a pre-installed client on the remote computer. With Bomgar, a support technician can see the screen and control the system virtually as if physically present.

Figure 1 - Bomgar FIPS Appliance

The Bomgar Appliance allows for the use of remote support in a secure, integrated, and manageable fashion within multiple areas of an organization. Logging is performed by the Bomgar Appliance and allows for the review of all customer and support representative interactions, including playback of all desktop screen data. It integrates with leading systems management and identity management solutions, including an API for deeper integration. With Bomgar, support managers can create support teams, customize queues, and report on all support activity. Network administrators can monitor the Bomgar Appliance using Simple Network Management Protocol (SNMP)[1].

The Bomgar Appliance allows remote access to multiple common operating systems, including various Linux distributions. It enables remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, smartphones, and network devices.

The Bomgar Appliance works over internal and extended networks and is internet-accessible. This allows a support organization to reduce less effective means of support by driving requests through custom support portals hosted on the appliance. The Bomgar Appliance routes support requests to the appropriate technician or team and mediates connections between customers and support representatives, allowing the execution of chat sessions, file downloads, file uploads, remote control of desktops, screen-sharing, and system information access and diagnostics.

To enable the functionality described above, Bomgar has implemented an architecture that places the Bomgar Appliance at the center of all communications. *Please see Figure 2 for a typical deployment scenario*. The Bomgar Appliance provides a platform upon which one or more support sites are constructed. Sites represent individual help centers, and multiple sites can be configured to support multiple departments or groups in a company. Each site offers a website interface using Hypertext Transfer Protocol (HTTP) for unauthenticated services and HTTP over TLS (HTTPS) for authenticated services, in addition to accepting direct client connections over a protocol running on top of TLS.

[1]SNMPv3 protocol has not been reviewed or tested by the CAVP and CMVP.

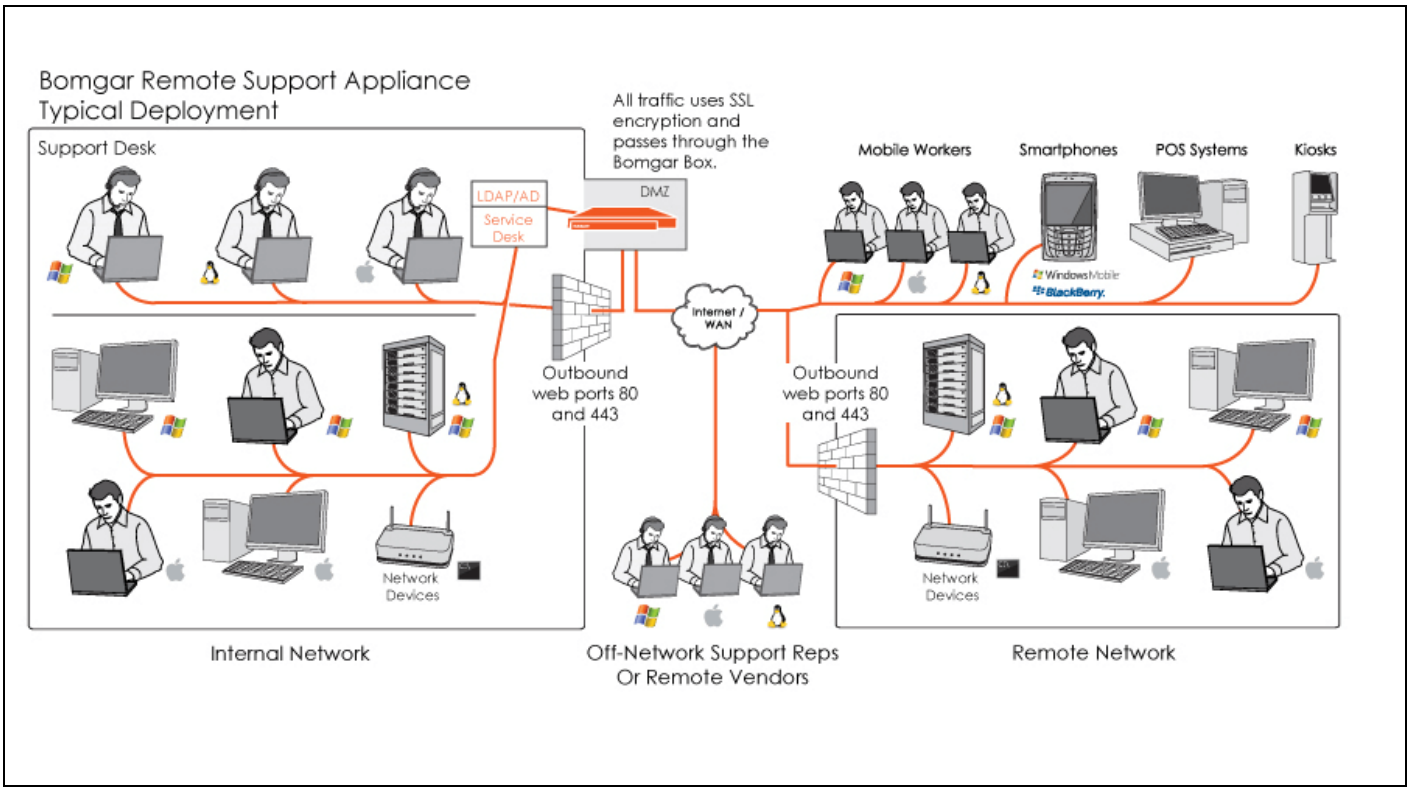


Figure 2 - Typical Deployment

The Bomgar Appliance has two firmware components which provide the appliance's functionality. The first is the module firmware and it provides system-level configuration of the Bomgar Appliance. Settings such as IP addresses and SSL/TLS configuration are all configured via the module firmware interface. The second firmware component is the instance firmware and it provides site-level configuration from the /login web interface, and is a repository for the remote client programs which users interact with. These remote client programs include the representative console, customer client, connection agent, and all other clients which are downloadable from the Bomgar Appliance and are executed outside of the module on external devices. These remote client programs are excluded components for this FIPS 140-2 validation.

The Bomgar Appliance is validated by the FIPS 140-2 Section levels shown in Table 1.

Table 1 - Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Modules 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 (EMI/ EMC)	2

Section	Section Title	Level
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Bomgar FIPS Appliance is a multi-chip standalone module that meets overall Level 2 FIPS 140-2 requirements. The appliance must be running the following firmware versions to be in compliance:

Firmware Version

- Module Firmware: 4.4.2FIPS
- Instance Firmware: 16.2.1FIPS

Hardware Version

- R630 - Appliance
- 720-1199-01 - Bezel Assembly, R630
- BMG-720-1214-00 - FIPS Conversion Kit and Bezel Logo Label, R630

Table 2 - FirmwareVersions

Physically, the module is composed of components for a standard server platform. Figure 3 shows a block diagram for the Bomgar Appliance and identifies various components, connections, and information flows. The cryptographic boundary of the module (denoted by the dotted lines in Figure 3) is defined by the outer case of the appliance, surrounding the complete set of hardware and firmware components.

Both Module and Instance firmware components reside in the HDD. All of the module code resides in the firmware. The remote client programs consist of code which is executable on external devices and is retrieved from the firmware on the HDD.

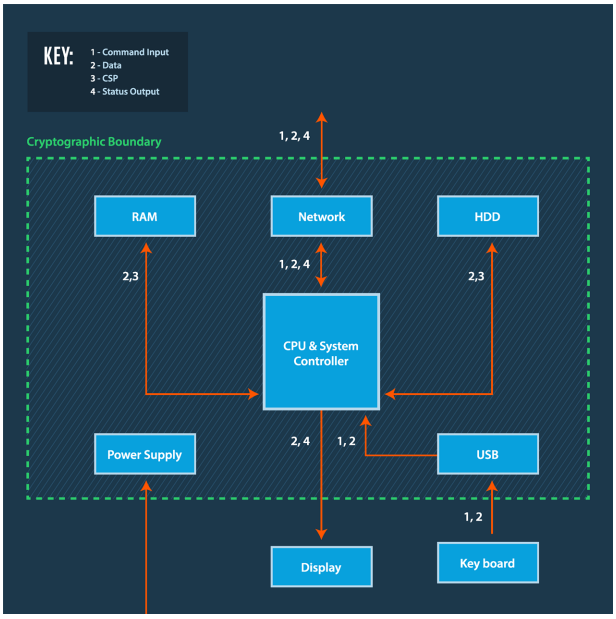


Figure 3 - Block Diagram with Cryptographic Boundary

2.3 Module Interface

The module's design separates the physical ports into four logically distinct and isolated categories. They are:

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

In addition, the module receives power via a defined power input interface.

Data input/output are the network data packets utilizing the services provided by the module. These packets enter and exit the module through the network ports. Control input consists of both configuration and administration data, entering the module through the web interface as well as the input for the Power and Reset buttons. Status output consists of status information relayed via the LED indicators and the web interface.

The physical ports and interface of the module are depicted in the Appendix.

- Network ports
- USB ports
- Power button
- Reset button
- Power connector(s)
- Power LED

The USB ports, serial port, and VGA port behind the rear port cover are inaccessible. These ports are excluded components for the FIPS 140-2 validation of the module.

The LCD display unit, USB ports, HDD LEDs, SD Card slot behind the front bezel are inaccessible. These components are also excluded from the FIPS 140-2 validation of the module.

Table 3 provides the mapping from the physical interface to the logical interface as defined by FIPS 140-2.

Table 3 - Physical Ports and Logical Interface

FIPS 140-2 Logical Interface	Bomgar Appliance Physical Port
Data Input	Network ports
Data Output	Network ports
Control Input	Network ports, Power button, and Reset button
Status Output	LEDs, Network ports
Power Input	Power connector(s)

The cryptographic module has a number of LEDs, which indicate the state of the module. The descriptions for the LEDs for the module are listed in Table 4.

Table 4 - LED Descriptions

Component	Indication	Status	Description
Power	LED[1]	On Off	System On System Off

2.4 Roles and Services

As required by FIPS 140-2, the module supports a Crypto-Officer (CO) role and a User role. The User role is comprised of an Instance-Admin role and an Instance-User role.

The module supports identity-based authentication for the Crypto-Officer as well as identity-based authentication for the Instance-Admin and Instance-User roles. The role for the Crypto Officer is provided explicitly on the /appliance site of the module and for the Instance-Admin and Instance-User on the /login site. All credentials established on /appliance assume the Crypto Officer role. Operators explicitly assume the role of Instance-Admin or Instance-User based on the authentication credentials employed on /login. The credentials used determine the services available to the operator.

2.4.1 Crypto-Officer Role

The Crypto-Officer role is an administrator for the module and is responsible for the initial setup and configuration. The Crypto-Officer has administrative rights to monitor and manage the module firmware component's configuration, to manage the CO account, and to reset the default Instance-Admin account passwords. It is assumed when logging into /appliance with the default admin identity or any configured identity on /appliance.

2.4.2 Instance-Admin Role

The Instance-Admin has administrative rights to monitor and manage the instance firmware's configuration, to manage Instance-Admin accounts, and to manage Instance-User accounts.

2.4.3 Instance-User Role

The Instance-User can access the support services in the module based on the permissions set by the Instance-Admin. The Instance-Admin must grant access to Instance-Users to access services on the module.

2.4.4 Services

All services available in FIPS mode are also available in non-FIPS mode.

Services provided to authenticated operators are listed in Table 5. Please note that the keys and Critical Security Parameters (CSPs) listed indicate the type of access required:

- Generate: The module generates or derives the CSP.
- Read: The CSP is read from the module (CSP output).
- Execute: The module executes using the CSP.
- Write: The CSP is written to the module (CSP entry).
- Zeroize: The module destroys the CSP.

Table 5 - Mapping of Authenticated Operator Services to Inputs, Outputs, CSPs, and Type of Access

[1]Only the Power LED is visible under the tamper-evident front bezel.

Service	Description	Operator	Input	Output	CSP and Type of Access
Manage Bomgar Appliance settings	Configure IP and TLS settings	CO	Command	Command response	TLS public key – Read, Write, Execute, Zeroize, Generate TLS private key – Read, Write, Execute, Zeroize, Generate Session key – Read, Write, Execute Session integrity key – Read, Write ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize CO Password – Read Firmware update key – Read, Write, Execute
Manage CO account	Manage CO account password	CO	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize CO Password – Read, Write

Service	Description	Operator	Input	Output	CSP and Type of Access
Reset Instance-Admin password	Reset Instance-Admin account password	CO	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize Instance-Admin Password – Write
Configure Instance-Admin accounts	Set up and monitor Instance- Admin accounts	CO, Instance-Admin	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize Instance-Admin Password – Read, Write

Service	Description	Operator	Input	Output	CSP and Type of Access
Configure Instance-User accounts	Set up and monitor Instance-User accounts	Instance-Admin, Instance-User	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize Instance-User Password – Read, Write
Execute self-tests	Perform power-up self-tests on demand	CO	Command	Command response	None
Monitor status	Monitor the status of the module	CO	Command	Status information	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize
Zeroize keys	Zeroize plaintext keys	CO	Command	Command response	All CSPs – Write, Zeroize

Service	Description	Operator	Input	Output	CSP and Type of Access
Perform Representative Console service	Access and perform services for representative consoles	Instance-Admin, Instance-User	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - REad, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize Instance-Admin Password – Read Instance-User Password – Read
Manage instance settings	Manage instance configuration settings	Instance-Admin, Instance-User	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - REad, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize

Service	Description	Operator	Input	Output	CSP and Type of Access
Update Firmware	Install new firmware package	CO	Command	Command response	TLS public key – Read, Execute TLS private key – Read, Execute Session key – Read, Write, Execute Session integrity key – Read, Write, Execute ECDH private key - Read, Generate, Write, Execute, Zeroize ECDH public key - Read, Generate, Write, Execute, Zeroize ECDH Shared Secret - Read, Generate, Execute, Zeroize CO Password – Read Firmware update public key – Read, Write, Execute

2.4.5 Unauthenticated Operator Services

The module provides a service to unauthenticated operators as listed in Table 6.

Table 6 - Unauthenticated Operator Services

Service	Description	Input	Output	CSP and Type of Access
Generate nonce	Generate a nonce to prevent replay attacks via web browser	Command	Command response	None
Start an unauthenticated support session	An unauthenticated user requests support service	Command	Command response	None
Power-up self-tests and module state monitoring	Power cycle the module by pressing the Power button to initiate power-up self-tests	Press the Power button	LEDs show state	None

2.4.6 Authentication Mechanism

The module supports identity-based authentication for the Crypto-Officer as well as identity-based authentication for the Instance-Admin and Instance-User roles. Operators explicitly assume the role of Crypto Officer when logging in with either the default or established credentials on /appliance. Multiple identities may be created on /appliance which assume the Crypto Officer role. Operators explicitly assume the role of either Instance-Admin or Instance user based on the authentication credentials employed on /login. The credentials used determine the services available to the operator.

The Crypto-Officer can access the module remotely over a TLS session. The Crypto-Officer authenticates to the module, using a user ID and password. Instance-Admins and Instance-Users authenticate themselves with a user ID and password combination.

Table 7 lists the authentication mechanisms used by the module.

Table 7 - Authentication Mechanism Used by the Module

Authentication Type	Strength
Password	Passwords are required to be a minimum of eight (8) characters in length and can be a maximum of 64 characters in length. Numeric, alphabetic, upper and lower cases, and keyboard/extended characters can be used for a total of 95 character choices. An eight (8) character password yields a total of 6.6342043e+15 possible combinations. Any failed authentication attempt results in at least one second delay in response. Hence, there cannot be more than 60 invalid attempts in any given minute. The probability of a random attempt succeeding or a false acceptance occurring is 60 x 1/ 6.6342043e+15. This is lower than the minimum acceptable probability of one in 1,000,000 (and one in 100,000 per minute) that a random attempt will succeed or false acceptance will occur.

2.5 Physical Security

The Bomgar Appliance is a multi-chip standalone cryptographic module. It is enclosed in a hard and opaque metal case that completely encloses all internal components of the module. Tamper-evident labels are applied to the cases to provide physical evidence of attempts to gain access to the module's internal components. The module's components are production grade. The placement of tamper-evident labels can be found in Section 3.1.1 of this document.

2.6 Operational Environment

The operational environment requirements do not apply to the Bomgar Appliance. The module provides only a limited operational environment, and it does not provide a general-purpose operating system environment.

2.7 Cryptographic Key Management

The following table shows the CAVS certificates and their associated information of the cryptographic implementation in FIPS mode.

Table 8 - Algorithms

FIPS-Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli (in bits)	Use
#4767	AES	[FIPS197], [SP800-38A] [SP800-38D]	CBC, CTR, GCM[1]	128, 192, 256	Data Encryption and Decryption
#1411	CVL ECC CDH Primitive	[SP800-56A] Section 5.7.1.2	N/A	P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571	EC Diffie-Hellman Key Agreement
#1648	DRBG	[SP800-90A]	CTR_DRBG: AES-256 with/ without DF, without PR	N/A	Deterministic Random Bit Generation

[1]The module generates the IV deterministically as per guidance in SP800-38D section 8.2.1. It is compatible with TLSv1.2 and supports acceptable GCM ciphers suites from SP 800-52 Rev. 1, Section 3.3.1. In accordance with IG A.5, the module compares the client_write_key and the server_write_key. If the client_write_key and server_write_key are the same, the session is aborted. The GCM implementation keeps a 64-bit counter which is checked for a wrap on invocation. If the counter wraps, the module triggers the handshake and establishes a new encryption key.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli (in bits)	Use
#1196	ECDSA[1], [2] [3]	[FIPS 186-4]	Key Pair Generation	P-256 P-384	Private and Public Key Generation
			Signature Generation	B-233 B-283 B-409 B-571 K-233 K-283 K-409 K-571 P-224 P-256 P-384 P-521 with SHA SHA-224 SHA-256 SHA-384 SHA-512	Digital Signature Generation
			Signature Verification	B-163 B-233 B-283 B-409 B-571 K-163 K-233 K-283 K-409 K-571 P-192 P-224 P-256 P-384 P-521 with SHA SHA-224 SHA-256 SHA-384 SHA-512	Digital Signature Verification

[1]Public Key Verification was tested but not used by the module.

[2]SigVer B-163, K-163, and P-192 are for Legacy Use Only.

[3]ECDSA key pairs (P-256, P-384) are generated using values from the Approved DRBG as seed materials of asymmetric key generation. Seed generation is vendor affirmed to comply with SP 800-133.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli (in bits)	Use
#3180	HMAC	[FIPS 198-1]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	112 or greater	Message authentication code
#2608	RSA[1] [2]	[FIPS 186-4]	Key Pair Generation	2048 3072	Private and Public Key Generation
			Signature Generation with PKCS#1v1.5 and PSS	2048 3072 with SHA SHA-224 SHA-256 SHA-384 SHA-512	Digital Signature Generation
			Signature Verification with PKCS#1v1.5 and PSS	1024[3] 2048 3072 with SHA SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	Digital Signature Verification
#3912	SHS	[FIPS 180-4]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	N/A	Message Digest

[1]RSA SigVer 1024 or SHA-1 is for Legacy Use Only.

[2]RSA key pairs (2048-bit, 3072-bit) are generated using values from the Approved DRBG as seed materials of asymmetric key generation. Seed generation is vendor affirmed to comply with SP 800-133.

[3]1024-bit key is CAVS tested in RSA Signature Verification for legacy use.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli (in bits)	Use
#1546	CVL TLS v1.2 KDF *TLS protocol has not been reviewed or tested by the CAVP and CMVP per IG D.11.	[SP800-135 rev 1]	N/A	N/A	Key Derivation
AES #4767 HMAC #3180	KTS[1]	SP 800-38F Section 3.1			TLS key pair import and export over TLS session

Allowed Algorithms

Allowed Algorithms	Caveat	Use	Reference
EC Diffie-Hellman	Key agreement provides 128 or 192 bits of encryption strength.	Key agreement within TLS protocol	CVL Cert #1411
NDRNG	The module generates cryptographic keys whose strengths are modified by available entropy.	Seeds the DRBG	SP 800-90A
RSA Key Wrapping	Key establishment methodology provides between 112 and 150 bits of encryption strength for RSA public and private keys of length 2048, 3072, and 4096.	Session key transport within TLS protocol	

Non-Approved Algorithms in Non-FIPS Approved Mode

Algorithm	Use	Reference
ECC CDH (B-163, K-163, P-192)	Key Generation	FIPS 186-4
ECC Key Generation (B-163, K-163, P-192)	Key Generation	FIPS 186-4
ECDSA PKG: CURVES (B-163, K-163, P-192 with all SHA-1, 224, 256, 384, 512) and (B-233, B-283, B-409, K-233, K-283, K-409. P-224, P-256, P-384, P-521 with SHA-1)	Key Generation and Verification	FIPS 186-4

[1]Key Wrapping: Key establishment methodology provides 128 or 256 bits of encryption strength.

Algorithm	Use	Reference
RSA Cryptographic Primitives with Size Less than 2048 bits	Encryption and Decryption	PKCS1
RSA with Non-Approved size 1024 bits	Signature Generation	FIPS 186-4

The module supports the CSP listed in Table 9.

Table 9 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation/ Input	Output	Storage	Zeroization	Use
TLS private key (SGK)	ECDSA key - (curves P-256 & P-384) or RSA private key - 2048, 3072, or 4096-bit	Internally generated or imported via a secure TLS session	Exits only via a secure TLS session	Hard disk in plaintext	By command or overwritten by another key or by factory reset	Server Authentication for TLS sessions Signature generation and verification
TLS public key	ECDSA key - (curves P-256 & P-384) or RSA public key - 2048, 3072, or 4096-bit	Internally generated or imported via a secure TLS session	Exits in plaintext form	Hard disk in plaintext	By command or overwritten by another key or by factory reset	Key exchange for TLS sessions Signature generation and verification
Session key	AES 128-bit key AES 256-bit key	Internally derived	Never exits the module	Resides on volatile memory only in plaintext	By power cycle or session termination	Data encryption and decryption for TLS sessions
Session integrity key	HMAC key (256 bits or 384 bits)	Internally derived	Never exits the module	Resides on volatile memory only in plaintext	By power cycle or session termination	Ensure authenticity of encrypted TLS session data
Crypto-Officer password (please see note below)	eight (8) character minimum password	Enters the module in encrypted form	Never exits the module	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the CO
Instance-Admin password	eight (8) character minimum password	Enters the module in encrypted form	Never exits the module	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the Instance-Admin

CSP	CSP Type	Generation/ Input	Output	Storage	Zeroization	Use
Instance-User password	eight (8) character minimum password	Enters the module in encrypted form	Never exits the module	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the Instance-User
DRBG entropy input[1]	Output of NDRNG (384-bit)	Internally generated	Never exits the module	Resides in volatile memory	By power cycle, session termination, or factory reset	Provides entropy for the DRBG
DRBG internal state	V (128-bit) Key (256-bit)	Internally generated	Never exits the module	Resides in volatile memory	By power cycle or factory reset	Generate random numbers
Firmware update key[2]	4096-bit RSA public key (SVK)	Generated by Bomgar Corp. and enters the module in encrypted form	Never exits the module	Hard disk in plaintext	Overwritten by another key distributed by Bomgar Corp.	Used to verify the authenticity (signature) of module firmware updates
TLS EC Diffie-Hellman Private Key	ECDH key (curve P-256)	Internally generated	Never exits the module	Resides in volatile memory only in plaintext	By power cycle or session termination	The private component used in ECDH exchange
TLS EC Diffie-Hellman Public Key	ECDH key (curve P-256)	Internally generated	Exits in plaintext	Resides in volatile memory only in plaintext	By power cycle or session termination	The public component used in ECDH exchange
TLS EC Diffie-Hellman Shared Secret	ECDH key (curve P-256)	Generated in ECDH	None	Resides in volatile memory only in plaintext	Power cycle and session termination	The shared exponent used in ECDH exchange
Saved Entropy Pool	512-bit random data	Internatlly generated before shutdown or reboot	Never exits the module	Hard disk in plaintext	Overwritten by another 512-bit random data at shutdown or reboot, by factory reset	Mixes with the entropy pool at start up

Note: Note: *The module comes pre-loaded with a default password. The Crypto-Officer is prompted to change this password before proceeding with any configuration steps.*

2.8 EMI/ EMC

The module was tested and found conformant to 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).

[1]The DRBG entropy input is provided by output of the NDRBG and contains minimum entropy of 384-bits.

[2]The firmware update key is initially loaded at factory and may be updated by a firmware update.

2.9 Self-Tests

2.9.1 Power-Up Self-Tests

The Bomgar Appliance performs the following self-tests when powering up to verify the integrity of the firmware and to verify that correct operation of the FIPS-Approved algorithm implementations was employed by the module:

- Firmware integrity check using a SHA-256 EDC
- AES Known Answer Test: Encrypt KAT
- AES Known Answer Test: Decrypt KAT
- ECDH Shared Secret KAT
- ECDSA PCT (sign/verify)
- RSA Sign KAT
- RSA Verify KAT
- HMAC KATs (SHA-1, SHA-256, and SHA-512)
- DRBG (instantiate/generate/reseed/health test)

If any of the power-up self-tests fail, then the module enters an error state, logs the error to a file, and disables all cryptographic operations.

2.9.2 Conditional Self-Tests

The Bomgar Appliance performs the following conditional self-tests:

- The module performs conditional self-tests on the output of NDRNG to ensure that consecutive random numbers do not repeat and performs DRBG health tests as defined in section 11.3 of [SP800-90A]. The module also does detection for stuck fault.
- RSA pair-wise consistency check (sign/verify and encrypt/decrypt): Verifies a newly generated key pair works properly.
- ECDSA pair-wise consistency check (sign/verify): Verifies a newly generated key pair works properly.
- Upgrade packages containing an SHA-256 digest of the firmware. It is digitally signed using RSA-4096 with SHA-512. The upgrade package is only loaded once the digital signature has been verified.

If any of the conditional self-tests fail, the module enters a soft error state until the error is cleared.

2.10 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 Bomgar Appliance meets Level 2 requirements for FIPS 140-2. The sections below describe how to ensure that the module is running securely.

3.1 Bomgar Appliance Label Inspection

The Bomgar Appliance with tamper-evident label kit – BMG-720-1214-00 FIPS Conversion Kit and Bezel Logo Label, R630– and front bezel –720-1199-01 Bezel Assembly, R630– is shipped from the factory with six (6) labels. Four (4) labels, *shown in Photos 1-4*, are pre-applied at factory. Two (2) labels, *shown in Photos 5-9*, are to be applied by the Crypto-Officer on the top of the chassis exactly 6.5 inches (165 mm) from the right edge and bottom of the chassis exactly 7.87 inches (199 mm) from the left edge, overlapping the front bezel. Upon delivery, the Crypto-Officer should ensure that the module was not tampered with during shipment and that the labels have been applied properly. Also, tamper-evident labels are routinely inspected for damage by the Crypto-Officer. If the Crypto-Officer finds a label that is questionable in appearance, they should contact Bomgar Support toll-free at 1 877 826 6427 x2 or internationally at +01 601 519 0123 x2. If any additional labels are needed, they should contact Bomgar Support toll-free at 1 877 826 6427 x2 or internationally at +01 601 519 0123 x2 with BMG-720-1214-00 FIPS Conversion Kit, R630. The Crypto-Officer is also responsible for securing and having control of the additional tamper-evident labels at all times.

IMPORTANT!IMPORTANT

The tamper-evident labels, front bezel label, and front bezel shall be installed for the module to operate in the approved mode of operation.

1. Inspect all tamper-evident labels that are shipped pre-applied to the Bomgar Appliance chassis, ensuring that each label does not show any signs of tampering and is placed properly. Any attempt to reposition or remove the label results in the voiding of that label and leaves a residue on the surface. If you find a label that is questionable in appearance, contact Bomgar Support toll-free at 1 877 826 6427 x2 or internationally at +01 601 519 0123 x2.
2. To apply the front bezel labels, clean the top and bottom surfaces and front bezel of the appliance with isopropyl alcohol in the areas where the tamper-evident labels are being placed.
3. While holding the labels by the edges, separately place the labels on the surfaces in the locations described above (and as depicted in Photos 6 and 7).
4. Apply the included tamper-evident labels by rubbing gently across the entire label to ensure adhesion to the surface.

   Note: Note: *Any attempt to reposition or remove the label results in the voiding of that label and leaves a residue on the surface.*

5. Allow the labels to fully adhere to the appliance for 24 hours in a physically secure environment before placing the appliance in the intended environment.

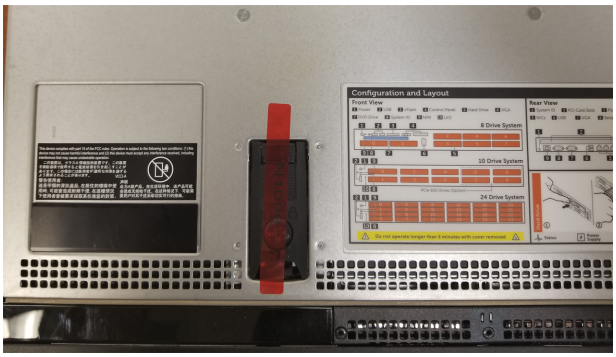


Photo 1

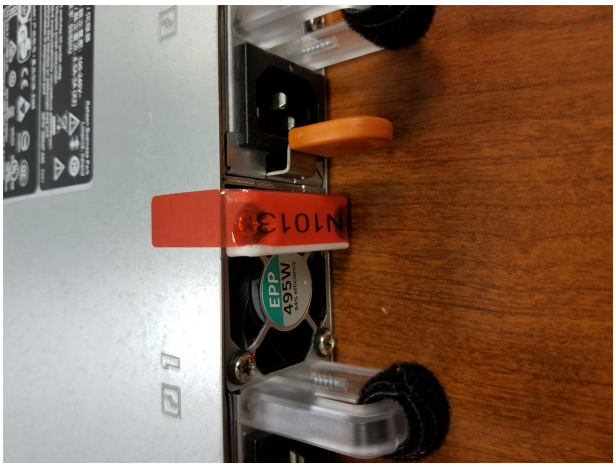


Photo 2

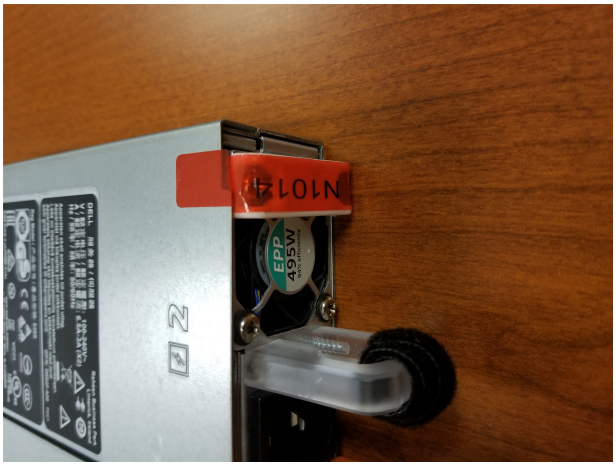


Photo 3

Photo 4

> ***Note: Note:*** *Labels depicted in Photo 5 are to be applied by the Crypto-Office. Photos 6,7,8, and 9 depict the exact location where the labels should be applied. The labels are to be applied by the Crypto-Officer on the top of the chassis exactly 6.5 inches (165 mm) from the right edge and bottom of the chassis exactly 7.87 inches (199 mm) from the left edge, overlapping the front bezel.*

Photo 5

> ***Note: Note:*** *Labels depicted in Photo 5 are to be applied by the Crypto-Officer.*

Photo 6 *(6.5 inches or 165 mm from the right edge; top of the chassis)*

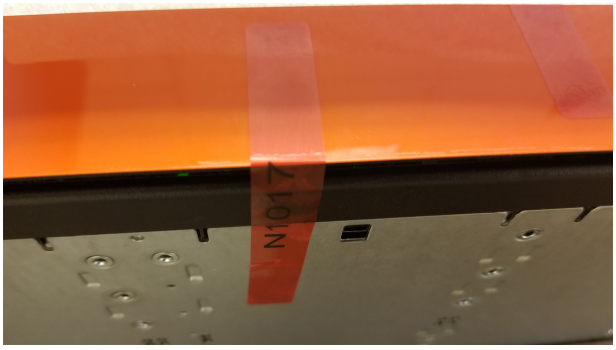


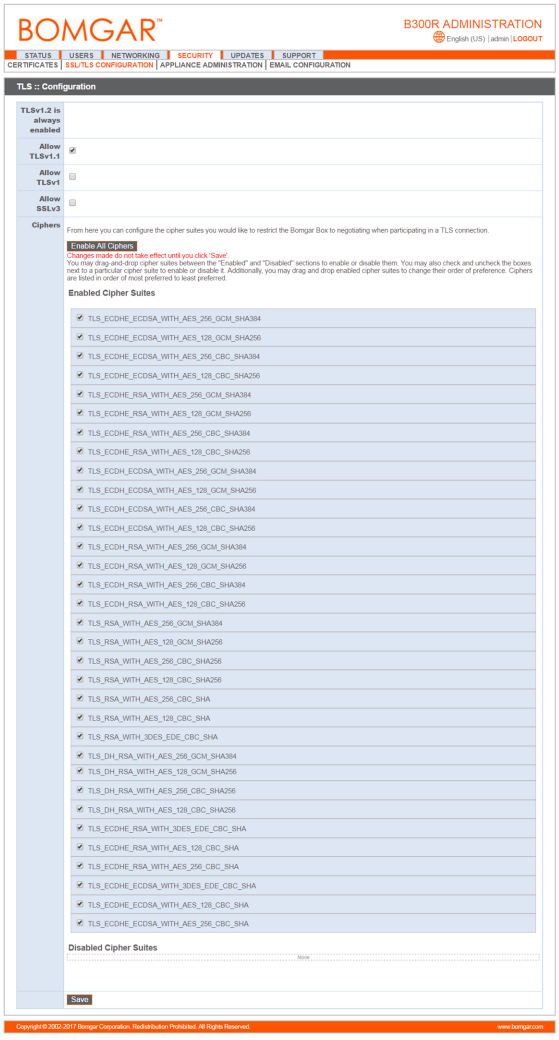
Photo 7 *(7.87 inches or 199 mm from the left edge; bottom of the chassis)*

Photo 8 *(Front view of both labels)*

Photo 9 *(Titled View of both labels)*

3.1.1 Bomgar Appliance FIPS Mode Configuration

Once all necessary initialization procedures have been performed as described in the preceding sections, the module needs to be configured to comply with FIPS 140-2 requirements. Once configured as described in this section, the module is considered to be in FIPS-Approved mode. This can be verified at any time by viewing the **IP Configuration** page and the **SSL Configuration** page and ensuring they match the images below.



FIPS-Approved Mode Configuration

Log into the Bomgar Appliance /appliance Administrative Interface (e.g., support.example.com/appliance) and configure your settings as described below:

1. Navigate to **Networking>IP Configuration**.
2. Click **169.254.1.1** IP address to edit.
3. Set the **Telnet Server** setting to **Simplified**.
4. Click **Save Changes** to commit these configuration changes.
5. Navigate to **Security>SSL Configuration**.
6. Disable SSLv3 by ensuring that the **Allow SSL v3** checkbox is cleared.
7. Disbale TLS 1.0 by ensuring that the **Allow TLSv1** checkbox is cleared.
8. Disable TLS 1.1 by ensuring that the **Allow TLSv1.1** checkbox is cleared.
9. Ensure that only cipher suites using FIPS-Approved algorithms are enabled:
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

10. Click **Save** to commit these configuration changes.
11. Navigate to **Status>Basics** and click **Reboot This Appliance**.

3.1.2 Firmware Version Verification

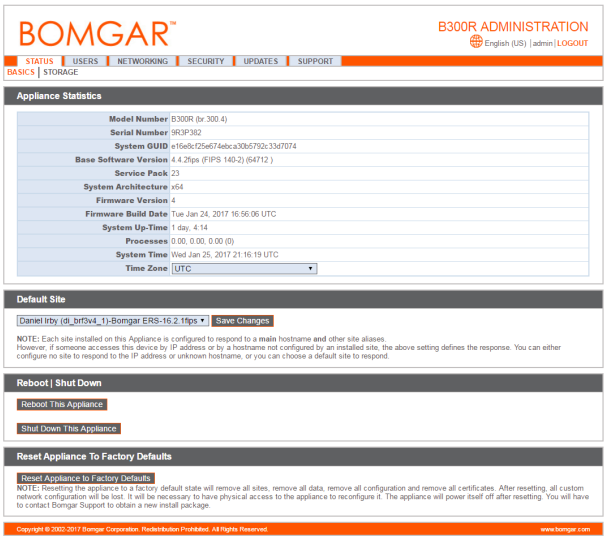
To ensure the module is running validated firmware versions, operators should compare the running versions to those documented in the Security Policy. To view the module firmware version, an operator must visit the /appliance site, the interface used by the Crypto-Officer. To view the instance firmware version, an operator must visit the /login site, which requires the credentials of the Instance-Admin role. Upon signing in, both display the Status page by default, which shows the version number.

3.2 FIPS Mode Compliance

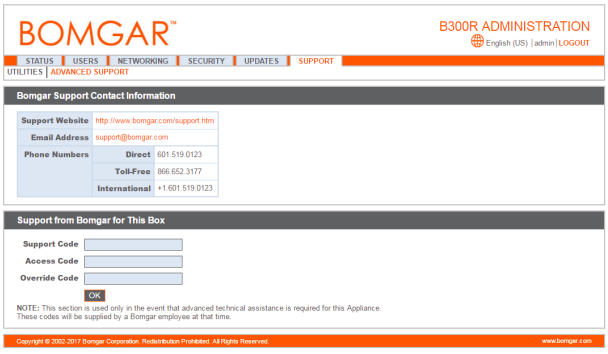
Any time the module deviates from the configuration detailed in Section 3.1.2 above, the module is considered to be in a non-FIPS-Approved mode of operation.

Additionally, the guidance provided must be followed to ensure that the module remains in a FIPS-Approved mode of operation. Failure to do so results in non-compliance.

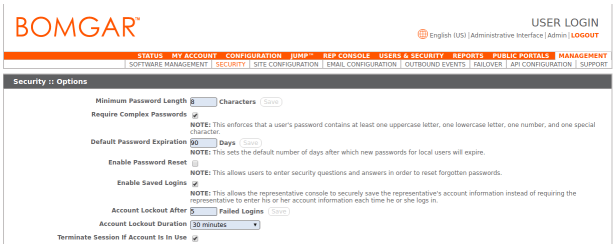
- When entering OR leaving FIPS-Approved mode, navigate to **Status > Basic** in the /appliance interface and clear all existing CSPs by clicking **Reset Appliance to Factory Defaults**.
- Never install firmware versions other than those listed on the cover page of this security policy. Only the firmware versions listed are considered part of the validated configuration.

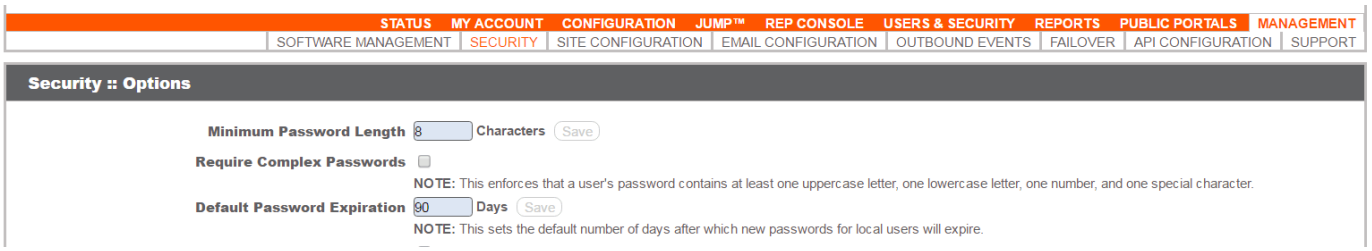


- When using the module's administrative interface, do not use the **Support > Advanced Support** in the /appliance interface. This action results in non-compliance.

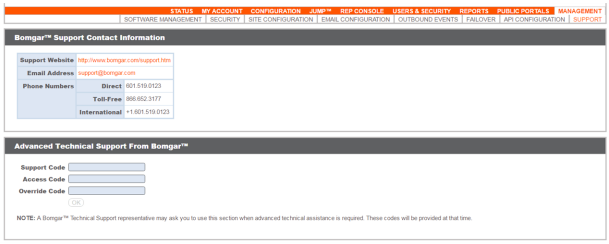


- Enforce minimum password requirements for the Instance-Admin and Instance-User roles by navigating to **Management > Security** in the /login interface.

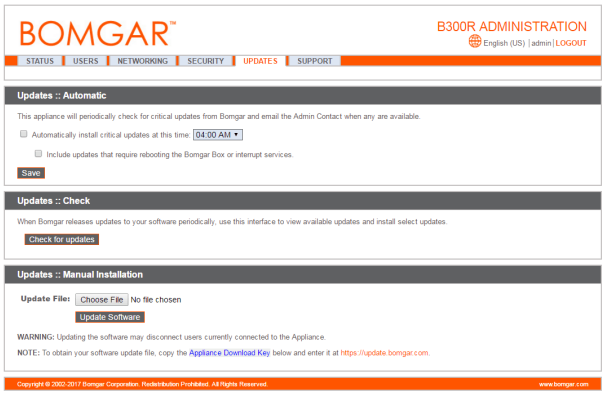




- When using the management interface, do not use the **Management>Support** page in the /login interface.



- Never install a Bomgar firmware package through the **Management > Software Management** page in the/login interface. Instead, ensure that any received Bomgar fimrware packages are FIPS-Approved and upload them from **Support >Updates** in the /appliance administrative interface (e.g. support.example.com/appliance). You should always upload updates manually rather than using the auto-update feature. Do not use the **Updates::Check > Check for Updates** functionality. To maintain compliance, only the firmware update versions listed in this Security Policy are to be used. Any firmware packages uploaded to this interface are still subject to the conditional test mentioned in 2.9.2.



3.3 Crypto-Officer Guidance

The Crypto-Officer can initiate the execution of self-tests and can access the module's status reporting capability. Self-tests can be initiated at any time by power cycling the module.

3.3.1 Management

It is the responsibility of the Crypto-Officer to ensure that the module is setup to run securely. Please refer to Section 3.2 above for guidance that the Crypto-Officer must follow for the module to be considered in a FIPS-Approved mode of operation. Additionally, the Crypto-Officer should be careful to protect any secret/private keys in their possession.

For details regarding the management of the module, please refer to the appropriate Bomgar Appliance Administrative Interface Guide.

3.3.2 Status Monitoring

Error message and status review are the responsibility of the Crypto-Officer. When any module self-tests fails, the module reports an error message which can be viewed over a network connection. This connection is set, under N**etworking > IP Configuration**

under the **Networking** tab. Issuing the command **telnet [ip-address-assigned-to-network-port]** brings up the following options:

1. Show error message
2. Shutdown the device
3. Reboot the drive
4. Reset the device to factory default
5. Done

Issuing the **Show Error Message** command displays the reported error message.

3.3.3 Zeroization

Session keys are zeroized at the termination of the session but are also cleared when the module is power-cycled. All other CSPs may be zeroized by either:

- Issuing the **Reset Appliance to Factory Defaults** command and rebooting the module, or
- Selecting the **Reset the Device to Factory Default** option from a telnet session and rebooting the module.

The zeroization of keys and CSP are immediate, providing insufficient time for an attacker to compromise them. The Crypto-Officer must wait until the module has successfully rebooted to verify that zeroization has completed.

3.4 Instance-Admin and Instance-User Guidance

The Instance-Admins do not have the ability to configure sensitive information on the module, except for the Instance-User and their own passwords. The Instance-Admin can configure the password strength policy for Instance-Admins and Instance-Users. Please refer to Section 3.2 above for information that should be followed to make sure the module is in a FIPS-Approved mode of operation.

Instance-Users do not have the ability to configure sensitive information on the module, except for their own passwords. The Instance-Admins and Instance-Users must employ strong passwords that meet or exceed the password strength requirements documented in Section 2.4.6 of this document and must not reveal their passwords to anyone.

4 Acronyms

This section describes the acronyms used in this document.

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Blocking Chain
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSE	Communication Security Establishment Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECC CDH	Elliptic-Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
N/A	Not Applicable
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SGK	Signature Generation Key
SHA	Secure Hash Algorithm
SNMP	SImple Network Management Protocol
SSL	Secure Socket Layer
SVK	Signature Verification Key

Acronym	Definition
TLS	Transport Layer Security
USB	Universal Serial Bus
WAN	Wide Area Network