Bomgar Corporation

B200™, B300™, and B400™ Remote Support Appliances

Firmware Version: 3.3.2FIPS, 3.4.0FIPS,3.4.1FIPS,3.5.1FIPS; Software Version: 12.1.6FIPs, 13.1.3FIPS,14.3.3FIPS

Hardware Version:

B200 with Tamper Evident Label Kit: TEL135325
B300r1 with Tamper Evident Label Kit: TEL135325 and Front Bezel: FB000300
B300r2 with Tamper Evident Label Kit: TEL135325 and Front Bezel: FB000300
B400r1 with Tamper Evident Label Kit: TEL135325 and Front Bezel: FB000400

BOMGAR™

FIPS 140-2 Security Level: 2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 2
Document Version: 2.3

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the B200, B300, and B400 Remote Support Appliances from Bomgar Corporation. This Security Policy describes how the B200, B300, and B400 Remote Support Appliances meet the security requirements of FIPS[1] 140-2 and how to run the modules in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the modules.

FIPS 140-2 – Security Requirements for Cryptographic Modules 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 Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/cmvp.

The B200, B300, and B400 Remote Support Appliances are referred to in this document as the Bomgar Appliances, the cryptographic modules, or the modules.

1.2 References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the modules from the following sources:

- The Bomgar website (http://www.bomgar.com/fips) contains information on the full line of products from Bomgar Corporation.
- 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 modules.

1.3 Document Organization

The 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
- Other supporting documentation as additional references

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

[1] FIPS – Federal Information Processing Standard

2 B200, B300, and B400 Appliances

2.1 Overview

Bomgar Corporation specializes in appliance-based solutions for remote support. Their remote support appliances give support technicians secure remote control of computers over the Internet, LAN[2], or WAN[3]. The software works through firewalls with no pre-installed client on the remote computer. With the Bomgar Appliances, a support technician can see the screen and control the remote system virtually as if physically present.

Figure 1 – Bomgar B200 (top), B300r1, B300r2, and B400r1

The B200, B300, and B400 Appliances (shown in Figure 1 above) enable the use of remote support in multiple areas of an organization in a way that is secure, integrated and manageable. The Bomgar Appliances can integrate with LDAP[4] for secure user management, prevent sensitive data from being routed outside the organization, and support extensive auditing and recording of support sessions. The logging is performed by the Bomgar Appliances, which allows for the review of all Customer and Support Representative interactions, including playback of all desktop screen data. The appliances also integrate with leading systems management and identity management solutions and include an Application Programming Interface (API) for deeper integration. With Bomgar, support managers can create support teams, customize queues, and report on all support activity. Network administrators can also monitor the Bomgar Appliances using Simple Network Management Protocol (SNMP).

The Bomgar Appliances enable remote access to multiple common operating systems, including various Linux distributions. They also enable remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, smartphones, and network devices.

The Bomgar Appliances can work over internal and extended networks and can be internet-accessible. This allows support organizations to reduce less effective means of support by driving requests through custom support portals hosted on the appliances. The Bomgar Appliances can route support requests to the appropriate technician or team and mediate connections between Customers and Support Representatives,

[2] LAN – Local Area Network
[3] WAN – Wide Area Network
[4] LDAP – Lightweight Directory Access Protocol

allowing chat sessions, file downloads/uploads, screen-sharing, remote control of desktops, and access to system and diagnostic information.

To enable the functionality described above, Bomgar has implemented architecture that places the Bomgar Appliances at the center of all communications (see Figure 2 below for a typical deployment scenario). The Bomgar Appliances provide a platform upon which one or more support sites are constructed. Sites represent individual help centers, and multiple sites can be set up to support multiple departments or groups in a company. Each site would offer a web site interface using Hypertext Transfer Protocol (HTTP) for unauthenticated services and HTTP over TLS[5] (HTTPS) for authenticated services, in addition to accepting direct client connections over a protocol running on top of TLS.

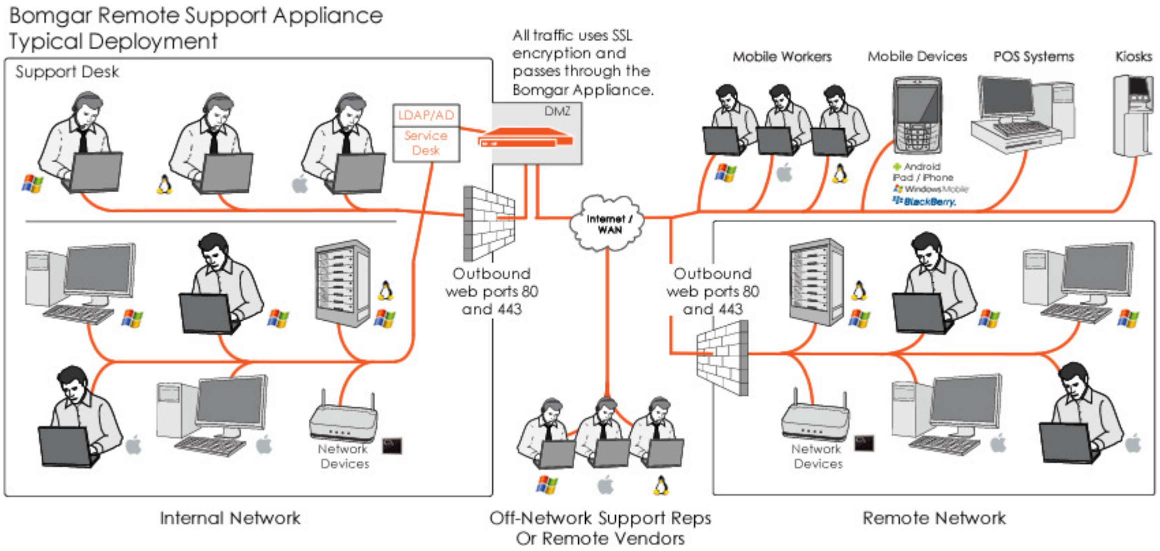


Figure 2 – Typical Deployment[6]

The Bomgar Appliances have two primary components that provide the appliances' functionality. The first is the Firmware that provides system-level configuration of the Bomgar Appliances. Settings such as IP[7] addresses and SSL/TLS configuration are all configured via the Firmware interface. The second component is made up of the software that provides site-level configuration, as well as the software clients that users interact with. The web interface behind the /login page is part of the software, as are the Representative Console, Customer Client, Connection Agent, and all other clients which are downloadable from the Bomgar Appliances.

The B200, B300, and B400 Remote Support Appliances are validated at the FIPS 140-2 Section levels in Table 1.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Modules Specification	2
2	Cryptographic Modules Ports and Interfaces	2
3	Roles, Services, and Authentication	2

[5] TLS – Transport Layer Security
[6] Rep – Representative; SSL – Secure Sockets Layer; DMZ – Demilitarized Zone; POS – Point of Sale; AD – Active Directory
[7] IP – Internet Protocol

Section	Section Title	Level
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[8]
7	Cryptographic Key Management	2
8	EMI/EMC[9]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The B200, B300, and B400 Appliances (running Firmware Version: 3.3.2FIPS, 3.4.0FIPS, 3.4.1FIPS, 3.5.1FIPS; Software Version: 12.1.6FIPs, 13.1.3FIPS,14.3.3FIPS) are multi-chip standalone modules that meet overall Level 2 FIPS 140-2 requirements.

Each hardware module must be running a specific version of the software to be in compliance. This is demonstrated in the table below.

Table 2 - Firmware / Software Versions

Module	Base Version / Software Version
B200	3.3.2FIPS / 12.1.6FIPS
	3.4.0FIPS / 13.1.3FIPS
	3.4.1FIPS / 13.1.3FIPS
	3.5.1FIPS / 14.3.3FIPS
B300r1	3.3.2FIPS / 12.1.6FIPS
	3.4.0FIPS / 13.1.3FIPS
	3.4.1FIPS / 13.1.3FIPS
	3.5.1FIPS / 14.3.3FIPS
B300r2	3.5.1FIPS / 14.3.3FIPS
B400r1	3.3.2FIPS / 12.1.6FIPS

Physically, the modules are composed of the components of a standard server platform. Figure 3 and Figure 4 show block diagrams for the B200, B300, and B400 respectively and identify the various components, connections and information flows. The cryptographic boundary of each module (denoted by the dotted lines in Figure 3 and Figure 4) is defined by the outer case of the appliance, which surrounds the complete set of hardware, firmware, and software components. Note that the B300 has four hard disks and the B400 has eight to support RAID[10] functionality.

[8] N/A – Not applicable

[9] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

[10] RAID – Redundant Array of Independent Disks

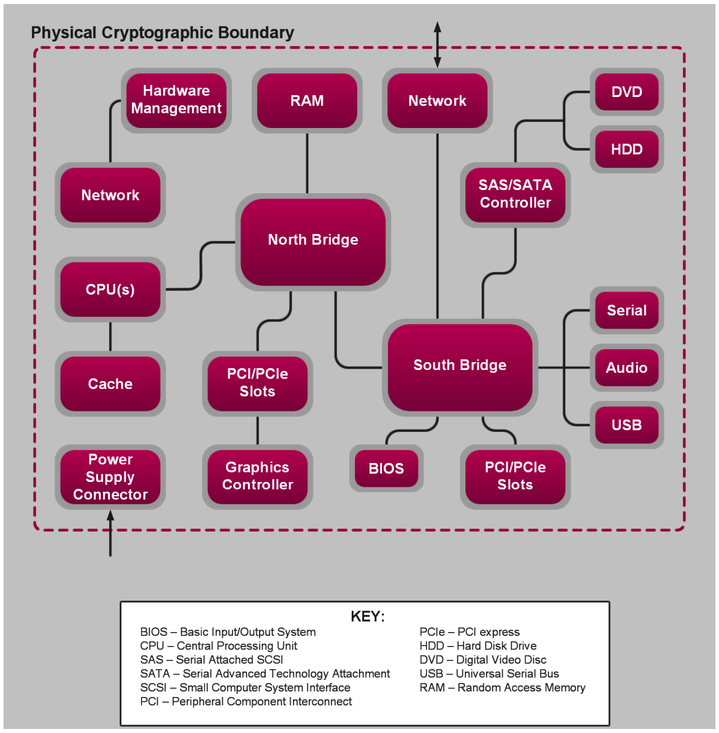

Physical Cryptographic Boundary
Hardware Management
RAM
Network
DVD
HDD
Network
SAS/SATA Controller
North Bridge
CPU(s)
Serial
South Bridge
Audio
Cache
PCI/PCIe Slots
USB
Power Supply Connector
Graphics Controller
BIOS
PCI/PCIe Slots
KEY:
BIOS – Basic Input/Output System
CPU – Central Processing Unit
SAS – Serial Attached SCSI
SATA – Serial Advanced Technology Attachment
SCSI – Small Computer System Interface
PCI – Peripheral Component Interconnect
PCIe – PCI express
HDD – Hard Disk Drive
DVD – Digital Video Disc
USB – Universal Serial Bus
RAM – Random Access Memory

Figure 3 – Block Diagram for B200 with Cryptographic Boundary

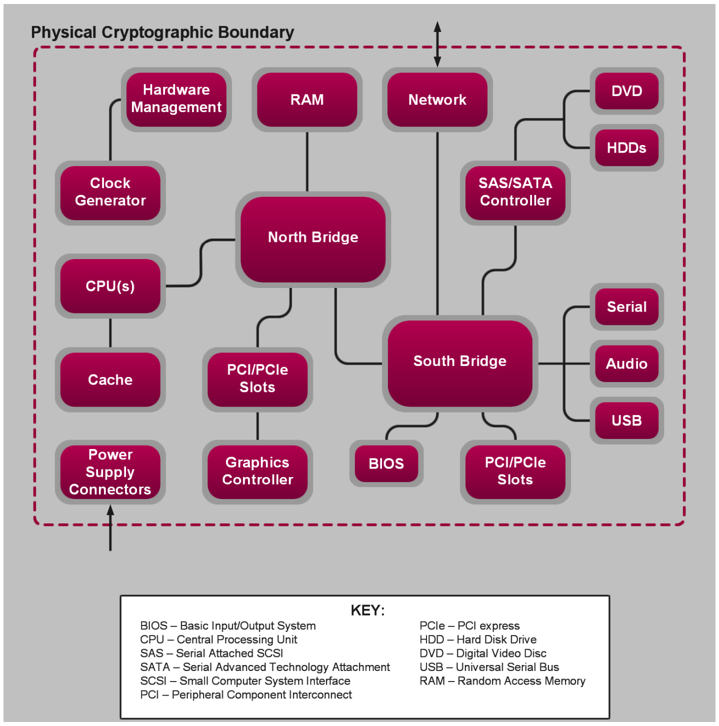

Physical Cryptographic Boundary
Hardware Management
RAM
Network
DVD
HDDs
Clock Generator
SAS/SATA Controller
North Bridge
CPU(s)
Serial
South Bridge
Audio
Cache
PCI/PCIe Slots
USB
Power Supply Connectors
Graphics Controller
BIOS
PCI/PCIe Slots
KEY:
BIOS – Basic Input/Output System
CPU – Central Processing Unit
SAS – Serial Attached SCSI
SATA – Serial Advanced Technology Attachment
SCSI – Small Computer System Interface
PCI – Peripheral Component Interconnect
PCIe – PCI express
HDD – Hard Disk Drive
DVD – Digital Video Disc
USB – Universal Serial Bus
RAM – Random Access Memory

Figure 4 – Block Diagram for B300 and B400 with Cryptographic Boundary

2.3 Module Interfaces

The modules' 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 modules receive power via a defined power input interface.

Data input/output are the network data packets utilizing the services provided by the modules. These packets enter and exit the modules through the network ports. Control input consists of both configuration and administration data entering the modules through the web interface and also the input for the power and reset buttons. Status output consists of status information relayed via the LED[11] indicators and the web interface.

The physical ports and interfaces of the modules are depicted in Figure 5, Figure 6, and Figure 7 below.

[11] LED – Light Emitting Diode

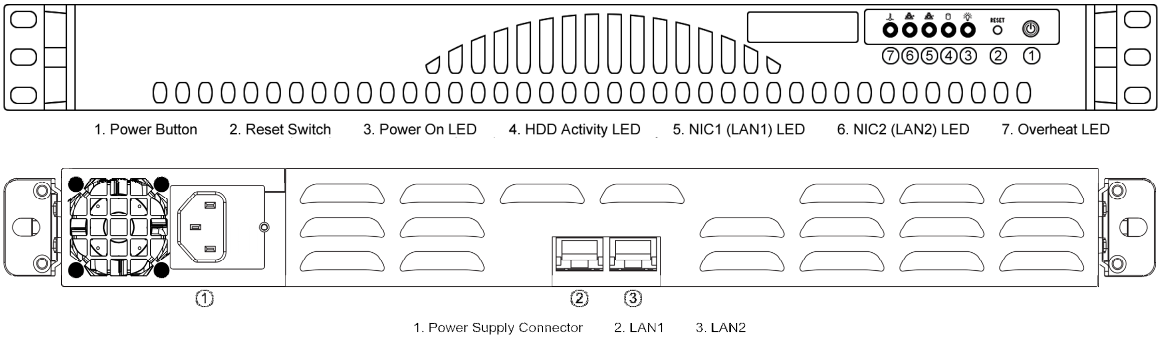


Figure 5 – Front and Rear View of the B200

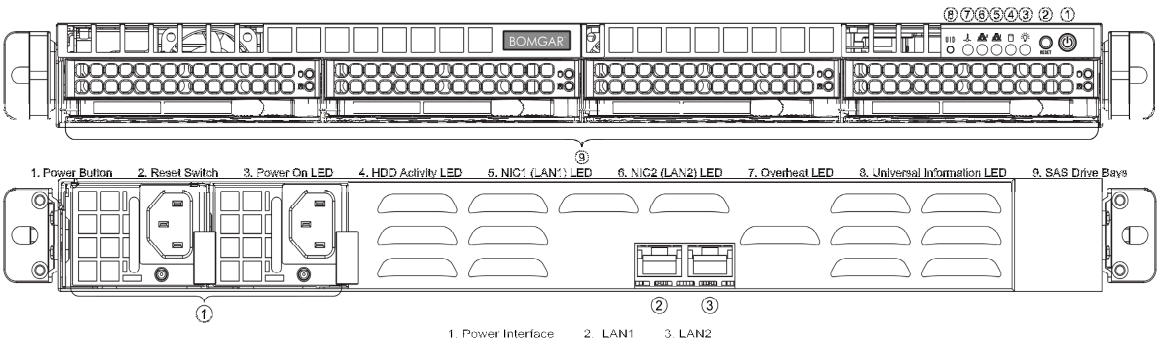


Figure 6 – Front and Rear View of the B300r1 and B300r2

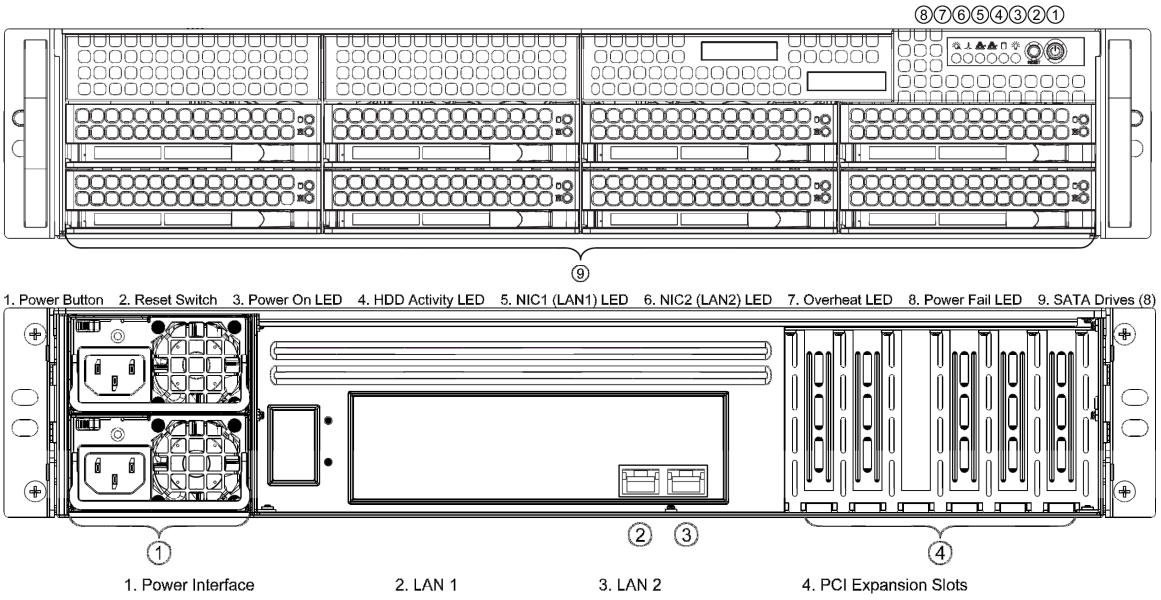


Figure 7 – Front and Rear View of the B400r1

Of the ports and interfaces depicted in the figures above, only the following are enabled to be used in FIPS mode of operation:

- Network ports

- Power button
- Reset button
- Power connector(s)
- LEDs

The mouse port, keyboard port, network port, 2 USB ports, serial port and VGA port behind the rear bezel are inaccessible. These ports are excluded components for the FIPS 140-2 validation of the modules.

Table 3 lists the physical interfaces available in the Bomgar Appliances and also provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2.

Table 3 – Physical Ports and Logical Interfaces

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

The cryptographic modules have a number of LEDs which indicate the state of the modules. The descriptions for the LEDs for each module are listed in Table 4 below.

Table 4 – LED Descriptions

Model	LED	Condition	Description
B200	Power	On	System on
		Off	System off
	Hard Disk Drive (HDD)	On	IDE channel activity
		Blink	SAS/SATA drive or DVD-ROM drive activity
		Off	No HDD activity
	LAN1/LAN2	On	Linked
		Blink	Network activity
		Off	Disconnected
	Overheat/Fan	On	System overheat condition
		Blink	Fan failure
		Off	System normal
B300r1 /	Power	On	System on

Model	LED	Condition	Description
B300 r2		Off	System off
	Hard Disk Drive (HDD)	Blink	HDD activity
		Off	No HDD activity
	LAN1/LAN2	On	Linked
		Blink	Network activity
		Off	Disconnected
	Universal Information	Fast Blink Red (1x/ sec)	Fan fail
		Solid Red	CPU overheat
		Slow Blink Red (1x/ 4 sec)	Power fail
		Solid Blue	Local Unit Identifier (UID) button depressed
B400r1	Power	On	System on
		Off	System off
	Hard Disk Drive (HDD)	On/Blink	HDD activity
		Off	No HDD activity
	LAN 1/LAN2	On	Linked
		Blink	Network activity
		Off	Disconnected
	Overheat/Fan	On	System overheat condition
		Blink	Fan failure
		Off	System normal
	Power fail	On	Power supply failure
		Off	System off

2.4 Roles and Services

As required by FIPS 140-2, the modules support a Crypto-Officer (CO) role and a User role. The User role comprises an Instance-Admin role and an Instance-User role.

The modules support role-based authentication for the Crypto-Officer and identity-based authentication for the Instance-Admin and Instance-User roles. Operators explicitly assume the role of Instance-Admin or Instance-User based on the authentication credentials used. The credentials used determine the services available to the operator.

2.4.1 Crypto-Officer Role

The Crypto-Officer role is the administrator for the module and is responsible for the initial setup and configuration. The Crypto-Officer has administrator rights to monitor and manage the firmware component's configuration, manage the CO account, and reset the default Instance-Admin account passwords.

2.4.2 Instance-Admin Role

The Instance-Admin has administrator rights to monitor and manage the software instance's configuration, manage Instance-Admin accounts, and 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 has to 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 below. Please note that the keys and Critical Security Parameters (CSPs) listed indicate the type of access required:

- Read: The CSP is read
- Write: The CSP is established, generated, modified, or zeroized.

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

Service	Description	Operator	Input	Output	CSP and Type of Access
Manage Bomgar Appliance settings	Configure IP[12] and TLS settings	CO	Command	Command response	• RSA[13] public key – Read, Write • RSA private key – Read, Write • Session key – Read, Write • Session integrity key – Read, Write • PRNG[14] seed/seed key – Read, Write • CO Password – Read • Firmware update key – Read, Write
Manage CO account	Manage CO account password	CO	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • CO Password – Read, Write

[12] IP – Internet Protocol
[13] RSA – Rivest, Shamir, and Adleman
[14] PRNG – Pseudo Random Number Generator

Service	Description	Operator	Input	Output	CSP and Type of Access
Reset Instance-Admin password	Reset Instance-Admin account password	CO	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • Instance-Admin Password – Write
Configure Instance-Admin accounts	Set up and monitor Instance- Admin accounts	CO, Instance-Admin	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • Instance-Admin Password – Read, Write
Configure Instance-User accounts	Set up and monitor Instance-User accounts	Instance-Admin, Instance-User	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • 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 modules	CO	Command	Status information	• RSA public key – Read • RSA private key – Read
Zeroize keys	Zeroize plaintext keys	CO	Command	Command response	• All CSPs – Write
Perform Representative Console service	Access and perform services for Representative Consoles	Instance-Admin, Instance-User	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • Instance-Admin Password – Read • Instance-User Password – Read

Service	Description	Operator	Input	Output	CSP and Type of Access
Manage instance settings	Manage instance configuration settings	Instance-Admin, Instance-User	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write
Update Firmware	Install new firmware package	CO	Command	Command response	• RSA public key – Read • RSA private key – Read • Session key – Read, Write • Session integrity key – Read, Write • PRNG seed/seed key – Read, Write • CO Password – Read • Firmware update public key – Read, Write

2.4.5 Unauthenticated Operator Services

The modules provide a service to unauthenticated operators as listed in Table 6 below.

Table 6 – Unauthenticated Operator Service

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 request 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 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. Instance-Admins and Instance-Users can also authenticate to the module via one of the following configurable methods: LDAP, Kerberos, or RADIUS.

Table 7 lists the authentication mechanisms used by the modules.

Table 7 – Authentication Mechanism Used by the Modules

Authentication Type	Strength
Password	Passwords are required to be at least 6 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 characters to choose from. A six-character password will yield a total of 95^6 = 735,091,890,625 possible combinations. Any failed authentication attempt will result in at least one second delay in response. Hence there cannot be more than 60 invalid attempts in any given minute and probability that a random attempt will succeed or a false acceptance will occur is 60 x 1/ 735,091,890,625 in one minute.

2.5 Physical Security

The B200, B300, and B400 Appliances are multi-chip standalone cryptographic modules. Each is enclosed in a hard and opaque metal case that completely encloses all of the internal components of the module. Tamper-evident labels are applied to the cases to provide physical evidence of attempts to gain access to the modules' internal components. All of the modules' components are production grade. The placement of tamper-evident labels can be found in Sections 3.1.2, 3.1.4, and 3.1.6 of this document.

2.6 Operational Environment

The operational environment requirements do not apply to the Bomgar Appliances. The modules provide only a limited operational environment; they do not provide a general-purpose operating system environment.

2.7 Cryptographic Key Management

The modules implement the FIPS-Approved algorithms listed in Table 8.

Table 8 – FIPS-Approved Algorithm Implementations

Algorithm	Bomgar Appliance Certificate Number	Reference
Advanced Encryption Standard (AES) in CBC[15], ECB[16], OFB[17], and CFB[18]128 modes (with 128-bit, 192-bit, and 256-bit keys)	2219, 2543, 3033, 3340	FIPS 197
Triple Data Encryption Standard (Triple DES) – CBC, ECB, OFB, CFB8, and CFB64 modes (with 2-key[19] and 3-key)	1389, 1538, 1774, 1909	FIPS 46-3 ANSI X.952-1998
RSA ANSI[20] X9.31 (key generation[19]) – 1024-, 1536-, and 2048-bit	1136, 1297, 1575, 1715	FIPS 186-2 ANSI X.931-1998
RSA Public Key Cryptography Standard #1 (PKCS#1) v1.5 (sign/verify) – 1024-, 2048-, 3072-, and 4096-bit	1136, 1297, 1575, 1715	FIPS 186-2
RSA Probabilistic Signature Scheme (PSS) (sign/verify) – 1024-, 2048-, 3072-, and 4096-bit	1136, 1297, 1575, 1715	FIPS 186-2

[15] CBC – Cipher Block Chaining
[16] ECB – Electronic Codebook
[17] OFB – Output Feedback
[18] CFB – Cipher Feedback
[19] SP800-131A provides guidance for transitions to use the stronger cryptographic keys.
[20] ANSI – American National Standards Institute

Algorithm	Bomgar Appliance Certificate Number	Reference
Secure Hash Algorithm (SHA)-1, SHA-224, SHA-256, SHA-384, and SHA-512	1910, 2143, 2531, 2774	FIPS 180-2
Keyed-Hash Message Authentication Code (HMAC[19]) using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	1350, 1564, 1915, 2130	FIPS 198
ANSI X9.31 A.2.4 PRNG[19]	1113, 1208, 1311, 1372	NIST-Recommended RNG Based on ANSI X9.31 Appendix A.2.4 Using the AES Algorithm, January 31, 2005

The modules also support the following non-FIPS-Approved algorithms:

- RSA key transport: 1024-, 1536-, 2048-, 3072- 4096-bits (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RC4[21]
- RC4-40
- DES
- DES-40
- MD5[22]

The modules support the Critical Security Parameters (CSPs) in Table 9.

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

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
RSA private key	1024-, 1536-, 2048-, 3072-, or 4096-bit RSA private key	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	Key exchange for TLS sessions
RSA public key	1024-, 1536-, 2048-, 3072-, or 4096-bit RSA public key	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

[21] RC4 – Rivest Cipher 4

[22] MD5 – Message Digest 5

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Session key	• 128-bit AES CBC 128 key • 256-bit AES CBC 256 key • 192-bit Triple DES CBC 112 key	Internally generated	Exits in encrypted form during TLS handshake	Resides on volatile memory only in plaintext	By power cycle or session termination	Data encryption and decryption for TLS sessions
Session integrity key	• HMAC-SHA Key length: 20 bytes	Internally generated	Exits in encrypted form during TLS handshake	Resides on volatile memory only in plaintext	By power cycle or session termination	Ensure authenticity of encrypted TLS session data
Crypto-Officer password	6-character minimum password	Enters the modules in encrypted form	Never exits the modules	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the CO
Instance-Admin password	6-character minimum password	Enters the modules in encrypted form	Never exits the modules	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the Instance-Admin
Instance-User password	6-character minimum password	Enters the modules in encrypted form	Never exits the modules	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the Instance-User
PRNG seed key	32 bytes of random value	Internally generated	Never exits the modules	Resides on volatile memory only in plaintext	By power cycle, session termination, or factory reset	Seeds the FIPS-Approved PRNG
PRNG seed	16 bytes of random value	Internally generated	Never exits the modules	Resides on volatile memory only in plaintext	By power cycle, session termination, or factory reset	Seeds the FIPS-Approved PRNG
Firmware update key	4096-bit RSA public key	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

2.8 EMI/EMC

The modules were 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).

2.9 Self-Tests

2.9.1 Power-Up Self-Tests

The Bomgar Appliances perform the following self-tests at power-up to verify the integrity of the software/firmware and the correct operation of the FIPS-Approved algorithm implementations employed by the modules:

- Software/firmware integrity check using a SHA-1 EDC[23]
- AES Known Answer Test (KAT) (encrypt/decrypt)
- Triple DES KAT (encrypt/decrypt)
- RSA KAT (sign/verify)
- HMAC KATs (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512)
- SHA-1 KAT (note that all SHA-2 implementations are tested as part of the underlying mechanism of the HMAC SHA self-tests)
- ANSI X9.31 PRNG KAT

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 Appliances perform the following conditional self-tests:

- ANSI X9.31 A.2.4 PRNG Continuous RNG test: Verifying the correct operation of the PRNG algorithm implementation.
- RSA pair-wise consistency check (sign/verify and encrypt/decrypt): Verifying that a newly generated RSA key pair works properly.
- Software/firmware load test: Verifying the upgrade packages. Upgrade packages are digitally-signed using RSA-4096, and are only loaded once the digital signature is verified.

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

2.10 Mitigation of Other Attacks

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

[23] EDC – Error Detection Code

3 Secure Operation

The B200, B300, and B400 Appliances meet Level 2 requirements for FIPS 140-2. The sections below describe how to ensure that the modules are running securely.

3.1 Initial Setup

The following sections provide the necessary step-by-step instructions for the secure hardware installation of the B200, B300, and B400 Appliances, as well as the steps necessary to configure the modules for a FIPS-Approved mode of operation. If you have any questions or if issues arise at any point during the installation and configuration of your Bomgar Appliances, contact the Bomgar support team toll-free at 1-877-826-6427 x2 or internationally at +01-601-519-0123 x2.

3.1.1 B200 Hardware Setup

In order to set up the Bomgar B200, the following steps will need to be performed by the Crypto-Officer:

1. Inspect the tamper-evident labels as described in Section 3.1.2 below. The tamper evident labels must be applied for the module to operate in a FIPS-Approved mode of operation. 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. Follow the procedures included in the Hardware Setup Guide to install your B200 in your server rack.
3. After you have installed the B200 per the Hardware Setup Guide, refer to the included Bomgar Hardware Installation Guide to configure your network settings.
4. Once the B200's network settings are correctly configured, return to Section 3.1.6.1 in this document to configure your B200 for FIPS mode.

3.1.2 B200 Label Inspection

The B200 with tamper-evident label kit – part # TEL135325 – and front bezel – part # FB000200 – will be shipped from the factory with two labels pre-applied (see Figure 8 and Figure 9 below). 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 shall be routinely inspected for damage by the Crypto-Officer. If the Crypto-Officer finds 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. If any additional labels are needed contact Bomgar support toll-free at 1 877 826 6427 x2 or internationally at +01 601 519 0123 x2 with part # TEL135325. The Crypto-Officer is also responsible for securing and having control of the additional tamper-evident labels at all times.

Inspect all tamper-evident labels that shipped pre-applied to the B200 chassis (see Figure 8 and Figure 9), ensuring that each label shows no sign of tampering and is properly placed. Any attempt to reposition or remove the label will result in the voiding of that label and leave 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.

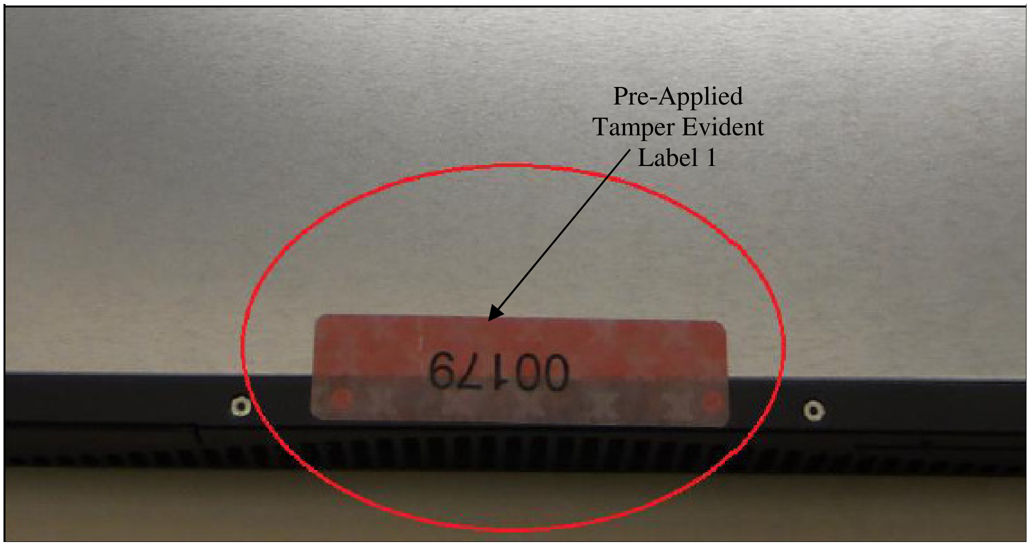


Figure 8 – Tamper-Evident Label Applied to Top of B200, Overlapping the Galvanized Metal Cover and the Front Panel

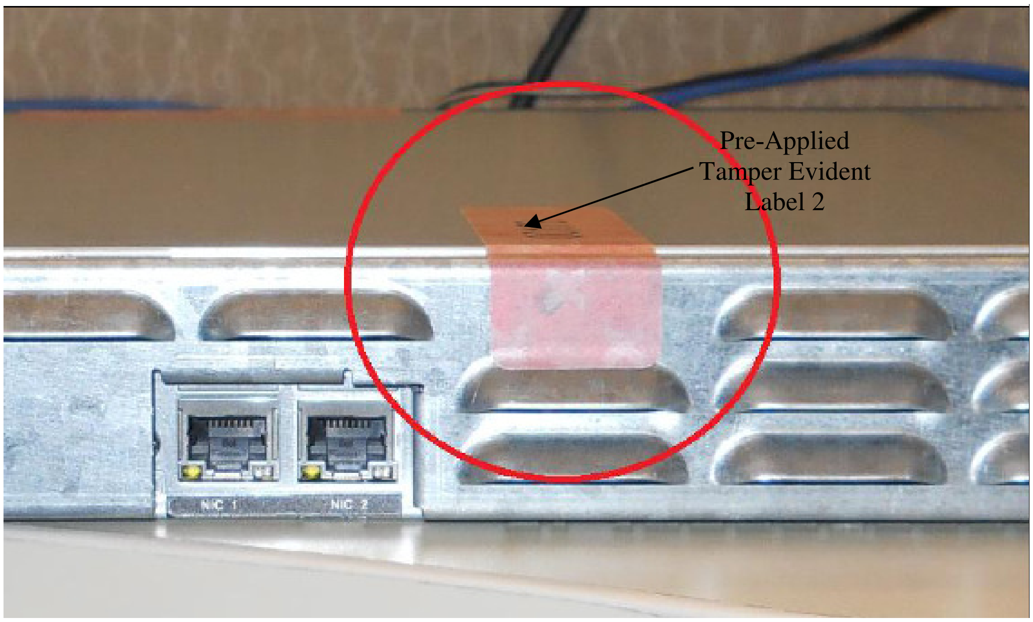


Figure 9 – Tamper-Evident Label Applied to Rear of B200, Overlapping the Galvanized Metal Cover and the Rear Steel Bezel

3.1.3 B300 Hardware Setup

B300r1 and B300r2 are referred as B300 when the information is same for both the models. In order to set up the Bomgar B300, the following steps will need to be performed by the Crypto-Officer:

1. Unpack the B300 and remove the front bezel from the front of the B300:
    a. Loosen the set screw on the right-hand side of the front bezel. This screw keeps the tab in place during shipping.
    b. Press the tab on the right side of the front bezel and pull the front bezel towards you, right side first.

2. Reseat the hard drives:
   a. Remove each of the hard drives by pressing the dark red buttons to unlatch the drive carrier handles. Use the handles to pull the drives about halfway out of the B300 chassis.
   b. As you reinsert each of the drives, the carrier handles will begin to close. Close the handles (you will feel them lock) and fully insert the drives into the B300 by firmly pressing on the left and right edges of the front of the drive carriers. Even if no movement is felt, this helps to ensure that the disk is completely engaged.
3. Reattach the B300's front bezel:
   a. Engage the left side of the faceplate first, taking care to align the stubs of the faceplate with the drilled holes in the left ear.
   b. Repeat on the right side and then tighten the set screw. Take care not to over tighten this screw.
4. Inspect the tamper-evident labels as described in Section 3.1.4 below. The tamper evident labels must be applied for the module to operate in a FIPS-Approved mode of operation. 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.
5. Follow the procedures included in the Hardware Setup Guide to install your B300 in your server rack.
6. After you have installed the B300 per the Hardware Setup Guide, refer to the included Bomgar Hardware Installation Guide to configure your network settings.
7. Once the B300's network settings are correctly configured, return to Section 3.1.6.1 in this document to configure your B300 for FIPS mode.

3.1.4 B300 Label Inspection

The B300r1 and B300r2 with tamper-evident label kit – part # TEL135325 – and front bezel – part # FB000300 – will be shipped from the factory with six labels. Four labels are pre-applied at factory (see Figure 10 and Figure 12 below). Two labels are to be applied by the Crypto-Officer on chassis top and bottom overlapping the front bezel (see Figure 11 below). This is to allow the end-user to reseat the drives upon receipt before affixing the front bezel to the appliance. 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 shall be routinely inspected for damage by the Crypto-Officer. If the Crypto-Officer finds 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. If any additional labels are needed contact Bomgar support toll-free at 1-877-826-6427 x2 or internationally at +01-601-519-0123 x2 with part # TEL135325. The Crypto-Officer is also responsible for securing and having control of the additional tamper-evident labels at all times.

1. Inspect all tamper-evident labels that shipped pre-applied to the B300 chassis (see Figure 10 below), ensuring that each label shows no sign of tampering and is properly placed. Any attempt to reposition or remove the label will result in the voiding of that label and leave 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, first you must clean the top surface and front bezel of the B300 with isopropyl alcohol in the area where the tamper-evident labels will be placed.
3. Holding the label by the edges, place the label on the surface as indicated in Figure 11 and Figure 12.
4. Apply the included tamper-evident labels by rubbing gently across the entire label to ensure adhesion to the surface.

   NOTE: Any attempt to reposition or remove the label will result in the voiding of that label and leave a residue on the surface.
5. Allow the labels to fully adhere to the B300 within 24 hours in a physically secure environment before placing the B300 in the intended environment.

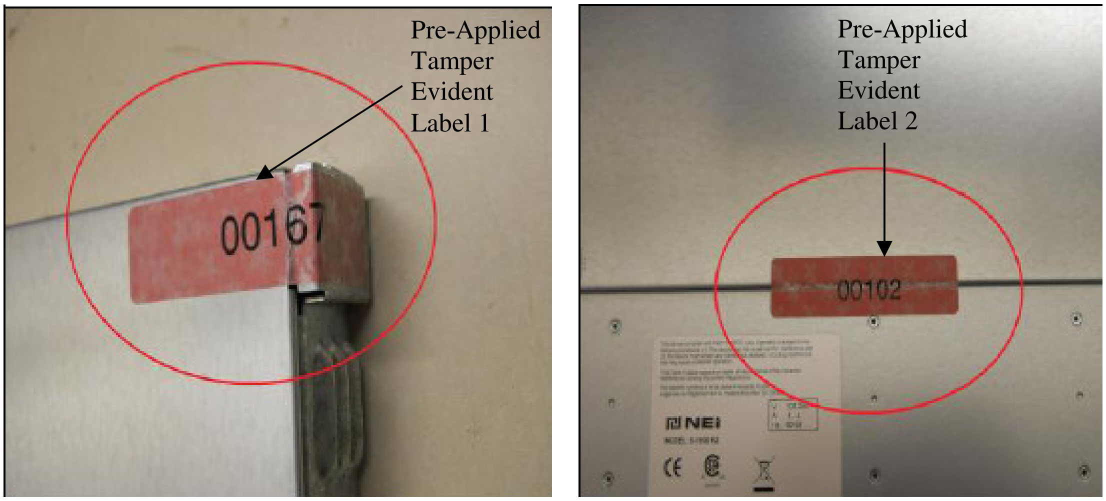


Figure 10 – Rear Metallic Bezel Seal (Left) and Sealed Top Cover (Right) of B300r1 and B300r2

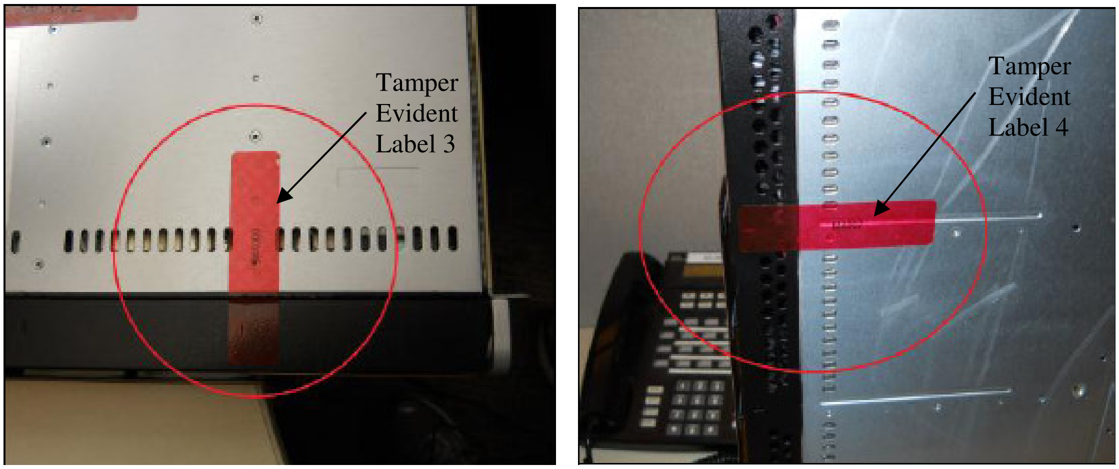


Figure 11 – Sealed Front Bezel to Chassis Top (Left) and Sealed Front Bezel to Chassis Bottom (Right) of B300r1and B300r2

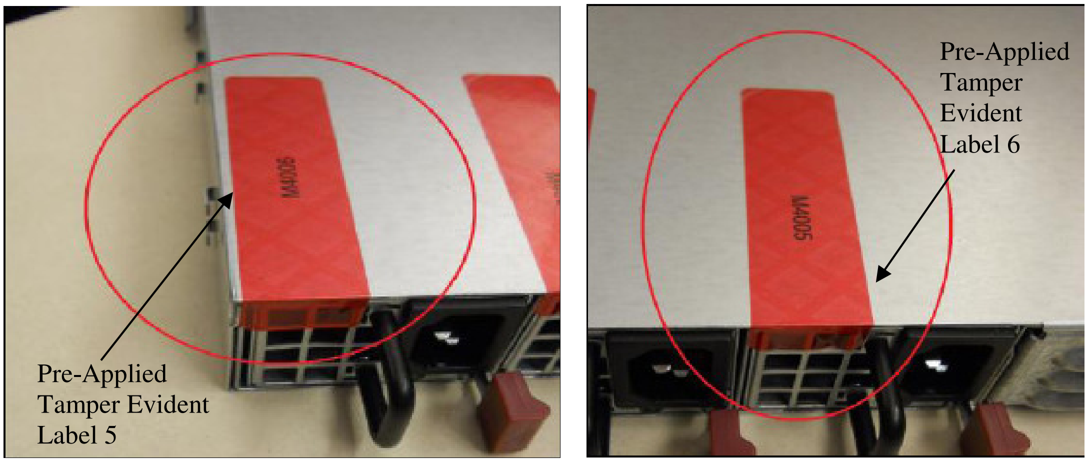


Figure 12 – Sealed Top Chassis to Left Power Supply (Left) and Sealed Top Chassis to Right Power Supply (Right) of B300r1 and B300r2

3.1.5 B400 Hardware Setup

In order to set up the Bomgar B400, the following steps will need to be performed by the Crypto-Officer:

1. Unpack the B400.
2. Reseat the hard drives:
   a. Remove each of the hard drives by pressing the dark red buttons to unlatch the drive carrier handles. Use the handles to pull the drives about halfway out of the B400 chassis.
   b. As you reinsert each of the drives, the carrier handles will begin to close. Close the handles (you will feel them lock) and fully insert the drives into the B400 by firmly pressing on the left and right edges of the front of the drive carriers. Even if no movement is felt, this helps to ensure that the disk is completely engaged.
3. Attach the B400's front bezel by engaging first the left side of the faceplate and then the right side.
4. Inspect the tamper-evident labels as described in Section 3.1.6 below. The tamper evident labels must be applied for the module to operate in a FIPS-Approved mode of operation. 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.
5. Follow the procedures included in the Hardware Setup Guide to install your B400 in your server rack.
6. After you have installed the B400 per the Hardware Setup Guide, refer to the included Bomgar Hardware Installation Guide to configure your network settings.
7. Once the B400's network settings are correctly configured, return to Section 3.1.6.1 in this document to configure your B400 for FIPS mode.

3.1.6 B400 Label Inspection and Application

The B400r1 with tamper evident label kit – part # TEL135325 – and front bezel – part # FB000400 – will be shipped from the factory with five labels. Three labels are pre-applied at factory (see Figure 13 and Figure 14 below). Two labels are to be applied by the Crypto-Officer on chassis top and bottom overlapping the front bezel (see Figure 15 below). This is to allow the end-user to reseat the drives upon receipt before affixing the front bezel to the appliance.

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 shall be routinely inspected for damage by the Crypto-Officer. If the Crypto-Officer finds 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. If any additional labels are needed contact Bomgar support toll-free at 1-877-826-6427 x2 or internationally at +01-601-519-0123 x2 with part # TEL135325. The Crypto-Officer is also responsible for securing and having control of the additional tamper-evident labels at all times.

1. Inspect all tamper-evident labels that shipped pre-applied to the B400 chassis (see Figure 13, Figure 14, and Figure 15 below), ensuring that each label shows no sign of tampering and is properly placed. Any attempt to reposition or remove the label will result in the voiding of that label and leave 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, first you must clean the surface and front bezel of the B400 with isopropyl alcohol in the area where the tamper-evident labels will be placed.
3. Holding the label by the edges, place the label on the surface as indicated below (see Figure 15).
4. Apply the included tamper-evident labels by rubbing gently across the entire label to ensure adhesion to the surface.

   NOTE: Any attempt to reposition or remove the label will result in the voiding of that label and leave a residue on the surface.
5. Allow the labels to fully adhere to the B400 within 24 hours in a physically secure environment before placing the B400 in the intended environment.

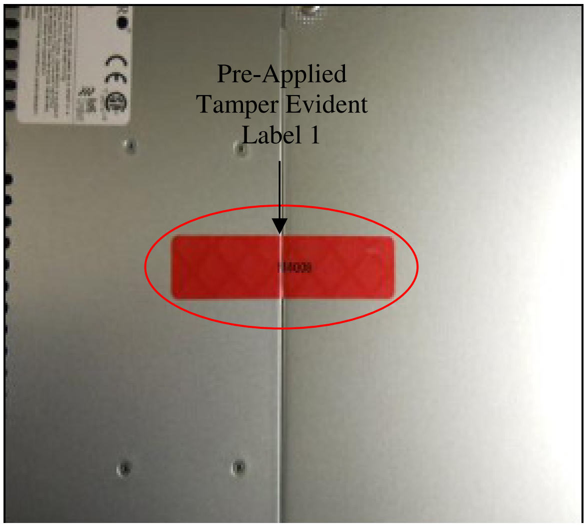


Figure 13 – Sealed Top Cover of B400r1

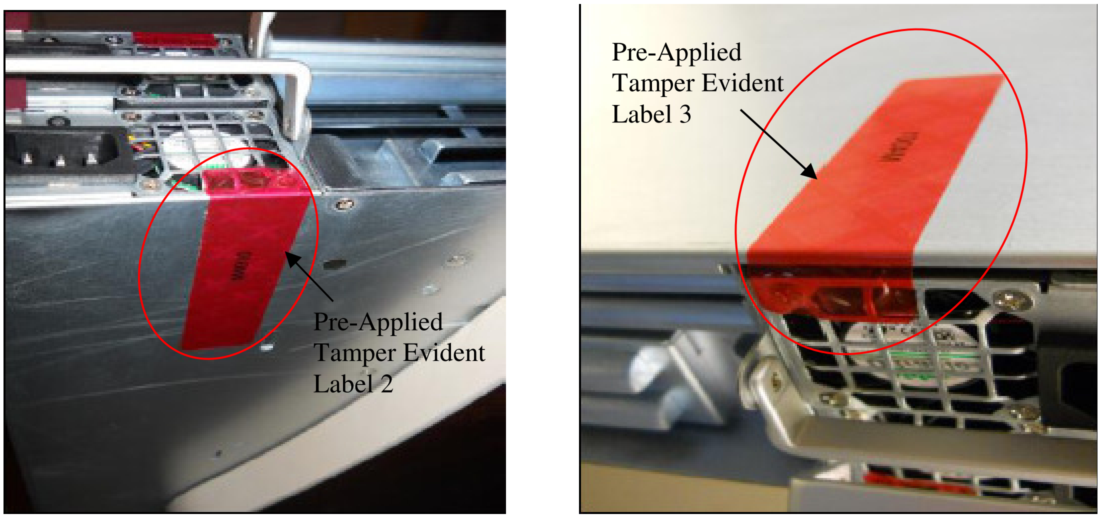


Figure 14 – Sealed power supply #1 to chassis bottom (Left) and Sealed power supply #2 to chassis top (Right) of B400r1

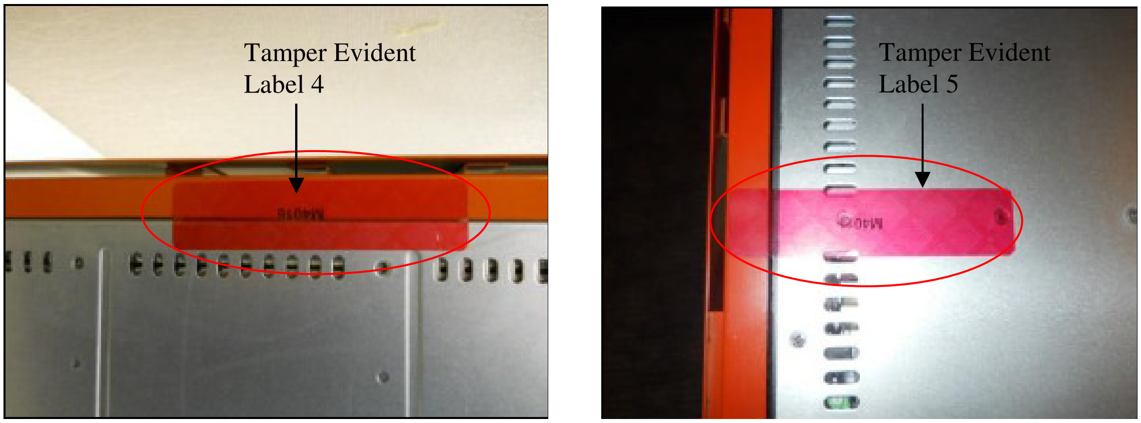
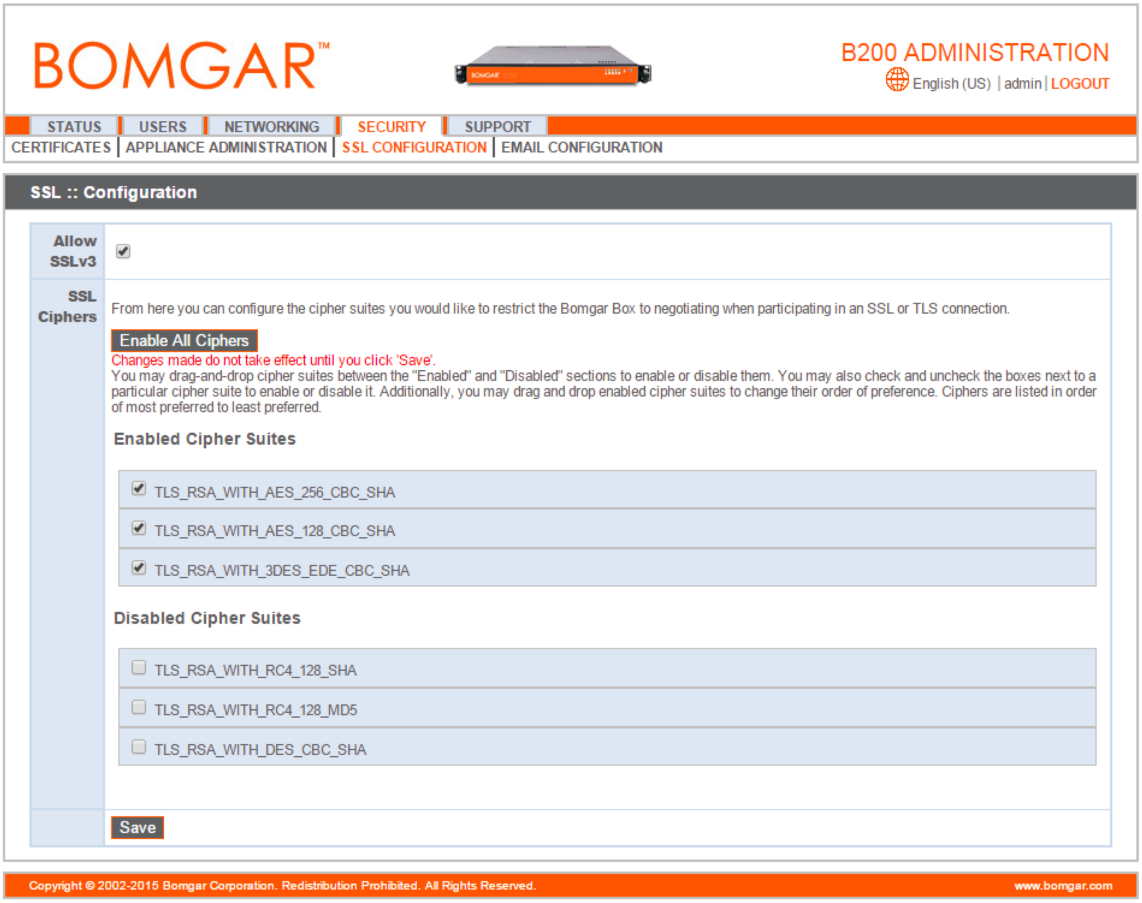


Figure 15 – Sealed front bezel to chassis bottom (Left) and Sealed front bezel to chassis top (Right) of B400r1

3.1.6.1 B200, B300, and B400 FIPS Mode Configuration

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



SSL :: Configuration

Allow SSLv3 ☑

SSL Ciphers

From here you can configure the cipher suites you would like to restrict the Bomgar Box to negotiating when participating in an SSL or TLS connection.

Changes made do not take effect until you click 'Save'.

You may drag-and-drop cipher suites between the "Enabled" and "Disabled" sections to enable or disable them. You may also check and uncheck the boxes next to a particular cipher suite to enable or disable it. Additionally, you may drag and drop enabled cipher suites to change their order of preference. Ciphers are listed in order of most preferred to least preferred.

Enabled Cipher Suites

☑ TLS_RSA_WITH_AES_256_CBC_SHA

☑ TLS_RSA_WITH_AES_128_CBC_SHA

☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA

Disabled Cipher Suites

☐ TLS_RSA_WITH_RC4_128_SHA

☐ TLS_RSA_WITH_RC4_128_MD5

☐ TLS_RSA_WITH_DES_CBC_SHA

Copyright © 2002-2015 Bomgar Corporation. Redistribution Prohibited. All Rights Reserved. www.bomgar.com

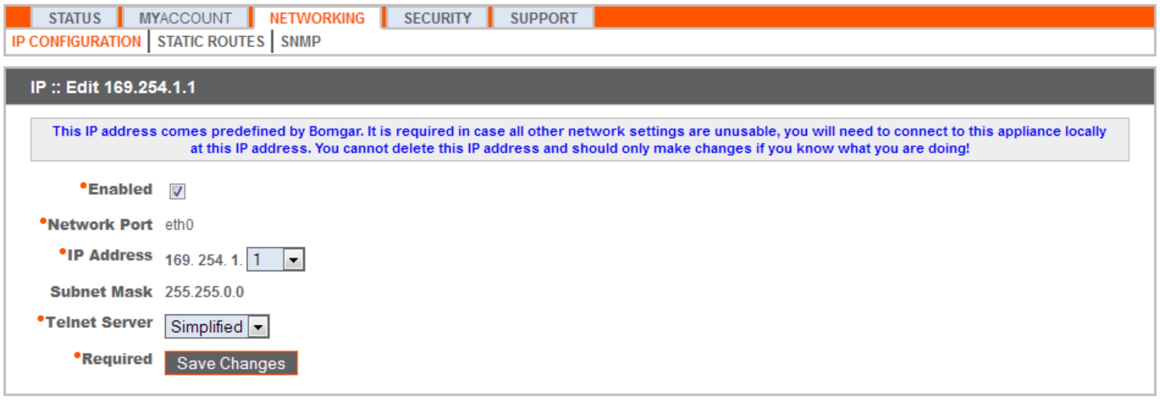
FIPS-Approved Mode Configuration

Log into the Bomgar Appliance Administrative Interface (e.g., support.example.com/appliance) and configure your settings as described below[24]:

1. Navigate to the **IP Configuration** page under the **Networking** tab (see Figure below).
2. Click the default **169.254.1.1** IP address to edit it.
3. Set the **Telnet Server** setting to **Simplified**.

[24] **NOTE**: The module comes preloaded with a default password. The Crypto-Officer is responsible for changing this password before proceeding with the configuration steps.

4. Click the **Save Changes** button to commit these configuration changes.



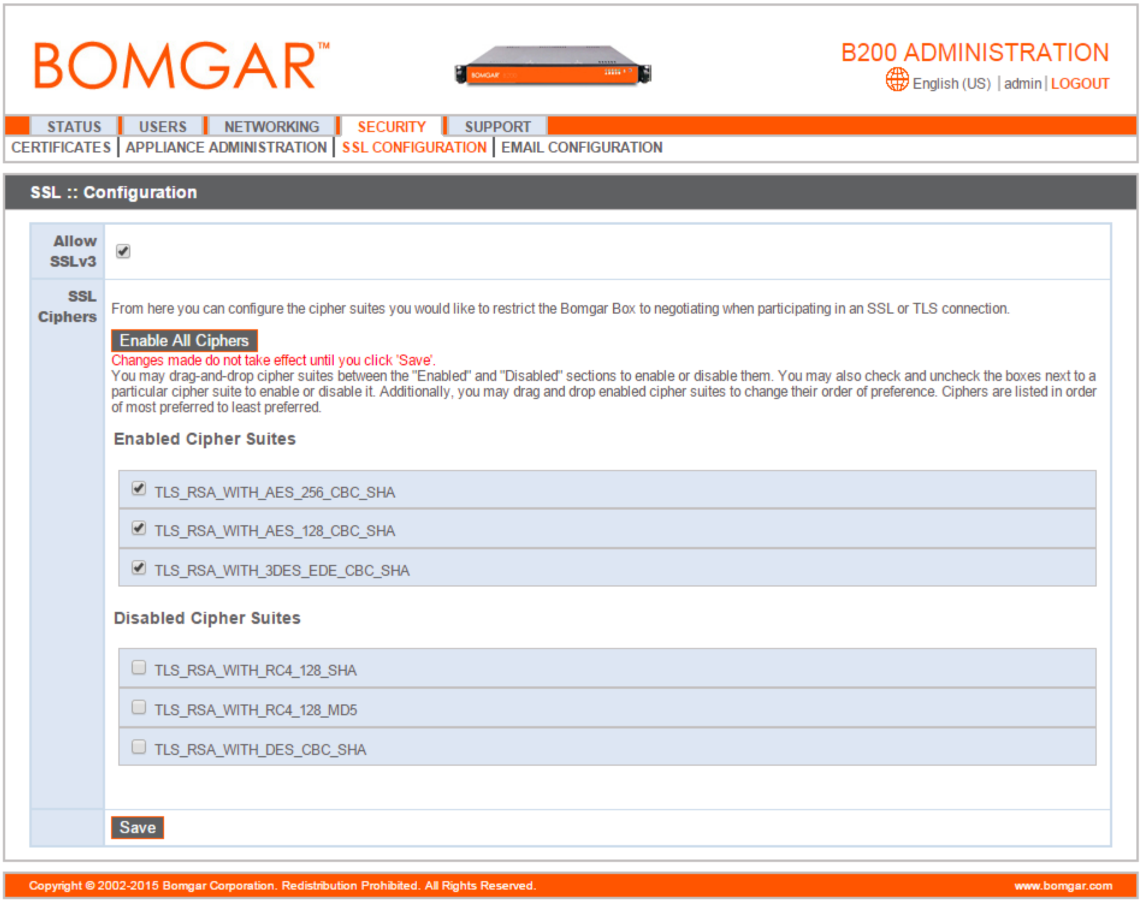
IP :: Edit 169.254.1.1

This IP address comes predefined by Bomgar. It is required in case all other network settings are unusable, you will need to connect to this appliance locally at this IP address. You cannot delete this IP address and should only make changes if you know what you are doing!

•Enabled	☑
•Network Port	eth0
•IP Address	169. 254. 1. 1
Subnet Mask	255.255.0.0
•Telnet Server	Simplified
•Required	Save Changes

Figure 17– IP Configuration Page

Navigate to the SSL Configuration **page under the** Security **tab (see**



SSL :: Configuration

Allow SSLv3 ☑

SSL Ciphers

From here you can configure the cipher suites you would like to restrict the Bomgar Box to negotiating when participating in an SSL or TLS connection.

Changes made do not take effect until you click 'Save'.
You may drag-and-drop cipher suites between the "Enabled" and "Disabled" sections to enable or disable them. You may also check and uncheck the boxes next to a particular cipher suite to enable or disable it. Additionally, you may drag and drop enabled cipher suites to change their order of preference. Ciphers are listed in order of most preferred to least preferred.

Enabled Cipher Suites

- ☑ TLS_RSA_WITH_AES_256_CBC_SHA
- ☑ TLS_RSA_WITH_AES_128_CBC_SHA
- ☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA

Disabled Cipher Suites

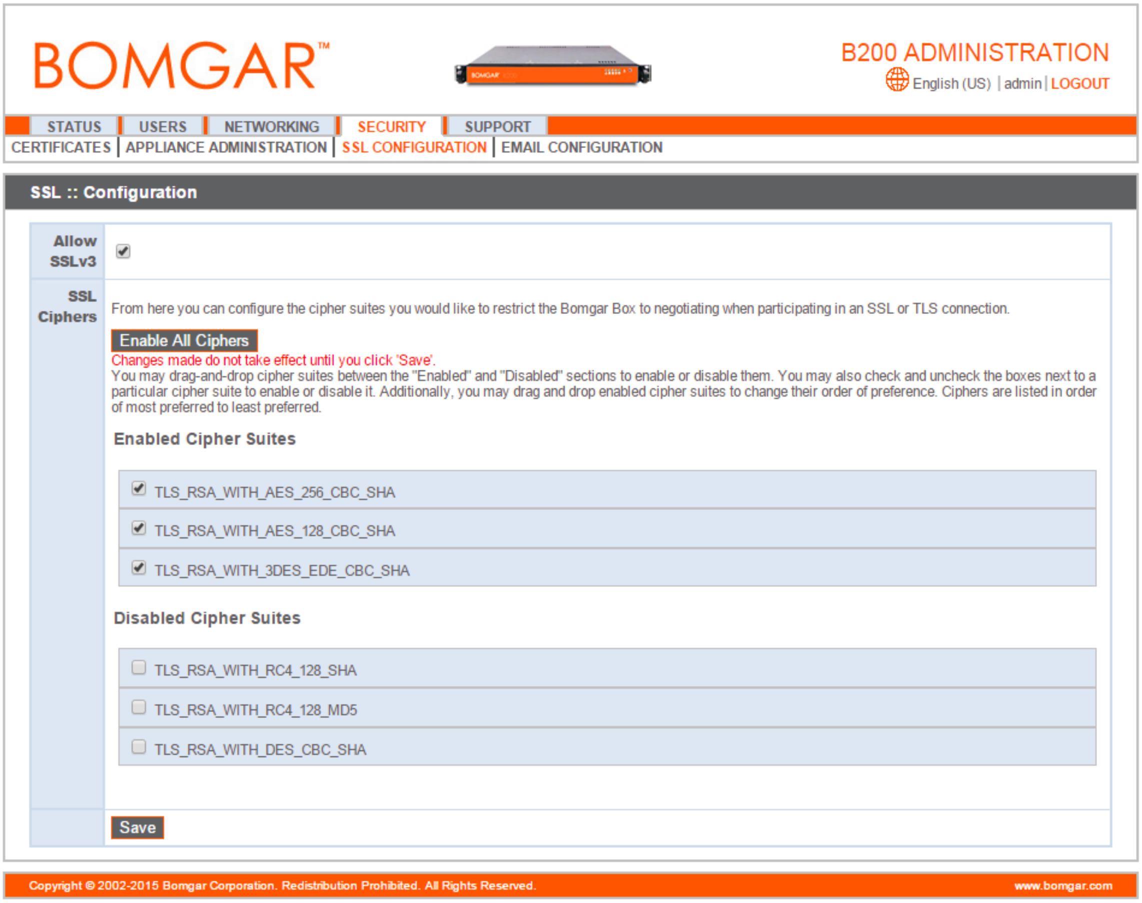
- □ TLS_RSA_WITH_RC4_128_SHA
- □ TLS_RSA_WITH_RC4_128_MD5
- □ TLS_RSA_WITH_DES_CBC_SHA

Copyright © 2002-2015 Bomgar Corporation. Redistribution Prohibited. All Rights Reserved.

5. Figure below).

6. Disable SSLv3 by ensuring that the **Allow SSL v3** checkbox is cleared.

7. Ensure that only FIPS-Approved cipher suites are enabled:
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA
   - TLS_RSA_WITH_3DES_EDE_CBC_SHA
8. Click the **Save** button to commit these configuration changes.
9. Navigate to **Basics** under **Status** tab and click on **Reboot This Appliance** (see Figure below).



SSL :: Configuration

Allow SSLv3 ☑

SSL Ciphers

From here you can configure the cipher suites you would like to restrict the Bomgar Box to negotiating when participating in an SSL or TLS connection.

Changes made do not take effect until you click 'Save'.
You may drag-and-drop cipher suites between the "Enabled" and "Disabled" sections to enable or disable them. You may also check and uncheck the boxes next to a particular cipher suite to enable or disable it. Additionally, you may drag and drop enabled cipher suites to change their order of preference. Ciphers are listed in order of most preferred to least preferred.

Enabled Cipher Suites

☑ TLS_RSA_WITH_AES_256_CBC_SHA
☑ TLS_RSA_WITH_AES_128_CBC_SHA
☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA

Disabled Cipher Suites

□ TLS_RSA_WITH_RC4_128_SHA
□ TLS_RSA_WITH_RC4_128_MD5
□ TLS_RSA_WITH_DES_CBC_SHA

Copyright © 2002-2015 Bomgar Corporation. Redistribution Prohibited. All Rights Reserved.

Figure 18– SSL Configuration Page

3.1.7 Firmware/Software Version Verification

To ensure that the modules are running the validated versions of the module Firmware and Software, operators should compare the running versions to those documented in this Security Policy. To obtain the version of the Firmware, an operator must visit the /appliance site, which is the interface used by the Crypto-Officer. To obtain the software version, an operator must visit the /login site, which requires the use of the credentials of the Instance-Admin role. Upon signing in, both display the **Status** page by default, showing the version number ([“3.3.2fips (FIPS140-2) (38611)” and “12.1.6fips (38611)”], [“3.4.0fips (FIPS 140-2)

(48368)" and "13.1.3fips (48024)"], ["3.4.1fips (FIPS 140-2) (53641)" and "13.1.3fips (48024)"] , or) ["3.5.1fips (FIPS 140-2) (56959)" and "14.3.3fips (56803)"].

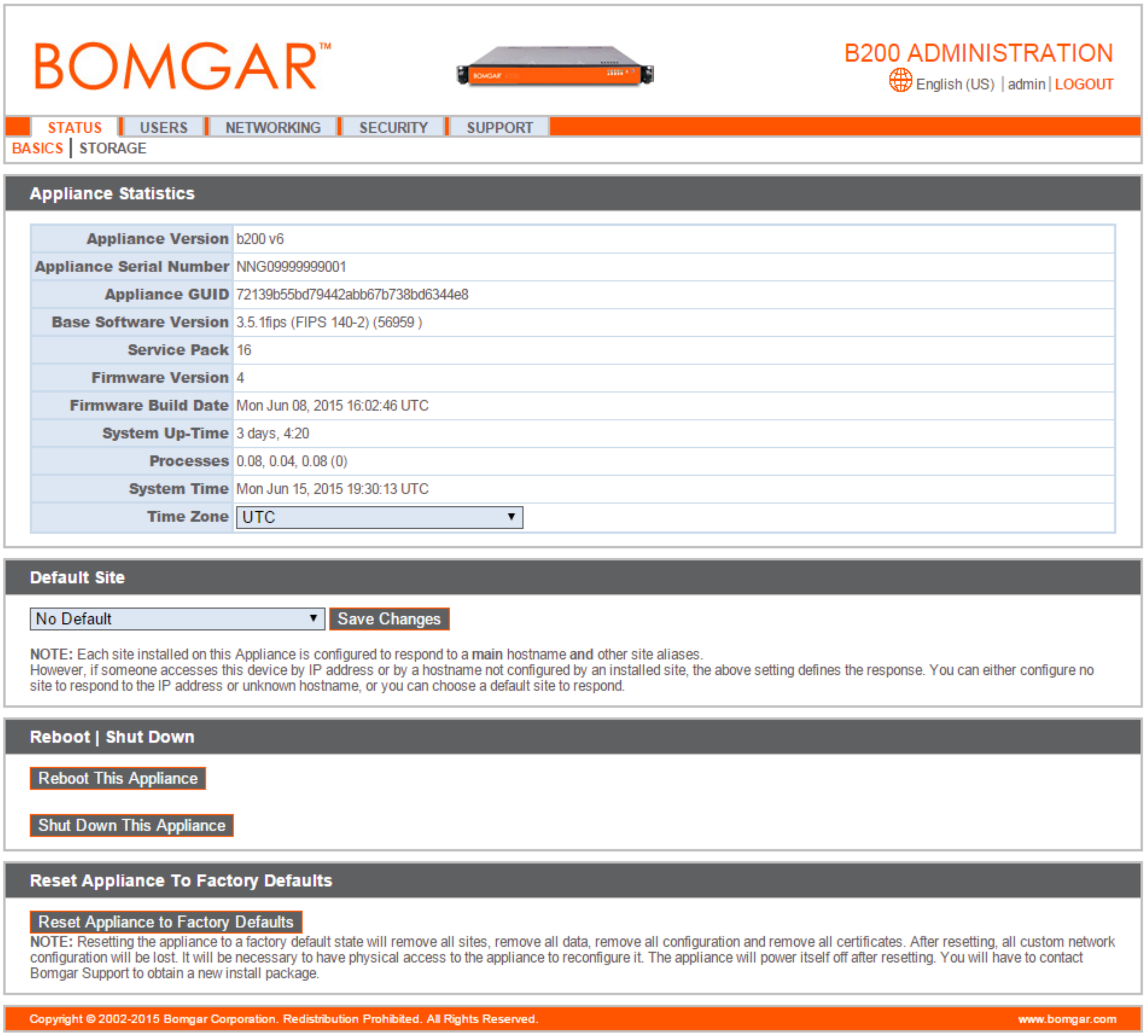
3.2 FIPS Mode Compliance

Any time the modules deviate from the configuration detailed in Section 3.1.6.1 above, the modules will be considered to be in a non-FIPS-Approved mode of operation.

Additionally, the guidance provided below must be followed to ensure that the modules remain in a FIPS-Approved mode of operation. Failure to do so will result in non-compliance.

- When entering OR leaving FIPS-Approved mode, navigate to the **Basics** page under the **Status** tab of the /appliance interface and clear all existing CSPs by clicking the **Reset Appliance to Factory Defaults** button.

  NOTE: All Firmware and Software will be completely uninstalled after reset.



Appliance Version	b200 v6
Appliance Serial Number	NNG09999999001
Appliance GUID	72139b55bd79442abb67b738bd6344e8
Base Software Version	3.5.1fips (FIPS 140-2) (56959)
Service Pack	16
Firmware Version	4
Firmware Build Date	Mon Jun 08, 2015 16:02:46 UTC
System Up-Time	3 days, 4:20
Processes	0.08, 0.04, 0.08 (0)
System Time	Mon Jun 15, 2015 19:30:13 UTC
Time Zone	UTC

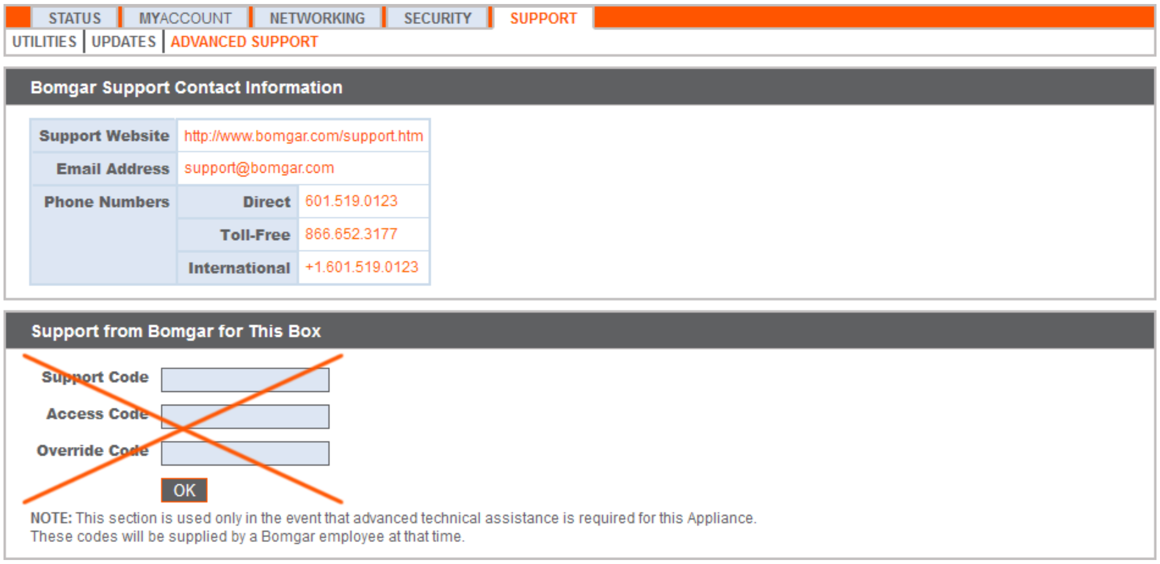
No Default

NOTE: Each site installed on this Appliance is configured to respond to a **main** hostname **and** other site aliases. However, if someone accesses this device by IP address or by a hostname not configured by an installed site, the above setting defines the response. You can either configure no site to respond to the IP address or unknown hostname, or you can choose a default site to respond.

NOTE: Resetting the appliance to a factory default state will remove all sites, remove all data, remove all configuration and remove all certificates. After resetting, all custom network configuration will be lost. It will be necessary to have physical access to the appliance to reconfigure it. The appliance will power itself off after resetting. You will have to contact Bomgar Support to obtain a new install package.

Figure 19– Status Basics Page

- Never install software or firmware versions other than those listed on the cover page of this security policy. Only the software and firmware versions listed are considered part of the validated configuration.
- When using the module's administrative interface, do not use the **Advanced Support** page under the **Support** tab of the /appliance interface. Doing so will result in non-compliance.



Bomgar Support Contact Information

Support Website	http://www.bomgar.com/support.htm	
Email Address	support@bomgar.com	
Phone Numbers	Direct	601.519.0123
	Toll-Free	866.652.3177
	International	+1.601.519.0123

Support from Bomgar for This Box

Support Code

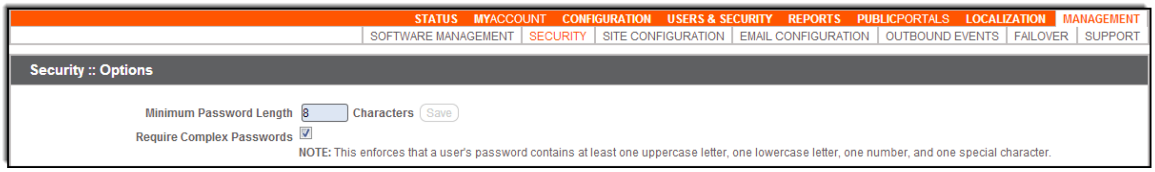
Access Code

Override Code

NOTE: This section is used only in the event that advanced technical assistance is required for this Appliance. These codes will be supplied by a Bomgar employee at that time.

Figure 0 – Advanced Support Page

- Enforce minimum password requirements for the Instance-Admin and Instance-User roles using the **Security** page under the **Management** tab of the /login interface.



Security :: Options

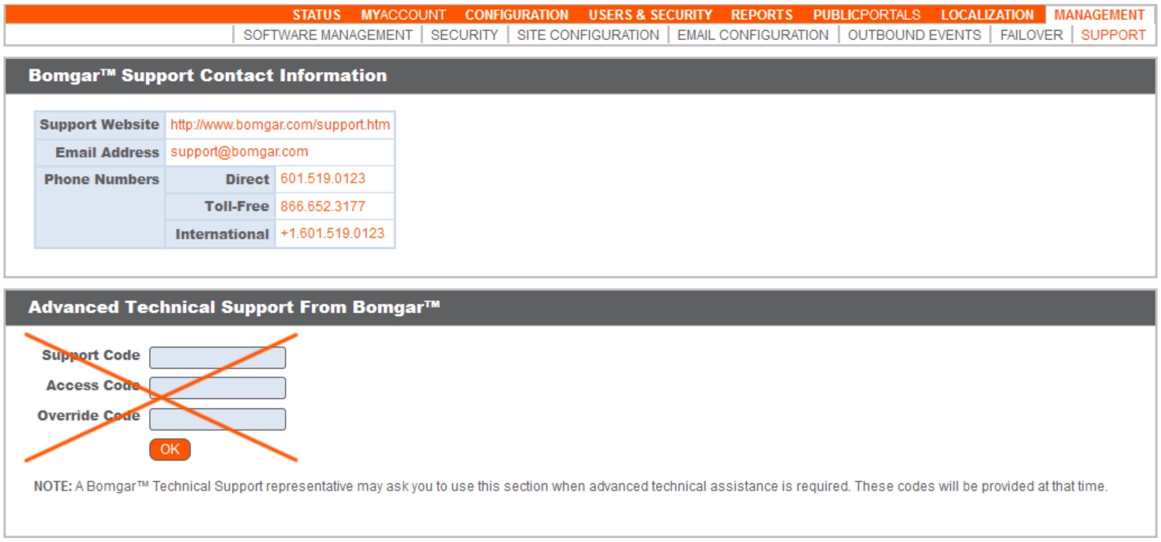
Minimum Password Length 8 Characters

Require Complex Passwords ☑

NOTE: This enforces that a user's password contains at least one uppercase letter, one lowercase letter, one number, and one special character.

Figure 1 – Security Page

- When using the management interface, do not use the **Support** page under the **Management** tab of the /login interface.



Bomgar™ Support Contact Information

Support Website	http://www.bomgar.com/support.htm	
Email Address	support@bomgar.com	
Phone Numbers	Direct	601.519.0123
	Toll-Free	866.652.3177
	International	+1.601.519.0123

Advanced Technical Support From Bomgar™

Support Code

Access Code

Override Code

NOTE: A Bomgar™ Technical Support representative may ask you to use this section when advanced technical assistance is required. These codes will be provided at that time.

Figure 162 – Support Page

- Never install a Bomgar software package via the **Software Management** page under the **Management** tab of the /login interface. Instead, ensure that any received Bomgar software packages are FIPS-Approved, and upload them from the **Updates** page under the **Support** tab of 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 Appliance Key Check for Updates functionality. To maintain compliance, only the software update versions listed in this security policy are to be used.

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 modules.

3.3.1 Management

It is the responsibility of the Crypto-Officer to ensure that the modules are set up to run securely. Please refer to Section 3.2 above for guidance that the Crypto-Officer must follow for the modules 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 modules, please refer to the appropriate Bomgar Appliance Administrative User's Guide.

3.3.2 Status Monitoring

Error message and status review is the responsibility of the Crypto-Officer. When any of a module's self-tests fail, the module reports an error message which can be viewed over a network connection. This connection is set using the **IP Configuration** page under the **Networking** tab as shown in Figure in Section 3.1.6.1 above. 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 Device
4. Reset the Device to Factory Default
5. Done

Issuing the **Show Error Message** command will display 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 (found on the **Basics** page under the **Status** tab of the /appliance interface) 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 CSPs is immediate, providing insufficient time for an attacker to compromise them. The Crypto-Officer must wait until the module has successfully rebooted in order 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 modules, with the exception of the Instance-User and their own passwords. The Instance-Admin has the ability to configure the password strength policy for Instance-Admins and Instance-Users. Please refer to Section 3.2 above for guidance that should be followed for the modules to be considered in a FIPS-Approved mode of operation.

Instance-Users do not have the ability to configure sensitive information on the modules, with the exception of 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.

Table 10 – Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSEC	Communication Security Establishment Canada
CSP	Critical Security Parameter
DMZ	Demilitarized Zone
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
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
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MD	Message Digest
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PCI	Peripheral Component Interconnect

Acronym	Definition
PKCS	Public Key Cryptography Standard
POS	Point of Sale
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
RAID	Redundant Array of Independent Disks
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
Triple DES	Triple Data Encryption Standard
TLS	Transport Layer Security
UID	Unit Identifier
USB	Universal Serial Bus
WAN	Wide Area Network