Bomgar Corporation
B200™ and B300™ Remote Support Appliances

(Hardware Versions: B200 and B300;
Firmware Version: Base version 3.0.5FIPS; Software Version: 10.2.8FIPS)

FIPS 140-2
Security Policy

Level 2 Validation

Document Version 1.0

Prepared for:

BOMGAR™

Bomgar Corporation
578 Highland Colony Parkway
Paragon Centre, Suite 300
Ridgeland, MS 39157
Phone: (601) 519-0123
Toll-Free : (866) 205-3650
Fax: (601) 510-9080
http://www.bomgar.com/

Prepared by:

Corsec®

Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050

Fax: (703) 267-6810
http://www.corsec.com/

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™ and B300™ Remote Support Appliances (running firmware Base version 3.0.5FIPS and software version 10.2.8FIPS) from Bomgar Corporation. This Security Policy describes how the B200™ and B300™ Remote Support Appliances meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. Government requirements for cryptographic modules. This document also describes 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.

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

1.2 References

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

- The Bomgar Corporation website (http://www.bomgar.com/) contains information on the full line of products from Bomgar.
- The Cryptographic Module Validation Program (CMVP) website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the module.

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 Machine document
- Executive Summary document
- Other supporting documentation as additional references

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

2 Bomgar B200™ and B300™ Remote Support Appliances

2.1 Overview

Bomgar Corporation specializes in appliance-based solutions for remote support. These Remote Support Appliances (shown in Figure 1 below) give support technicians secure remote control of computers over the internet/LAN[1]/WAN[2]. The software works through firewalls with no 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 B200 (left) and B300

The B200™ and B300™ Remote Support Appliances enable the use of remote support in multiple areas of an organization in a way that is secure, integrated and manageable. Bomgar's Remote Support Appliances integrate with LDAP[3] 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 Boxes, which allows for the review of all Customer and Support Representative interactions, including playback of all desktop screen data. They also integrate with leading systems management and identity management solutions, and include an API for deeper integration. Also with Bomgar, support managers can create support teams, customize queues and report on all support activity.

The B200™ and B300™ Remote Support 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 Boxes can work over internal and extended networks, or they can be internet accessible. This allows support organization to reduce less effective means of support by driving requests through custom support portals hosted on the appliance. The Bomgar Boxes can route support requests to the appropriate technician or team. The Bomgar Boxes then mediate connections between Customers and Support Representatives, allowing chat sessions, file downloads/uploads, remote control of desktops, screen-sharing in either direction, running of presentations, and access to system information and diagnostics.

To enable the functionality described above, Bomgar has implemented an architecture that places the Bomgar Boxes at the center of all communications (see Figure 2 below for a typical deployment scenario). The Bomgar Boxes 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 Secure HTTP (HTTPS) for authenticated services, in addition to accepting direct client connections over a proprietary Bomgar-defined protocol.

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

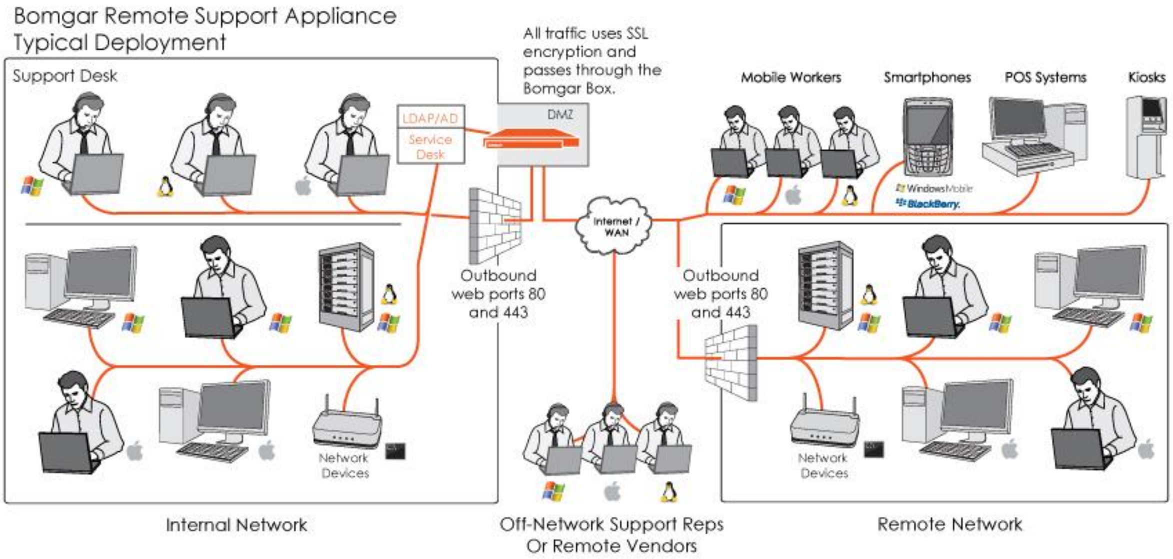

Bomgar Remote Support Appliance
Typical Deployment
Support Desk
LDAP/AD
Service Desk
All traffic uses SSL encryption and passes through the Bomgar Box.
DMZ
Mobile Workers
Smartphones
POS Systems
Kiosks
Windows Mobile
BlackBerry
Internet / WAN
Outbound web ports 80 and 443
Outbound web ports 80 and 443
Network Devices
Network Devices
Internal Network
Off-Network Support Reps Or Remote Vendors
Remote Network

Figure 2 – Typical Deployment[4]

The Bomgar Boxes have two primary binary components that provide the appliances' functionality. The first, called Base, is made up of the firmware that provides system-level configuration of a Bomgar Box. Settings such as IP[5] addresses and SSL[6] configuration are all configured via the Base interfaces. 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 Boxes.

The Bomgar B200™ and B300™ Remote Support Appliances are validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[7]
7	Cryptographic Key Management	2

[4] Rep – Representative; SSL – Secure Socket Layer; DMZ - Demilitarized Zone
[5] IP – Internet Protocol
[6] SSL – Secure Socket Layer
[7] N/A – Not applicable

Section	Section Title	Level
8	Electromagnetic Interference / Electromagnetic Compatibility	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Specification

The B200™ and B300™ Remote Support Appliances (running firmware Base version 3.0.5FIPS and software version 10.2.8FIPS) are multi-chip standalone modules that meet overall Level 2 FIPS 140-2 requirements.

Physically, the modules are composed of the components of a standard server platform. The cryptographic boundary of the modules (denoted by the blue dotted line in Figure 3 and Figure 4) is defined by the outer case of the appliances, which surrounds the complete set of hardware, firmware, and software components.

Figure 3 shows a block diagram for the B200, and identifies the various components, connections, and information flows.

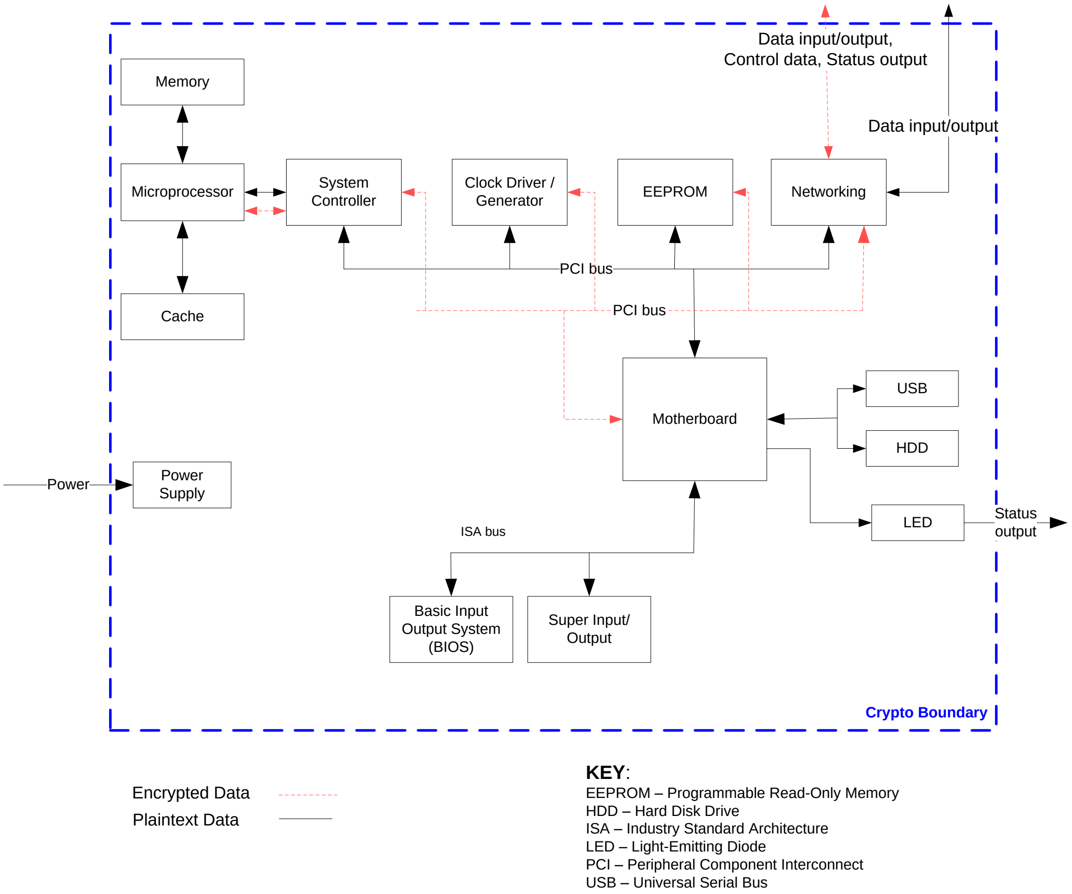


Figure 3 – Block Diagram for the B200

Figure 4 shows the same information for the B300. Note that, though Figure 4 shows a single hard disk, the B300 can support up to four to support RAID[8] functionality. Additionally, please note that the B300 power supply is <u>not</u> included the within the cryptographic boundary

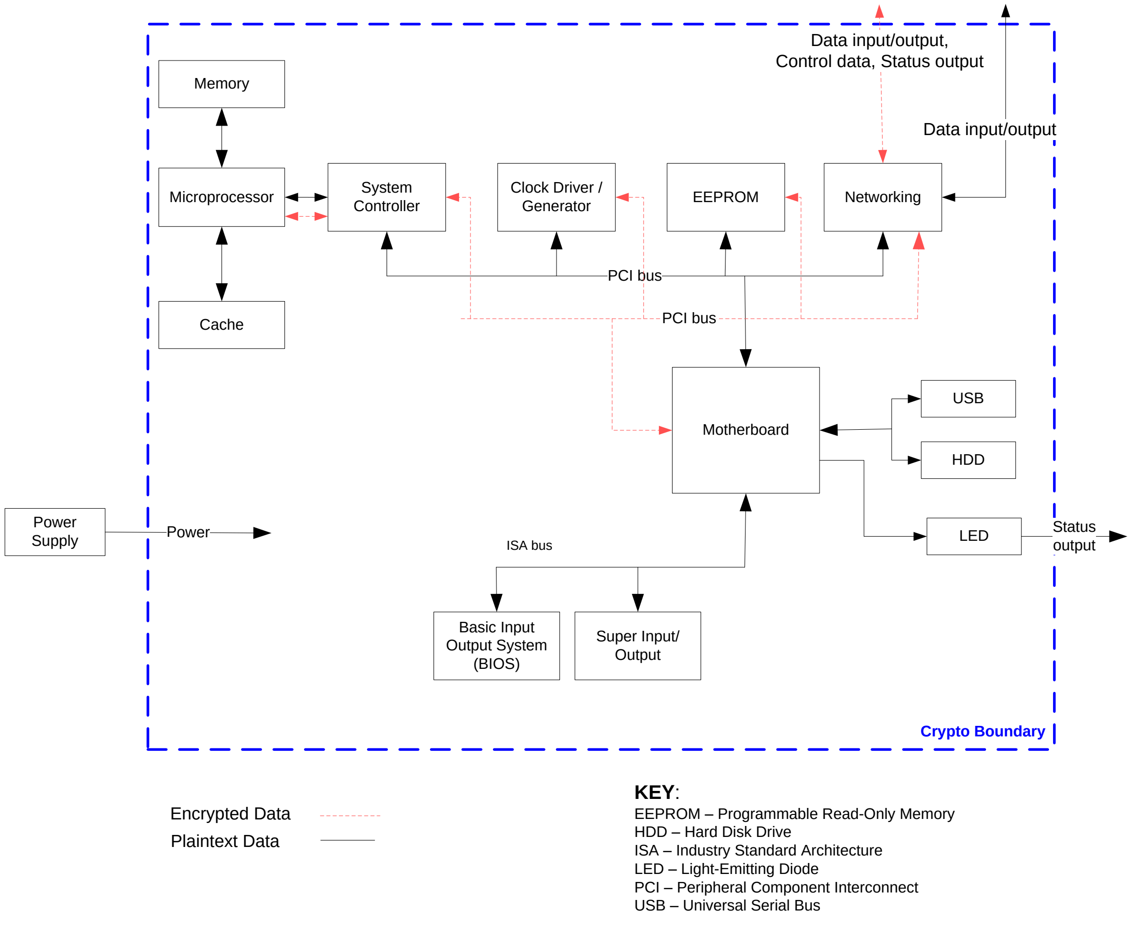


Figure 4 – Block Diagram for the B300

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
- Power Input

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 configuration and administration data

[8] RAID – Redundant Array of Independent Disks

entering the modules through the web interface and the input for the power and reset buttons. Status output consists of status information relayed via the LED[9] indicators and the web interface.

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

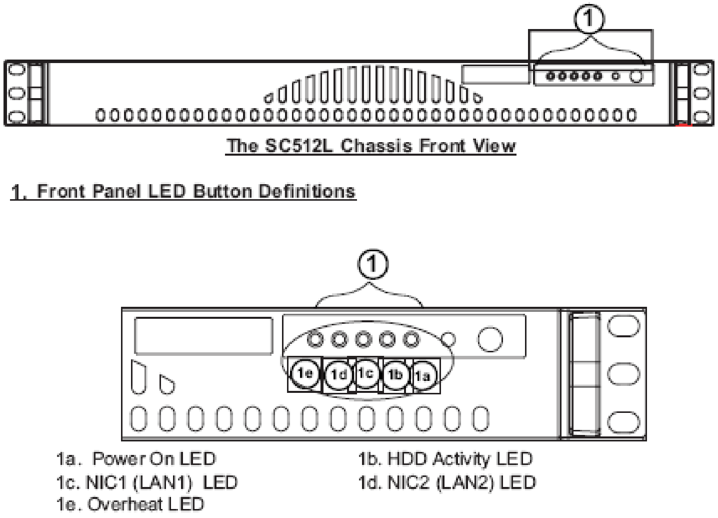


Figure 5 – Front View of B200

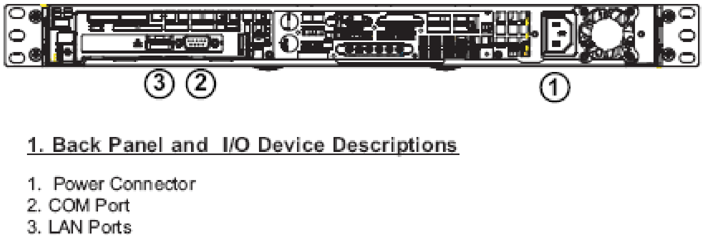


Figure 6 – Rear View of B200

[9] LED – Light Emitting Diode

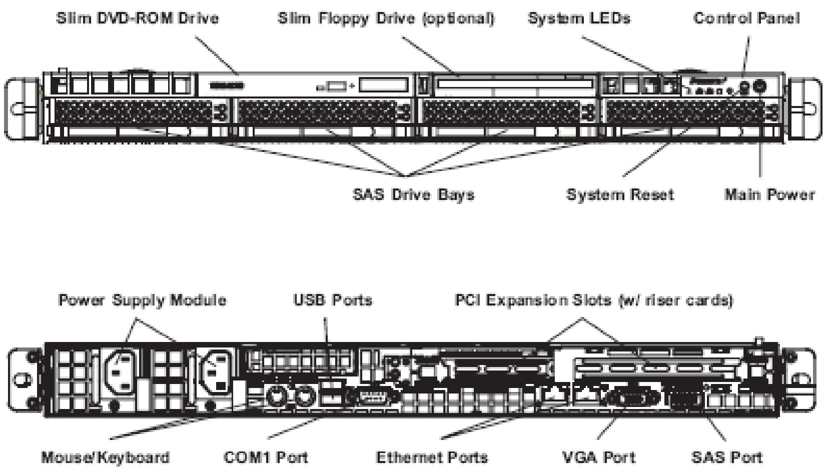


Figure 7 – Front and Rear View of B300

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 connectors
- LEDs

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

Table 2 – Physical Ports and Logical Interfaces

FIPS 140-2 Logical Interface	B200 Physical Port	B300 Physical Port
Data Input	Network ports	Network ports
Data Output	Network ports	Network ports
Control Input	Network ports, power button, reset button	Network ports, power button, reset button
Status Output	LEDs, network ports	LEDs, network ports
Power Input	Power connector	Power connectors

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

Table 3 – LED Descriptions

Model	LED	Condition	Description
B200	Power	On	System on

Model	LED	Condition	Description
		Off	System off
	Hard Disk Drive (HDD)	Blink	HDD activity
		Off	No HDD activity
	LAN1/LAN2	On	Linked
		Blink	Network activity
		Off	Disconnected
	Overheat	On	System overheat condition
		Off	System normal
B300	Power	On	System on
		Off	System off
	Hard Disk Drive (HDD)	Blink	HDD 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

2.4 Roles and Services

The modules support role-based authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role.

2.4.1 Crypto Officer Role

The Crypto Officer (CO) role is the administrator for the modules, and is responsible for the initial setup and maintenance. Descriptions of the services available to the Crypto Officer role are provided in the table below.

Table 4 – Crypto Officer Services

Service	Description	Type of Access
Monitor status	Monitor the status of the modules	Read, write, execute
Configure Bomgar Box settings	Configure IP and TLS[10] settings	Read, write, execute
Manage CO account	Manage CO account password	Read, write, execute
Configure user accounts	Setup and monitor User accounts	Read, write, execute
Execute self-tests	Perform power-up self-tests on demand	Execute
Zeroize keys	Zeroize plaintext keys	Read, write , execute

2.4.2 User Role

The User role is any Bomgar Support Representative who employs the remote support functionality provided by the Bomgar Boxes (see Table 5 below). User accounts are created and managed by the Crypto Officer, and specific features available to the User are based on the permissions set by the CO. A User does not have administrator rights to manage the modules or other users. A User cannot view or manage modules configuration or User settings.

Table 5 – User Service

Service	Description	Type of Access
Employ Support Representative functionality	Use the modules' available remote support features	Read, write, execute

2.4.3 Unauthenticated Operator Services

The module provides one service for unauthenticated operators. Its function is to provide a random identifier that is used to protect against a specific form of web browser attack. See Table 6 for that service.

Table 6 – Unauthenticated Operator Service

Service	Description	Type of Access
Generate nonce	Generate a nonce to prevent replay attacks via web browser	None

2.4.4 Authentication Mechanism

The Crypto Officer can access the modules remotely over a TLS session. The Crypto Officer authenticates to the modules using a user ID and password. Users authenticate themselves with a user ID/password combination. RSA digital certificate authentication is used during TLS sessions. Table 7 lists the authentication mechanisms used by the modules.

Table 7 – Authentication Mechanism Used by the Modules

Authentication Type	Strength

[10] TLS – Transport Layer Security

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.
RSA Public Key Certificates	The modules support RSA digital certificate authentication during TLS sessions. Using conservative estimates and equating a 1024-bit RSA key to an 80-bit symmetric key, the probability for a random attempt to succeed is $1:2^{80}$.

2.5 Physical Security

The Bomgar B200™ and B300™ Remote Support Appliances are multi-chip standalone cryptographic modules and are enclosed in a hard and opaque metal case that completely encloses all of the internal components of the modules. There are only a limited set of vent holes provided in the case, and these obscure the view of the internal components of the modules. Tamper-evident labels are applied to the case 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 Section 3 of this document.

2.6 Operational Environment

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

2.7 Cryptographic Key Management

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

Table 8 – Implemented Algorithms and Certificate Numbers

Approved Security Function	Certificate Number	
	B200	B300
Advanced Encryption Standard (AES) in CBC[11], ECB[12], and OFB[13] (8-bit and 128-bit) modes (128-bit, 192-bit, and 256-bit keys)	1043	1043
Triple Data Encryption Standard (TDES) – CBC, ECB, OFB (8-bit and 128-bit), and CFB[14] (8-bit and 64-bit) with 2- and 3-key	791	791
RSA ANSI[15] X9.31 (key generation) – 1024-, 1536-, 2048-, 3072-, and 4096-bit	497	497
RSA Public Key Cryptography Standard #1 (PKCS#1) v1.5 (sign/verify) – 1024-, 2048-, 3072-, and 4096-bit	497	497
RSA Probabilistic Signature Scheme (PSS) (sign/verify) – 1024-, 2048-, 3072-, and 4096-bit	497	497

[11] CBC – Cipher Block Chaining
[12] ECB – Electronic Codebook
[13] OFB – Output Feedback
[14] CFB – Cipher Feedback
[15] ANSI – American National Standards Institute

Approved Security Function	Certificate Number	
	B200	B300
Secure Hash Algorithm (SHA)-1, SHA-224, SHA-256, SHA-384, and SHA-512	993	993
Keyed-Hash Message Authentication Code (HMAC) using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	585	585
ANSI X9.31 A.2.4 PRNG	594	594

The module also supports 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)
- RC4
- RC4-40
- DES
- DES-40
- MD5

The module supports the CSPs listed in Table 9 below.

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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA private key pair	1024-, 1536-, 2048-, 3072-, or 4096-bit RSA key	Internally generated	Exits in encrypted form	Hard disk in plaintext	By command or overwritten by another key or by factory reset	Key exchange for TLS sessions
Session key	256-bit AES CBC 128 key, or 192-bit TDES 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
Crypto Officer password	6-character minimum password	Enters the module in encrypted form	Never exits the modules	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the CO
User password	6-character minimum password	Enters the module in encrypted form	Never exits the modules	Hard disk in hashed form	Overwritten by another password or zeroized by factory reset	Authenticates the 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

2.8 EMI/EMC

The modules were tested and found conformant to the EMI/EMC[16] 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

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

- Firmware integrity check using a SHA-1 EDC[17]
- AES Known Answer Test (KAT)
- TDES KAT
- RSA KATs (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 modules enters an error state, logs the error to a file, and disables all cryptographic operations.

The Bomgar Boxes 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.
- Continuous RNG test for entropy gathering: Verifying the correct operation of the seeding mechanism for the FIPS 182-2 PRNG.
- RSA pair-wise consistency check (sign/verify): Verifying that a newly generated RSA key pair works properly.

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

2.10 Design Assurance

Bomgar follows highly stabilized design procedures. The design goes through many phases of review and inspections, and implementations undergo rigorous quality assurance testing. Bomgar uses the following products for configuration management (CM) of the firmware and documentation:

- Subversion 1.6.4 (source code control and build management)
- SharePoint MOS Server 2007 (product management and user documentation)
- Agile Advantage 2006 (Network Engines Inc. hardware)

These tools are used for firmware version control, code sharing, build management, and document control.

Additionally, Microsoft Visual SourceSafe version 6.0 is used to provide configuration management for the module's FIPS documentation. This firmware provides access control, versioning, and logging.

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

[17] EDC – Error Detection Code

2.11 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.

2.12 Cryptographic Module Security Policy

As stated above, this Security Policy specifies the following for the Bomgar Boxes:

- identification and authentication policy
- services provided to the supported authorized roles
- “show status” and “self-test” services
- allowed type(s) of access to the CSPs
- the physical security mechanisms implemented

3 Secure Operation

The Bomgar B200™ and B300™ Remote Support Appliances meet Level 2 requirements for FIPS 140-2. The sections below describe how to ensure that the module is running securely.

3.1 Initial Setup

The following sections provide the necessary step-by-step instructions for the secure hardware installation of the Bomgar B200 and B300, as well as the steps necessary to configure the modules for FIPS Approved mode operation. If you have any questions or if issues arise at any point during the installation and configuration of your Bomgar Box, contact the Bomgar support team at 1-877-8-BOMGAR x2.

3.1.1 B200 Hardware Setup

In order to setup the Bomgar B200 the following steps will need to be performed by an authorized individual:

1. Inspect and apply the tamper evident labels as described in Section 3.1.2 directly below.

2. Follow the procedures included in the Hardware Setup Guide to install your B200 in your server rack.

3. After you've installed the Bomgar B200 per the Hardware Setup Guide, refer to the included Getting Started Guide and configure your network settings.

4. Once the Bomgar B200's network settings are correctly configured, return to Section 3.1.4.1 in this document to configure your B200 for FIPS mode.

3.1.2 B200 Label Inspection

The B200 will be shipped from the factory with all required labels affixed. Upon delivery an authorized individual shall take the following steps to ensure that the module was not tampered with during shipment and that the labels have been applied properly:

1. Inspect all tamper-evident labels that shipped pre-applied to the B200 chassis, ensuring that each label shows no sign of tampering. The label placement should be exactly as show in Figure 8, Figure 9, Figure 10, and Figure 11 and in addition should not show any signs of removal or tampering. If you find a label that is questionable in appearance, contact Bomgar support at 1-877-8-BOMGAR x2.

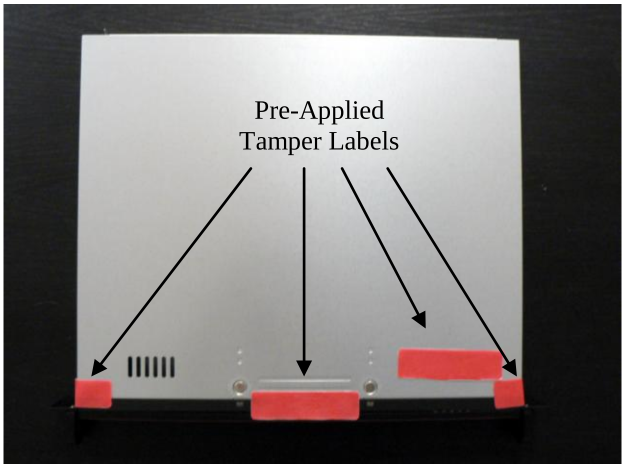


Figure 8 – B200 Top Label Placement

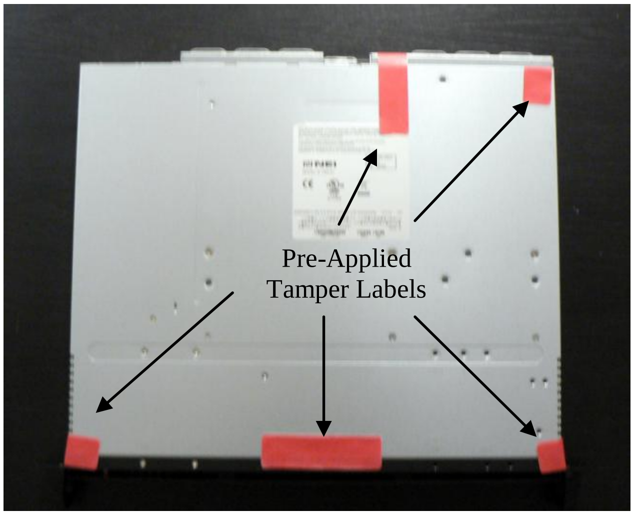


Figure 9 – B200 Bottom Label Placement

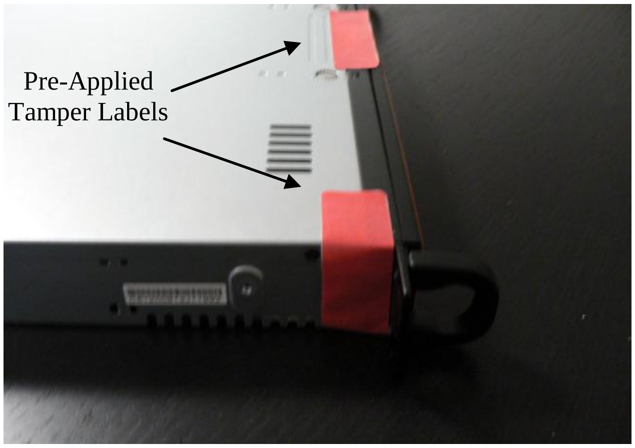


Figure 10 – B200 Left Top Label Placement

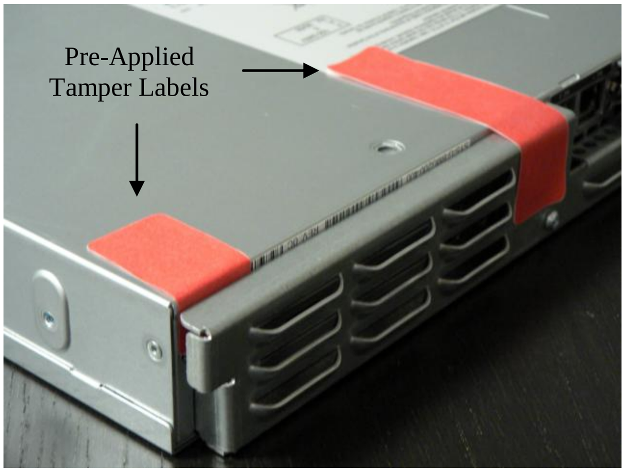


Figure 11 – B200 Rear Vent Label Placement

3.1.3 B300 Hardware Setup

In order to setup the Bomgar B300 the following steps will need to be performed by an authorized individual:

1. Unpack the Bomgar B300 and remove the front bezel from the front of the B300.
2. Loosen the set screw on the right side of the front bezel. This screw keeps the tab in place during shipping.
3. Press the tab on the right side of the front bezel and pull the front bezel towards you, right side first.
4. 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 Bomgar 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.
5. 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 then tighten the set screw. Take care not to over tighten this screw.
6. Inspect and apply the tamper-evident labels as described in Section 3.1.4.
7. Follow the procedures included in the Hardware Setup Guide to install your B300 in your server rack.
8. After you've installed the Bomgar B300 per the Hardware Setup Guide, refer to the included Getting Started Guide and configure your network settings.
9. Once the Bomgar B300's network settings are correctly configured, return to Section 3.1.4.1 in this document to configure your B300 for FIPS mode.

3.1.4 B300 Label Inspection and Application

The B300 will be shipped from the factory with all required labels pre-applied except for the two front bezel labels. This is to allow the end-user to reseat the drives upon receipt before affixing the front bezel to the appliance. Upon delivery an authorized individual shall take the following steps to ensure that the module was not tampered with during shipment and that the labels have been applied properly:

1. Inspect all tamper-evident labels that shipped pre-applied to the Bomgar B300 chassis (see Figure 12 Figure 13 and Figure 14), ensuring that each label shows no sign of tampering and is properly placed. If you find a label that is questionable in appearance, contact Bomgar support at 1-877-8-BOMGAR 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 (see Figure 12 and Figure 13).

3. Holding label by edges, place label on surface as indicated in Figure 12 and Figure 13.

4. Apply the included tamper-evident labels by rubbing gently across 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 within a physically secure environment before placing into the intended environment.

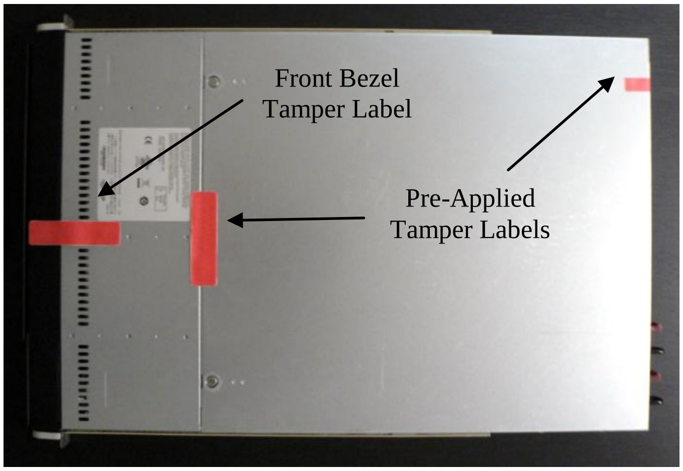


Figure 12 – B300 Top Label Placement

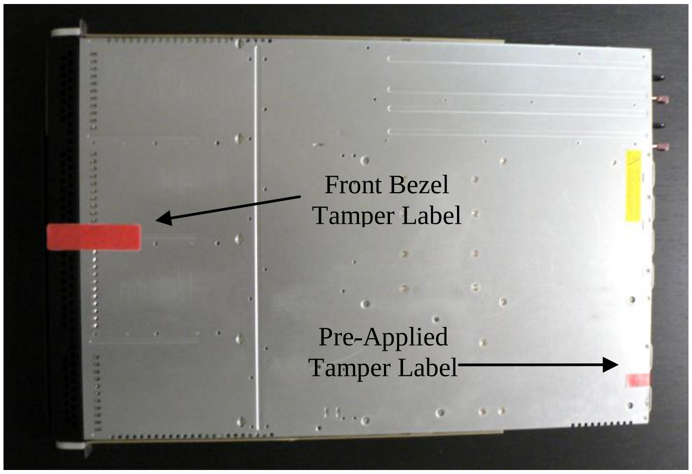


Figure 13 – B300 Bottom Label Placement

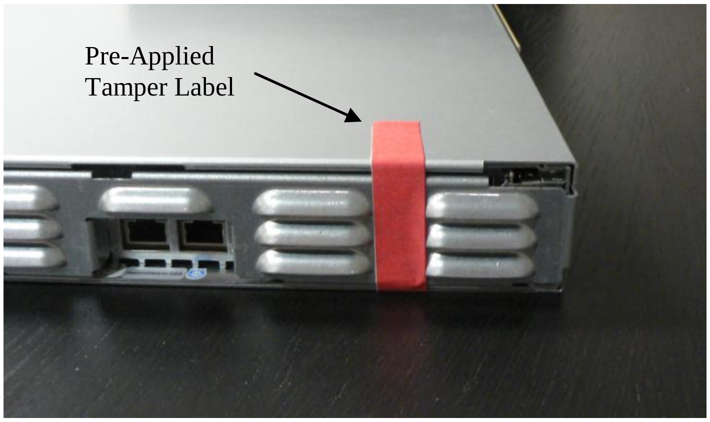


Figure 14 – B300 Rear Vent Label Placement

3.1.4.1 B200 and B300 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 will be considered to be in FIPS-Approved mode, which can be verified at any time by viewing the Security Tab configuration and ensuring it matches Figure 15 (NOTE: Figure 15 is identical for both the B200 and 300 with the exception of the heading).

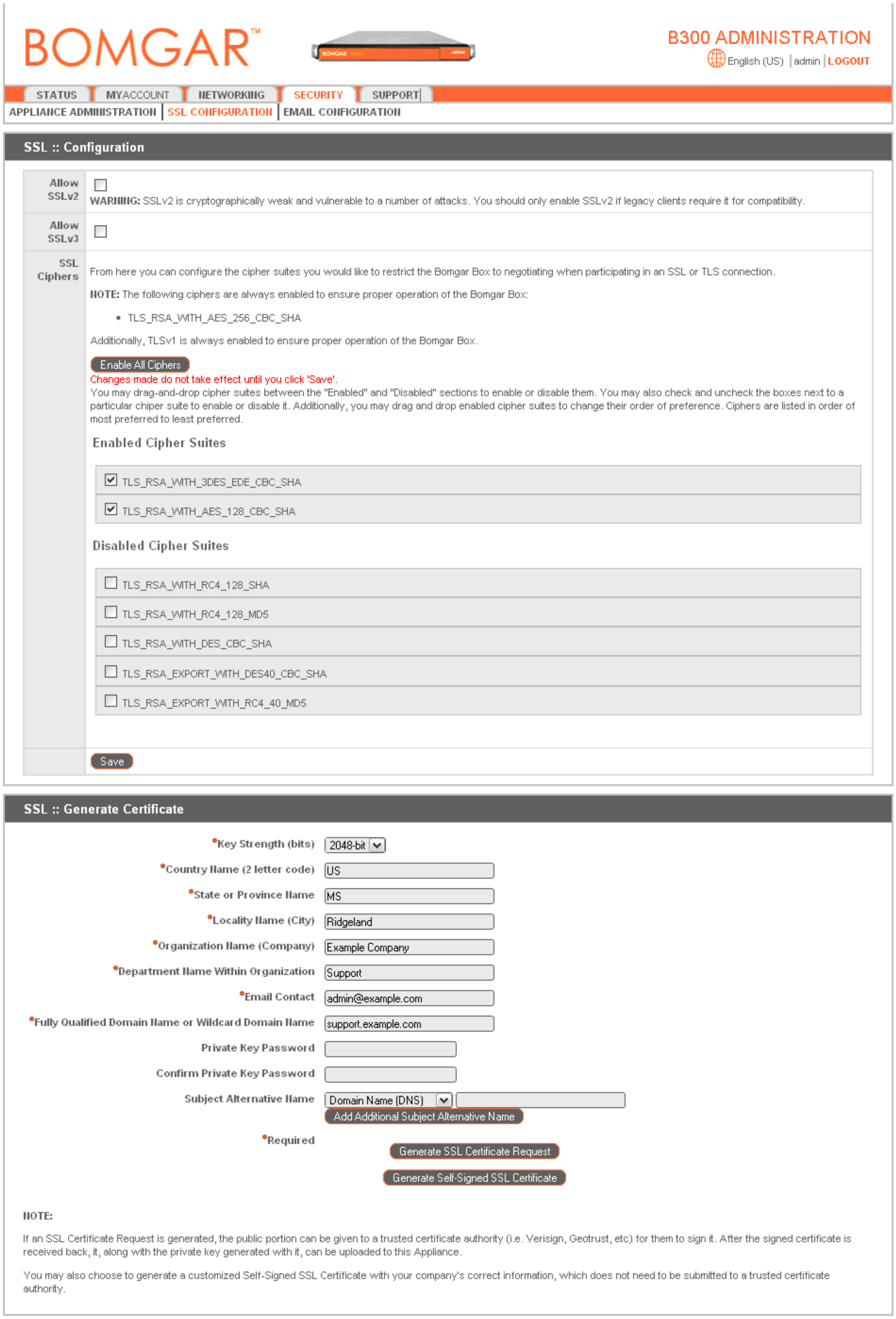
FIPS-Approved Mode Configuration

Log into the Bomgar Administrative Interface (e.g. support.example.com/appliance/) and configure your settings as described below[18]:

1. Navigate to the **SSL Configuration** page under the **Security** tab (see Figure 15 below).

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

2. Disable SSLv2 by ensuring that the **Allow SSLv2** checkbox is cleared.
3. Disable SSLv3 by ensuring that the **Allow SSLv3** checkbox is cleared
4. Ensure that only FIPS-Approved cipher suites are enabled:
    a. TLS_RSA_WITH_3DES_EDE_CBC_SHA
    b. TLS_RSA_WITH_AES_128_CBC_SHA
5. Click the **Save** button to commit these configuration changes.
6. When generating an SSL Certificate, do NOT specify a private key password prior to generating the certificate.



SSL :: Configuration

Allow SSLv2 □
WARNING: SSLv2 is cryptographically weak and vulnerable to a number of attacks. You should only enable SSLv2 if legacy clients require it for compatibility.

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.

NOTE: The following ciphers are always enabled to ensure proper operation of the Bomgar Box:

- TLS_RSA_WITH_AES_256_CBC_SHA

Additionally, TLSv1 is always enabled to ensure proper operation of the Bomgar Box.

Enable All Ciphers

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 chiper 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_3DES_EDE_CBC_SHA
☑ TLS_RSA_WITH_AES_128_CBC_SHA

Disabled Cipher Suites

□ TLS_RSA_WITH_RC4_128_SHA
□ TLS_RSA_WITH_RC4_128_MD5
□ TLS_RSA_WITH_DES_CBC_SHA
□ TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
□ TLS_RSA_EXPORT_WITH_RC4_40_MD5

Save

SSL :: Generate Certificate

•Key Strength (bits)	2048-bit
•Country Name (2 letter code)	US
•State or Province Name	MS
•Locality Name (City)	Ridgeland
•Organization Name (Company)	Example Company
•Department Name Within Organization	Support
•Email Contact	admin@example.com
•Fully Qualified Domain Name or Wildcard Domain Name	support.example.com
Private Key Password	
Confirm Private Key Password	
Subject Alternative Name	Domain Name (DNS) Add Additional Subject Alternative Name

•Required

Generate SSL Certificate Request

Generate Self-Signed SSL Certificate

NOTE:

If an SSL Certificate Request is generated, the public portion can be given to a trusted certificate authority (i.e. Verisign, Geotrust, etc) for them to sign it. After the signed certificate is received back, it, along with the private key generated with it, can be uploaded to this Appliance.

You may also choose to generate a customized Self-Signed SSL Certificate with your company's correct information, which does not need to be submitted to a trusted certificate authority.

Figure 15 – SSL Configuration Page

3.1.5 Firmware/Software Version Verification

To ensure that the module is 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 Base 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 User role. Upon signing in, both display the "Status" page by default showing the version number.

3.2 FIPS Mode Compliance

Any time the module deviates from the configuration detailed in Section 3.1.4.1 above, the module 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 module remains in its 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 and clear all existing CSPs by clicking the **Reset to Factory Defaults** button.

  NOTE: All firmware and software will be completely uninstalled after reset.

- Never install a non-FIPS-validated version of the Bomgar software.
- When using the module's administrative interface, do not use the **Advanced Support** page under the **Support** tab.
- When using the management interface, do not use the **Support** page under the **Management** tab.
- Never install a Bomgar software package via the **Software Management** page under the **Management** tab. Instead, ensure that any received Bomgar software packages are FIPS-Approved, and upload them from the **Updates** page under the **Support** tab of the administrative interface (e.g. support.example.com/appliance/).

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 modules are set up to run securely. Please refer to Section 3.1 above for guidance that the Crypto Officer must follow for the modules to be considered in a FIPS-Approved mode of operation.

For details regarding the management of the modules, please refer to the appropriate Bomgar Box Administrative User's Guide.

3.3.2 Zeroization

Session keys are zeroized at the termination of the session, but are also cleared when the modules are power-cycled. All other CSPs may be zeroized by issuing the **Reset to Factory** command and rebooting the modules. The Crypto Officer must wait until the modules have successfully rebooted in order to verify that zeroization has completed.

3.4 User Guidance

The User does not have the ability to configure sensitive information on the modules, with the exception of their password. The User must be diligent to pick strong passwords, and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession.

4 Acronyms

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AGP	Accelerated Graphics Port
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
DMZ	Demilitarized Zone
ECB	Electronic Codebook
EDC	Error Detection Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
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	Secure Hypertext Transfer Protocol
IP	Internet Protocol
ISA	Industry Standard Architecture
KAT	Known Answer Test
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme

Acronym	Definition
RAID	Redundant Array of Independent Disks
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
WAN	Wide Access Network