4281 Katella Ave
Suite 100
Los Alamitos, CA 90720

Black Lantern®

Guidance Documentation

Version 1.1
September 1, 2022

Table of Contents

1 Common Criteria Introduction 7
1.1 Target of Evaluation (TOE) 7
1.2 Conformance Claims 7
1.3 Acronyms 9
1.4 Cryptography Support 10
1.5 Operational Environment 10
1.6 Delivery Configuration 13

2 Hardware Overview 14
2.1 Black Lantern 300 Specifications 14
2.1.1 Dimensions 14
2.1.2 Power 15
2.1.3 Environmental 15
2.1.4 Ports 15
2.2 Black Lantern 400 Specifications 16
2.2.1 Dimensions 16
2.2.2 Power 16
2.2.3 Environmental 17
2.2.4 Ports 17
2.3 Connectivity 17
2.3.1 Serial Console RS232 (RJ45) 17
2.3.2 Management Port (RJ45) 17
2.3.3 Service Ports (SFP+ and RJ45) 17
2.4 Network Interfaces, Protocols, and Ports 18
2.4.1 Management Interfaces 18
2.4.2 Service Interfaces 18

3 Security Overview 18
3.1 Environment Requirements 18
3.1.1 Physical Separation of Service and Management Interfaces for Out of Band (OOB) Management 18
3.1.2 Firewall Configuration 19
3.1.3 Serial Management Interface 19
3.2 Management Guidance 19
3.2.1 Physical separation of management traffic 20
3.2.2 TLS Communication 20
3.2.3 Operation and Maintenance (O&M) Access 20
3.2.3.1 Accounts and Roles 20
3.2.3.2 Password Policies 21
3.2.3.2.1 Password entropy rules 21
3.2.3.2.2 Minimum Password Length 21
3.2.3.2.3 Password expiration 21
3.2.3.2.4 Force change on reset password 21
3.2.3.3 Account Disable and Expiration 21
3.2.3.4 Serial Terminal Session Timeout 22
3.3 Black Lantern Software Updates and Patches 22

4 Black Lantern Installation 22
4.1 Safety Information 22
4.1.1 Definition of Safety Warnings 22
4.1.2 General Safety 23

4.2 Hardware Setup 24
4.2.1 Packing List 24
4.2.2 BL300 Rack Installation 24
4.2.3 BL400 Rack Installation 26
4.3 Connectivity 26
4.4 Network Configuration 27
4.4.1 Network Configuration Setup Procedure 28
5 Initial Configuration 31
5.1 Local Login 31
5.1.1 Configuring Local Login 32
5.2 Remote Login 35
5.2.1 Configuring Remote Login 35
5.2.1.1 Importing Localhost Certificate and Certificate Authority (CA) Chain (as identity of the Black Lantern) 37
5.2.1.1.1 Key Generation 37
5.2.1.1.2 Certificate Signing Request (CSR) generation 37
5.2.1.2 Importing Remote Host CA Chain 39
5.3 Secure Communication 40
5.3.1 Client Mode Configuration 41
5.3.1.1 Trusted Communication Channel with a Remote Logging Server 41
5.3.2 Server Mode Configuration 43
5.3.2.1 Trusted Communication Path with Remote Management Client 43
5.3.3 Additional Related Information 44
5.3.3.1 Random Number Generation 44
5.3.3.2 Key Generation 44
5.3.3.3 Key Establishment 45
5.3.3.3.1 Elliptic Curve-based Key Establishment 45
5.3.3.4 Key Destruction 45
5.3.3.5 Hash Algorithms 45
5.3.3.6 Keyed Hashing (HMAC) 45
6 Audit Functionality 46
6.1 Configuring Remote Audit Storage 47
6.2 Configuring Local Audit Storage 47
6.2.1 Low Local Storage Space Warnings 47
6.2.2 Clearing Local Log Data 48
6.3 Viewing local audit records 48
6.4 Audit Events 50
7 Management 60
7.1 TSF Data 60
7.1.1 User Roles 60
7.2 Security Settings 62
7.2.1 Configuration 62
7.2.2 Password Guidance 63
7.3 Login Banner 64
7.4 Internet Control Message Protocol (ICMP) 64
7.5 Time Synchronization 65
7.5.1 NTP Settings 65
7.5.2 Setting Time Manually 65
7.6 Self Test 66
7.7 Software Updates 69

8 Appendix A: Serial Console Interface Command Reference 72
8.1 Security Admin........ 72
8.2 Network Admin 81
8.3 Recovery-Agent........ 86
9 Appendix B: RESTful APIs 90
9.1 Overview........ 90
9.2 Additional Error Handling 90
9.2.1 Error Response 90
9.2.2 Error Code 90
9.2.2.1 Domain Prefix 90
9.2.2.2 Error Codes 91
9.3 Config RESTful Endpoint 91
9.3.1 Purpose 91
9.3.2 URI 91
9.3.3 GET Method........ 92
9.3.3.1 Request........ 92
9.3.3.1.1 Additional HTTP Headers 92
9.3.3.1.2 Query Options........ 92
9.3.3.2 Response 92
9.3.3.2.1 Payload Schema........ 92
9.3.3.2.2 Payload Example 93
9.3.4 PUT Method........ 93
9.3.4.1 Request........ 93
9.3.4.1.1 Additional HTTP Headers 93
9.3.4.1.2 Payload Schema........ 94
9.3.4.1.3 Payload Example 94
9.3.4.2 Response 94
9.4 Status RESTful Endpoint 95
9.4.1 Purpose 95
9.4.2 URI 95
9.4.3 GET Method........ 95
9.4.3.1 Request........ 95
9.4.3.1.1 Additional HTTP Headers 95
9.4.3.1.2 Query Options........ 95
9.4.3.2 Response 95
9.4.3.2.1 Payload Schema........ 95
9.4.3.2.2 Payload Example 96
9.4.4 PUT Method........ 96
9.4.4.1 Request........ 96
9.4.4.1.1 Additional HTTP Headers 96
9.4.4.1.2 Payload Schema........ 97
9.4.4.1.3 Payload Example 97
9.4.4.2 Response 97
9.5 User RESTful Endpoint 97
9.5.1 Purpose 97
9.5.2 URI 97
9.5.3 GET Method........ 98
9.5.3.1 Request........ 98
9.5.3.1.1 Additional HTTP Headers 98
9.5.3.2 Response 98
9.5.3.2.1 Payload Schema........ 98
9.5.3.2.2 Payload Example 99
9.5.4 PUT Method........ 99

9.5.4.1 Request 99
9.5.4.1.1 Additional HTTP Headers 99
9.5.4.1.2 Payload Schema 99
9.5.4.1.3 Payload Example 101
9.5.4.2 Response 101
10 Appendix C: Black Lantern Configuration 102

List of Tables

Table 1: TOE Management Functions 19
Table 2: Summary of Black Lantern Supported Roles 20
Table 3: Black Lantern 300 Appliance Packing List 24
Table 4: Black Lantern 400 Appliance Packing List 24
Table 5: Black Lantern Network Ports States at Factory Reset 27
Table 6: Black Lantern Supported Asymmetric Key Sizes 37
Table 7: Syslog Protocol Mapping 46
Table 8: Black Lantern Audit Events 51
Table 9: Functions for Managing TSF Data 60
Table 10: Black Lantern Configuration DB v2.0 102

Table of Figures

Figure 1: Black Lantern Operational Environment 11
Figure 2: Black Lantern 300 Physical Dimensions 14
Figure 3: Black Lantern 300 Ports 15
Figure 4: Black Lantern 400 Physical Dimensions 16
Figure 5: Black Lantern 400 Ports 17
Figure 6: Black Lantern Installation 25
Figure 7: Black Lantern 300 Port Connectivity 26
Figure 8: Black Lantern 400 Port Connectivity 27
Figure 9: Guardtime Federal Delivery Process 31
Figure 10: Required Certificate Storage and Interchange for TLS Communication 36
Figure 11: Black Lantern Certificate Loading Order 36

1 Common Criteria Introduction

1.1 Target of Evaluation (TOE)

The Target of Evaluation (TOE) is the Guardtime Federal's Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS. Throughout this report, the term TOE and Black Lantern will be used interchangeably. The Black Lantern is a secure network device appliance that is an integrated hardware and software platform purposely built to mitigate both remote and physical attacks against a customer infrastructure and applications. The Black Lantern comes with a built-in KSI® gateway and extender, which allows for secure implementation of KSI-based data assurance and cybersecurity solutions with built-in active anti-tamper measures.

The product numbers of the Black Lantern under evaluation are BL300-B2, BL300-C2, and BL400-A1:

- BL = Black Lantern Appliance Type
- 300 or 400 = Denotes Black Lantern Module
- A1 = Revision of new model
- B2 = Hardware revision, letter (B): major, digit (2) = minor

The BL300-C2 is equipped with higher accuracy oscillators compared to the BL300-B2. These oscillators allow the BL300-C2 to have a smaller drift from true time: 1) in the event it's not communicating with NTP server, and 2) while it's been powered OFF. The BL400-A1 also includes high accuracy oscillators. The upgraded hardware functionality does not affect any of the security requirements of the [NDcPPv2.2E].

The complete part number is BL300-B2-AC-GAE

- AC = Power supply option -- expecting AC power supply.
- GAE = Gateway, Aggregator, Extender

GAE are KSI related applications that are independent of what is required to comply with the collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [NDcPP]. The TOE's software version under evaluation is BLKSI.2.2.1-FIPS. Sections 2 and 3, respectively, provide a further overview of the Black Lantern's hardware and security features. Note that only interfaces and commands relevant to the security functions specified in the Security Target were evaluated and tested for conformance against the NDcPP.

1.2 Conformance Claims

To comply with Commercial Solutions for Classified (CSfC) Selections for Transport Layer Security (TLS) Protected Servers last updated on 07-19-2021, the Security Administrator must utilize the Black Lantern in the following supported configuration for each category:

TLS Server Protocol (FCS_TLSS_EXT.1)

- ECDHE key establishment must be limited to using P-384 curve.

Cryptographic Key Generation (FCS_CKM.1)

- ECC key generation must be limited to using P-384 curve.
- RSA key generation must be limited to using 4096 bit modulus.

Cryptographic Key Establishment (FCS_CKM.2)

- Elliptic curve-based key establishment schemes (this is the only scheme supported; therefore no configuration is necessary)

Cryptographic Operation (FCS_COP.1/DataEncryption)

- AES encryption/decryption must be limited to using 256 bits key size.

Cryptographic Operation (FCS_COP.1/SigGen)

- RSA digital signature generation/verification must be limited to using 4096 bits key size.
- ECDSA digital signature generation/verification must be limited to using P-384 curve.

Cryptographic Operation (FCS_COP.1/Hash)

- Hash operations must be limited to using SHA-256, SHA-384 or SHA-512[1].

Cryptographic Operation (FCS_COP.1/KeyedHash)

- Keyed-hash MAC generation must be limited to using HMAC-SHA-384[2].

In addition to the configuration steps detailed in other sections of this guide for conformance to Common Criteria (CC), the following steps must be taken to ensure the proper configuration for environments also requiring CSfC conformance.

Generate and load certificates with only RSA 4096-bit or ECC P-384 cryptographic keys following the instructions in Sections 5.2.1.1 and 5.2.1.2.

Use the following setconfig command to enable CSfC compliance:

Key Name	Description (Refer to Section 10)
management.csfcmode	Enable/Disable Commercial Solutions for Classified (CSfC) compliance. Set to “1” to enable and “0” to disable.

Enabling this setting limits the presented elliptic curves to secp384r1 and restricts the use of digital signatures as specified above.

[1] Note that the TOE supports the use of SHA-1 for NTP authentication only. It is not supported for TLS.

[2] Note that the TOE uses HMAC-SHA-256 in support of PBKDF only. It is not used with TLS.

The Black Lantern firmware automatically enables FIPS mode which ensures all other settings are enforced (e.g. Hash operations are limited to using SHA-256, SHA-384 or SHA-512 in TLS communications). No other configuration is required for CSfC or CC conformance.

1.3 Acronyms

Item	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
BL	Black Lantern
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CLI	Command Line Interface
CN	Common Name
CR	Condition Register
CSfC	Commercial Solutions for Classified
CSL	Cryptographic Support Library
CSR	Certificate Signing Request
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GPR	General Purpose Register
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS, or HTTP secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
IV	Initialization Vector
JSON	JavaScript Object Notation
KSI	Keyless Signature Infrastructure
NDcPP	Network Device collaborative Protection Profile
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OOB	Out-of-Band
PCIe	Peripheral Component Interconnect Express
PBKDF2	Password-Based Key Derivation Function 2
POST	Power On Self Test
RAM	Random Access Memory
REST	Representational State Transfer
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman

Item	Description
SAN	Subject Alternative Name
SCI	Serial Console Interface
SDK	Software Development Kit
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SPR	Special Purpose Register
SRAM	Static Random Access Memory
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.4 Cryptography Support

The TOE leverages the cryptographic capabilities of the NXP T4240r2 QorIQ processor and security engine, secure real time operating system software, and cryptography libraries to provide cryptographic algorithms and support cryptographic protocols, including TLS and HTTPS. To satisfy the cryptographic requirements specified in [NDcPP], Guardtime Federal’s Cryptographic Support Library (CSL) Direct module implements each of the required cryptographic algorithms, which are certified via the NIST Cryptographic Algorithm Validation Program (CAVP). No configuration is necessary to enable the CSL Direct module and/or FIPS mode.

The cryptographic mechanisms support cryptographic protocols used for secure communication—TLS (both as client and server and with RESTful Interface utilizing mutual authentication), HTTPS, and NTP.

1.5 Operational Environment

The following figure provides a graphical representation of the operational environment of the Black Lantern. The figure depicts the connectivity of the KSI application entities (not applicable to NDcPP) as well as the IT entities that enable the compliance with the NDcPP requirements.

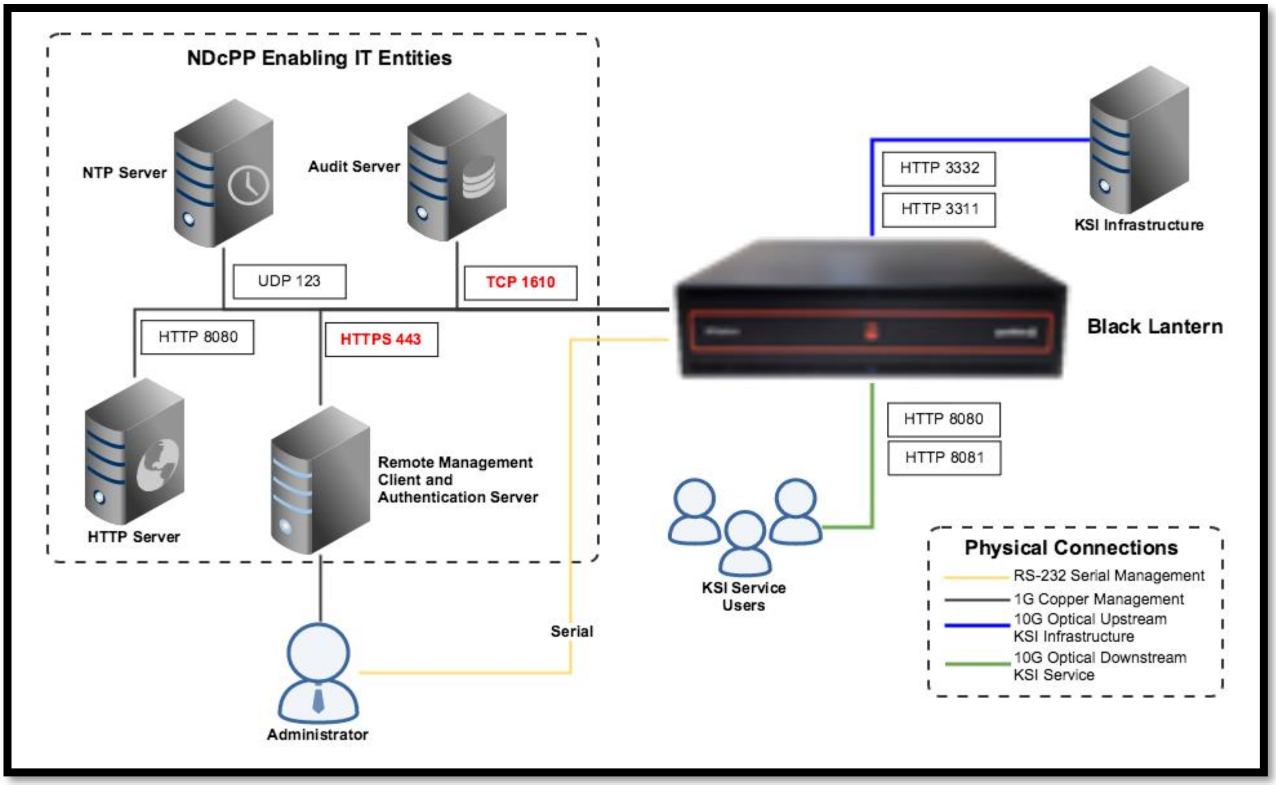


Figure 1: Black Lantern Operational Environment

Figure 1 combines the physical and logical interconnectivity of the Black Lantern to external IT entities and users. All network connections are associated with a port the Black Lantern uses for specific communication; the ports are configurable. Secured ports are designated with color red.

All IT entities that enable the Black Lantern to comply with the NDcPP requirements are connected to the Black Lantern via its serial or management interface. The following are the required entities:

- Local Management: NDcPP requires the TOE (Black Lantern) to provide the capabilities to be managed locally. Local management of the Black Lantern is performed via the RS-232 serial interface, which provides access to its Serial Console Interface (SCI). All management commands and configurations of the Black Lantern are accessible via this interface by the appropriate administrator user. For this interface, the Black Lantern uses its local authentication mechanisms to grant access to the administrator.
- Remote Management: NDcPP requires the TOE to be able to be managed remotely. The Black Lantern provides a RESTful Interface that enables it to be managed remotely by an administrator making requests with calls to the Black Lantern’s RESTful application program interface (API).
- Syslog Server: NDcPP requires the TOE (Black Lantern) to send logs to an external remote logging server over a secured channel.

The non-required IT entities that help the Black Lantern comply with NDcPP requirements are:

- NTP Server: The Black Lantern supports synchronization to NTP servers, which helps comply with the requirement of providing reliable time services. For more information refer to Section 7.5.1.
- HTTP Server: The Black Lantern supports connection to an HTTP server for the purpose of updating the software in the Black Lantern. For more information refer to Section 7.7.

The non NDcPP IT entities are the ones associated with providing KSI services. The Black Lantern utilizes the additionally supported network interface connections to provide KSI services to the service users. The following are the types of connections required to provide KSI services. The Security Administrator has the ability to determine if a KSI service connection type requires 1, 2, or 3 physical connections.

- Downstream KSI Services: The Black Lantern provides the interface for users to obtain KSI services. Through this interface type, the user can request signing or extending services. The Black Lantern uses ports 8080 and 8081 as default SDK signing and extender request, respectively.
- Upstream KSI Infrastructure: The Black Lantern interface with the higher-level aggregator in the KSI infrastructure through this type of interface. Service users do not have access to this interface, and only the Black Lantern is allowed to interact with the rest of the KSI infrastructure through this interface.

Administrators shall meet the following security objectives for the operational environment:

OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

1.6 Delivery Configuration

The Black Lantern is delivered with all required software loaded. An activation file will be delivered through a second channel. The activation file will be imported to the Black Lantern by the end user which will setup the Black Lantern with a default configuration and a default administration account. The credentials for this account will be transmitted to the customer via a pre-defined means of communication established by Guardtime Federal and the customer.

Note: It is recommended to only use the default administration account to create identity-based accounts for administration activities moving forward. Then, after creating a new Security Administrator account along with any other role-based accounts, use this new account to permanently disable the default administration account to avoid its further use.

For details configuring the Black Lantern from the initial Security Administrator account, refer to Section 5.

2 Hardware Overview

2.1 Black Lantern 300 Specifications

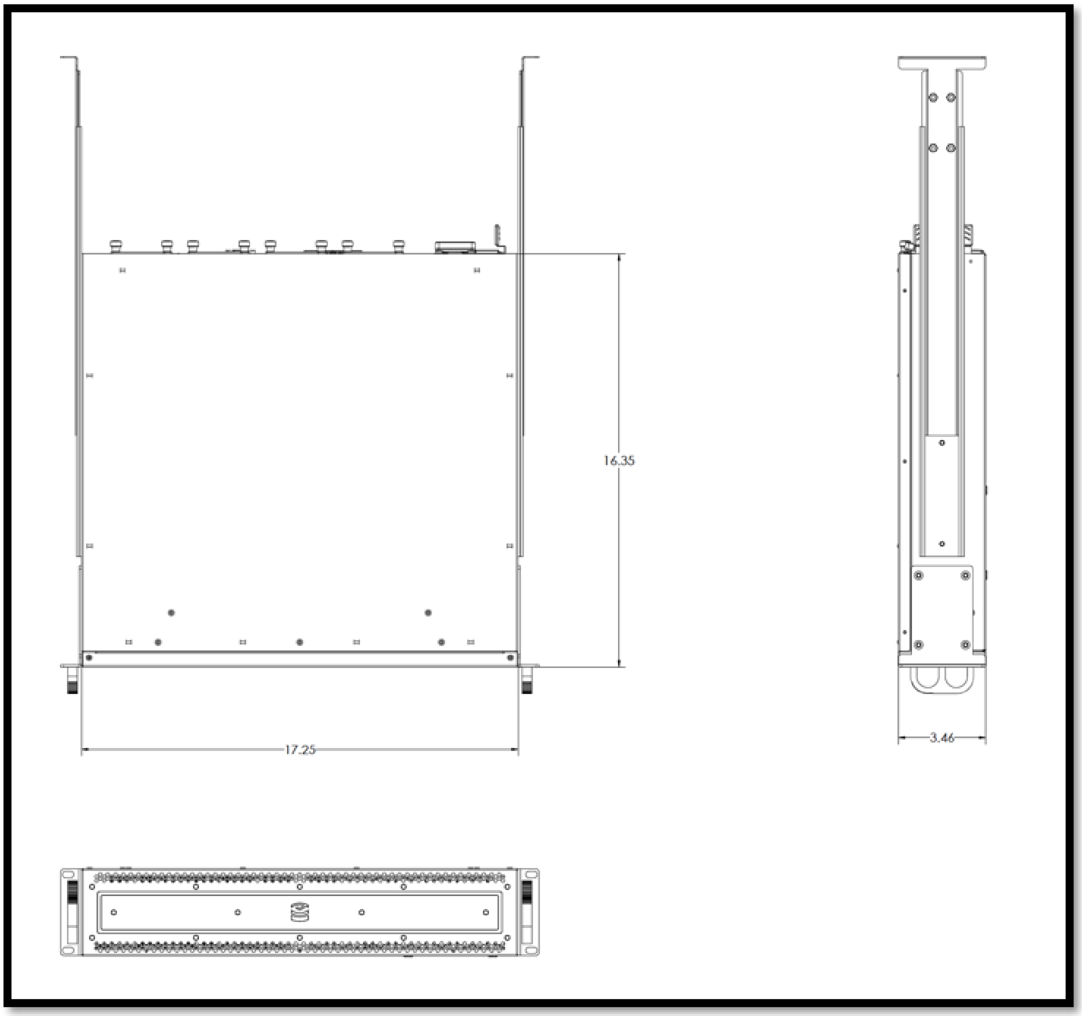


Figure 2: Black Lantern 300 Physical Dimensions

2.1.1 Dimensions

Width	17.25 in.	43.8 cm
Height	3.46 in.	8.8 cm
Depth	16.35 in.	41.5 cm
Weight	29 lbs.	13 kg

2.1.2 Power

Max Wattage	327.7 Watts

2.1.3 Environmental

Operating Temperature	0 to 40 °C or 32 to 104 °F
Relative Humidity	5 to 95%
Storage Temperature	-0 to 40 °C or 32 to 104 °F
Operating Altitude	0-10000ft (0-3000m)

2.1.4 Ports

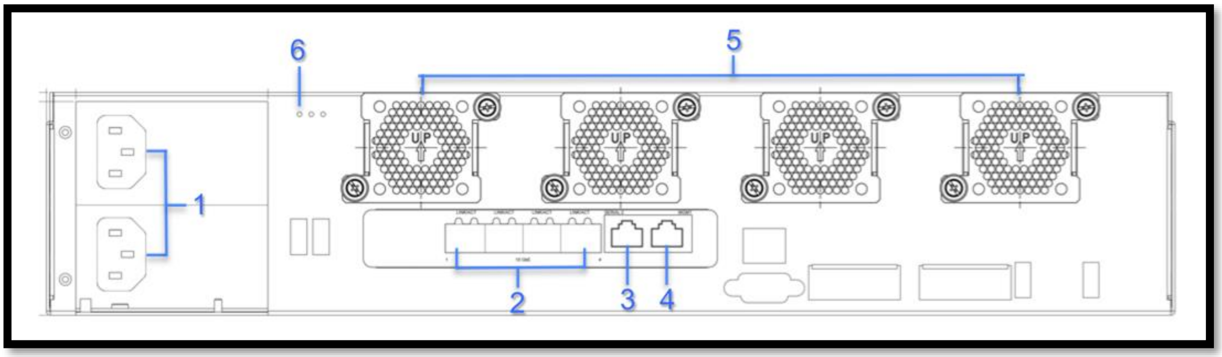


Figure 3: Black Lantern 300 Ports

1. Redundant Power Supplies (2)
2. SFP+ Service Ports (1-4)
3. Serial Console RS232 (RJ45)
4. Management Port (RJ45)
5. Redundant Fans (4)
6. Reset/Power Button

2.2 Black Lantern 400 Specifications

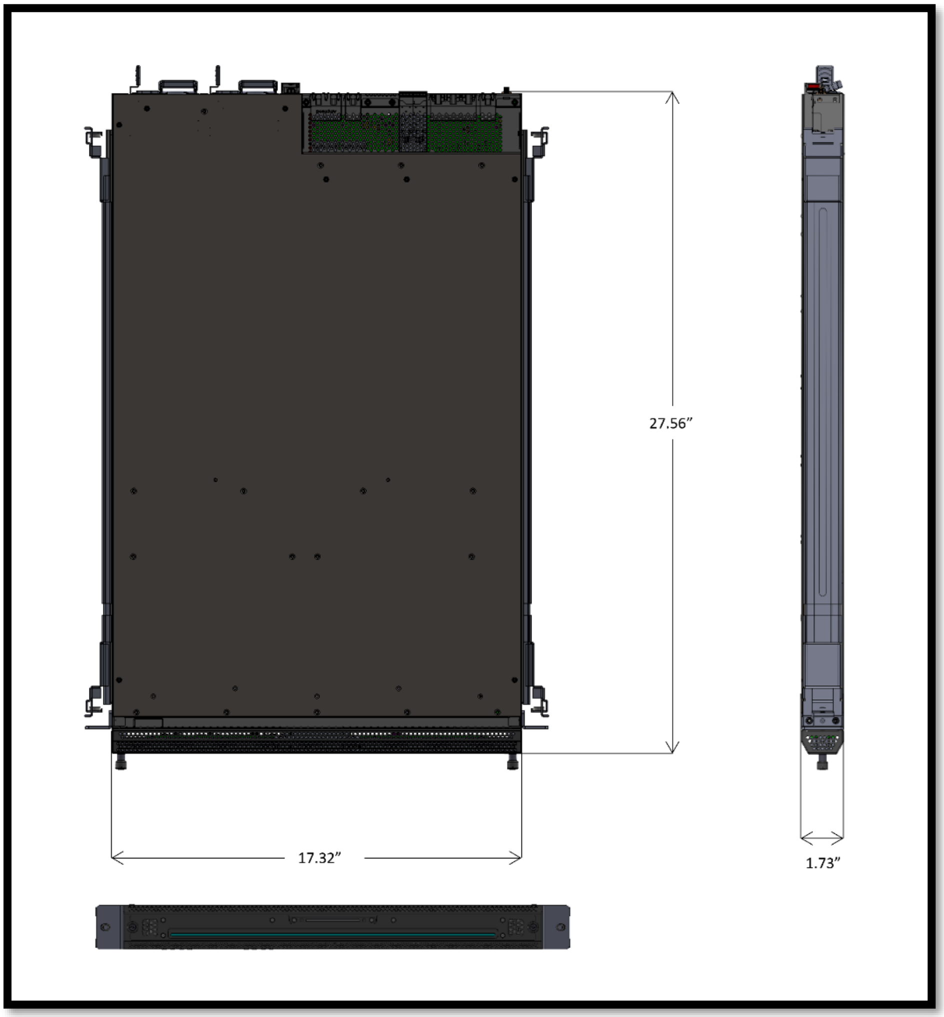


Figure 4: Black Lantern 400 Physical Dimensions

2.2.1 Dimensions

Width	17.32 in.	44.0 cm
Height	1.73 in.	4.4 cm
Depth	27.56 in.	70.0 cm
Weight	31.3 lbs.	14.20 kg

2.2.2 Power

Max Wattage	430.0 Watts

2.2.3 Environmental

Operating Temperature	0 to 40 °C or 32 to 104 °F
Relative Humidity	10 to 90%
Storage Temperature	-0 to 45 °C or 32 to 113 °F
Operating Altitude	0-10000ft (0-3000m)

2.2.4 Ports

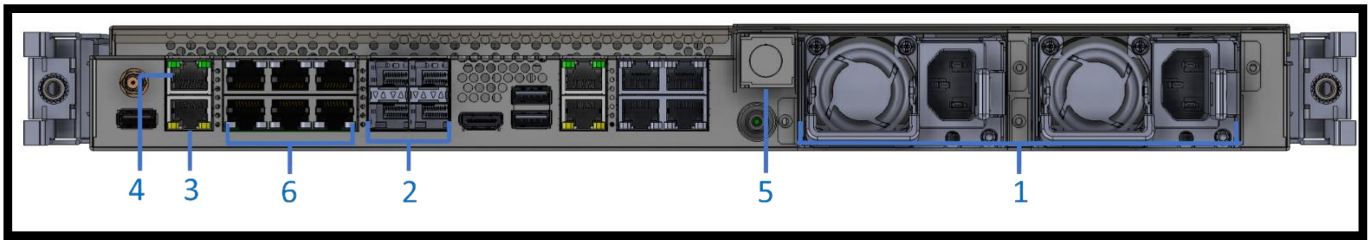


Figure 5: Black Lantern 400 Ports

1. Redundant Power Supplies (2)
2. SFP+ Service Ports (1-4)
3. Serial Console RS232 (RJ45)
4. Management Port (RJ45)
5. Reset/Power Button (under flip open cover)
6. 6 x 1G BASE-T Service Ports (RJ45)

2.3 Connectivity

2.3.1 Serial Console RS232 (RJ45)

The Black Lantern provides an RJ45 serial port as a console management interface for local administration of the unit. This interface can be accessed using a third-party terminal emulation application from a directly connected PC.

2.3.2 Management Port (RJ45)

The Black Lantern provides an Out-of-Band management interface which allows administration of the unit over the network.

2.3.3 Service Ports (SFP+ and RJ45)

Both Black Lanterns have four high speed 10GbE SFP+ service ports are provided for service traffic. The Black Lantern 400 provides an additional six RJ45 ports for service traffic.

2.4 Network Interfaces, Protocols, and Ports

Figure 1 illustrates the network interfaces utilized by the Black Lantern for KSI service and operations and management activities. These interfaces are detailed below, and their ports are configurable.

2.4.1 Management Interfaces

Inbound to Black Lantern:

- RS232 (Device management activities using local serial console)
- HTTPS 443 (Device management activities using HTTP over TLS)

Outbound from Black Lantern:

- RS232 (Device management activities using local serial console)
- HTTPS 443 (Device management activities using HTTP over TLS)
- HTTP 8080 (Configuration and update files download)
- TCP 1610 (Syslog over TLS)
- UDP 123 (NTP Server)

2.4.2 Service Interfaces

Black Lantern inbound from SDK client

- HTTP 8080 (Default SDK Signing Requests)
- HTTP 8081 (Default SDK Extender Requests)

Black Lantern outbound to Upstream KSI

- TCP 3311 (Extender)
- TCP 3332 (Signing)

3 Security Overview

3.1 Environment Requirements

3.1.1 Physical Separation of Service and Management Interfaces for Out of Band (OOB) Management

It is highly recommended to utilize separate network connections for Service and Management interfaces to enable out-of-band (OOB) management of the Black Lantern. Not only will this increase resiliency of Black Lantern service, by removing dependencies between management functionality and service network status, but it will also remove the ability for external service users to potentially access sensitive management functions.

To support this, a separate network must be setup with security conditions met. The management network must have trust boundaries established to prevent unauthorized access and commingling of management and service traffic. Refer to your network equipment manufacturers guidelines for best practices in setting up OOB management networks.

3.1.2 Firewall Configuration

Since the Black Lantern utilizes the management and service ports described in Section 2.4, any firewalls must be configured to allow these connections for the Black Lantern to function correctly. Note, these ports are configurable through the management interfaces. The firewall rules must match the configured ports in the Black Lantern.

3.1.3 Serial Management Interface

The Black Lantern provides a serial port (RS232) for terminal management capabilities. The intention of the serial interface is to provide local administration capabilities for an administrator with physical possession of the unit.

3.2 Management Guidance

The TOE administrators can administer the TOE locally via the SCI and remotely via the RESTful interface. The following table lists TOE management functions, identifies the SCI command the TOE provides to invoke each function, and identifies the functions available via the RESTful interface.

Table 1: TOE Management Functions

Management Function	**CLI Command**	**RESTful API Action**
Configure the access banner	`banner`	n/a
Configure the session inactivity time before termination of the local administrative session	`setconfig`	`PUT` method on `config` endpoint
Update the TOE and verify TOE updates prior to installation using digital signature	`updatebl`	n/a
Configure the authentication failure parameters	`setconfig`	`PUT` method on `config` endpoint
Configure audit behavior (i.e., configure local log storage size, configure TOE behavior when local audit storage space is full)	`setconfig`	`PUT` method on `config` endpoint
Configure the list of TOE-provided services available before an entity is identified and authenticated, per FIA_UIA_EXT.1	`setconfig`	`PUT` method on `config` endpoint
Manage cryptographic keys	`genkey`, `gencsr`, `rm`	n/a
Re-enable an administrator account	`moduser`	n/a
Set the time used for time stamps	`settime`	n/a

Management Function	CLI Command	RESTful API Action
Configure NTP	`setconfig`	`PUT` method on `config` endpoint
Manage the TOE's trust store and designate X.509 v3 certificates as trust anchors	`import`	n/a
Import X.509 v3 certificates to the TOE's trust store	`import`	n/a

3.2.1 Physical separation of management traffic

The Black Lantern provides one (BL300) or seven (BL400) 1GbE (RJ45) and four 10GbE (SFP+) network interfaces which can be independently configured. By default, the first RJ45 interface is presumed the management port. When installing the Black Lantern, its interfaces will need to be configured to match the network settings of your service and out-of-band management networks. Though it is possible to configure both service and management traffic to utilize the same network interface, it is highly recommended to maintain separation of this traffic and implement an out-of-band management capability.

3.2.2 TLS Communication

By default, the HTTPS RESTful API remote management communication is protected using TLS encryption. The syslog traffic should also be configured to require TLS. To enable TLS to function properly, certificates will need to be created and installed in the Black Lantern and the corresponding remote host machines. Please see Section 5.2 and 5.3 for instructions on TLS setup and configuration.

3.2.3 Operation and Maintenance (O&M) Access

3.2.3.1 Accounts and Roles

The Black Lantern (BL) provides role-based access control which enables distinct separation of duties. These roles are defined as follows:

Table 2: Summary of Black Lantern Supported Roles

BL Roles	Definitions
Security	Manages security configurations (add user, update user, add user to group, delete user from group, log management, provision Black Lantern, update software & certificate)
Network	Manage network-related configuration (device network and remote host configuration)
Application	Manage application-related configuration (KSI aggregator and extender configuration)
Recovery Agent	Specialized role associated with backup and recovery of TOE root key

To maintain separation of duties principles, it is highly recommended to only assign minimum necessary roles to each account. For example, a single user account should not be allocated

Security, Network and Application roles at the same time. Doing so increases risks and consequences of user error, misconfiguration, and abuse.

Only the Security and Network Administrator have the necessary authorizations to be able to manage the TOE security functionality and TSF data, as specified by the TSF of [NDcPP]. Therefore, for the purpose of this evaluation, the TOE's Security and Network Administrator combined are equivalent to the NDcPP Security Administrator.

3.2.3.2 Password Policies

3.2.3.2.1 Password entropy rules

Password rules are enforced on the Black Lantern when changing or creating passwords to help ensure the passwords that have at least a minimal level of entropy. The following password rules are enforced:

1. Password length must be at least 8 characters long (configurable)
2. Must have at least one lower case letter
3. Must have at least one capital letter
4. Must have at least one digit
5. Must contain at least one of the following special characters: _!@#$%^&*()?<>.,~|

3.2.3.2.2 Minimum Password Length

The Black Lantern allows for a configurable minimum password length to provide flexibility in supporting your security policies. The default value for this setting is 8 characters. The minimum value is 8 and the maximum is 32.

3.2.3.2.3 Password expiration

The Black Lantern provides the ability to enforce password aging policies with a configurable password expiration timeout period. By default, passwords expire after 60 days. It is recommended to enable password expiration rules on the Black Lantern, and to configure the password expiration period to match your enterprise password aging policies.

3.2.3.2.4 Force change on reset password

When accounts are created or passwords are reset, it is common for the security administrator to assign a temporary password. To prevent any user from using this temporary password ad infinitum, the Black Lantern provides a means to force a user to change their password upon next login. This is accomplished by prompting the Security Administrator the option to apply this policy when an account is created, or a user's password is changed.

3.2.3.3 Account Disable and Expiration

Inactive user accounts can pose a security risk. Situations such as employees leaving the organization or temporary special purpose accounts which are not deleted can leave accounts enabled when they are no longer needed. To help combat this situation, Black Lantern can be configured to automatically disable accounts which have not been accessed after a period of time. By default, accounts are configured to be disabled after 180 days of inactivity but can be configured to match your organization's policies.

Note: The Security Administrator role is exempt from this policy.

3.2.3.4 Serial Terminal Session Timeout

Open login sessions which are not actively in use can increase security risk by allowing malicious users to gain access to the system and circumvent login authentication requirements. Sessions can become inactive when a negligent user leaves the console without properly logging out, or in some cases when serial session servers malfunction and disconnect a remote user. To mitigate this risk, the Black Lantern will automatically log users off and end the session after a configurable amount of inactivity. The inactivity period should be configured to match your organization's policies. NDcPP compliance further requires this inactivity period to be defined greater than 0.

3.3 Black Lantern Software Updates and Patches

Updates to Black Lantern software will be introduced which can add additional functionality or provide fixes for known issues. These software patches will be made available in the form of a new Black Lantern Firmware image which is loaded onto the Black Lantern during the secure software update process. When the new update is released, the customers will get notified and the update image will be sent to them via a pre-defined means of communication. The customers will follow updates instructions, detailed in Section 7.7, to manually update the software in the Black Lantern.

4 Black Lantern Installation

4.1 Safety Information

4.1.1 Definition of Safety Warnings

ⓘ **NOTE:** A note indicates information that may be useful or helpful to you in certain situations

⚠ **CAUTION:** A caution indicates that specific guidelines must be followed to avoid potential damage to hardware or potential minor bodily injury or discomfort

❗ **WARNING:** A warning indicates a dangerous situation the potential for property damage or personal injury

4.1.2 General Safety

❗

Before working on, moving, or changing connections on the device, be sure that the unit is switched off and the power has been disconnected from the appliance. There are multiple power supplies in the unit and power connections must be disconnected from all power supplies to remove power from the unit.

Before installing or removing the front faceplate, ensure the unit is powered off. Otherwise. the LED board may be damaged. It is recommended the faceplate remain installed during normal operation to avoid unnecessary detection of removal events.

Do not remove any covers from the unit and do not operate the unit with any covers removed. Removal of covers may void your warranty.

Do not use damaged equipment, including any exposed, damaged, or frayed power cords.

Do not use the unit in any wet environments or areas where the unit can get wet. If the unit becomes exposed to liquid, follow safety procedures to remove power from the unit and reduce risk of electric shock.

⚠

Do not push objects into vents, fans, or other openings in the chassis of the appliance.

When performing maintenance on the unit, such as replacing the fans or power supplies, read and follow the maintenance instructions carefully to prevent damage to the system.

Operate the appliance in an area with proper air circulation. Avoid positioning the appliance such that the air intakes are exposed to heated air such as exhaust from another appliance.

ℹ

Do not attempt to dispose of the unit. Return the unit to Guardtime Federal for proper disposal.

4.2 Hardware Setup

4.2.1 Packing List

Table 3: Black Lantern 300 Appliance Packing List

Qty	Description
1	Appliance Unit
2	Front Mounting Ears
2	Rear Bracket
2	Rail Sliders
8	Screw Type A – for front mounting ears (8-32 X 1/4 flat)
8	Screw Type B – for Rails (8-32 X 1/4 truss)
8	Screw Type C – for rear bracket (10-32 X 5/16 truss)
1	Cat 5 Ethernet Cable
1	Serial Console Cable
2	Power Cables

Table 4: Black Lantern 400 Appliance Packing List

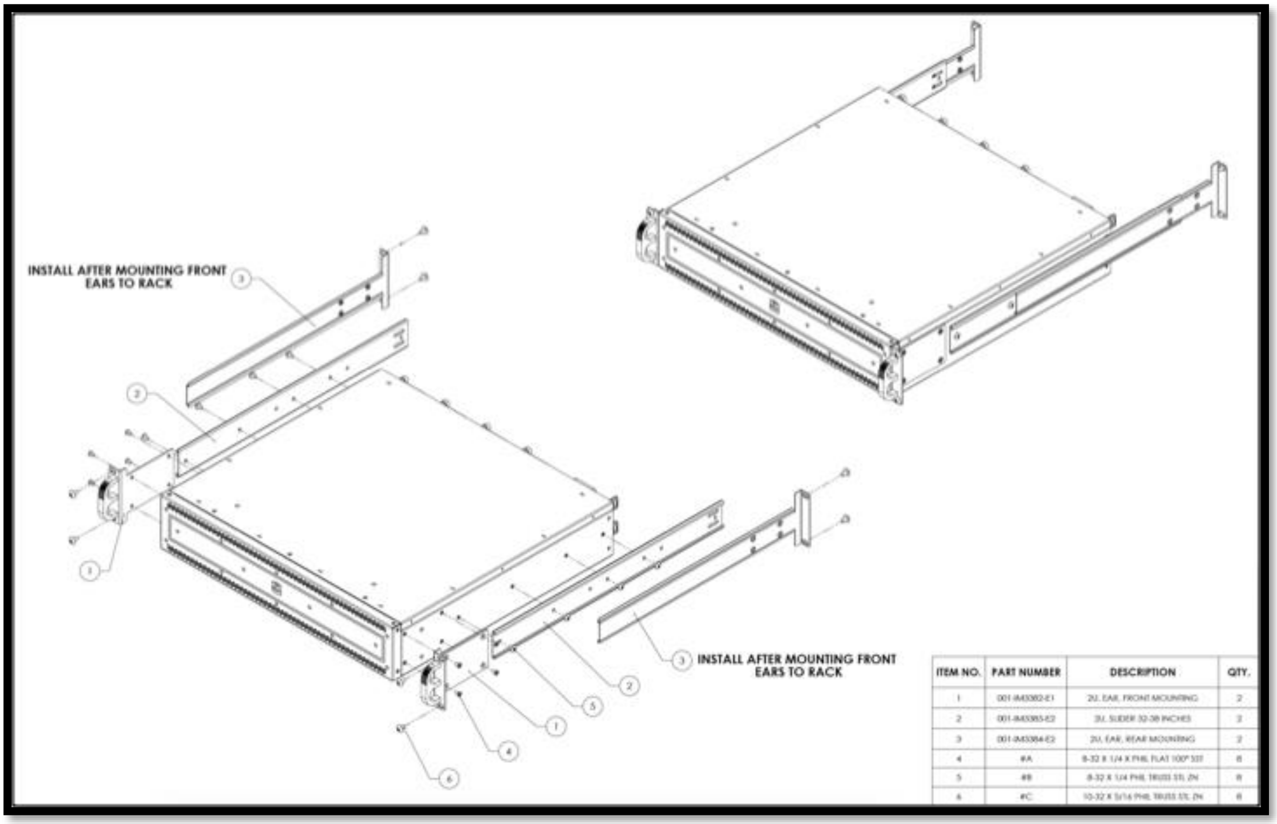
Qty	Description
1	Appliance Unit
2	Front Mounting Ears
2	Rail Sliders (24 inches) ASL-2209DS30
4	Screw Type A – for front mounting ears (6-32 X 5/16 PHIL FLAT STL BLK)
10	Screw Type B – for inner rail (8-32 X 1/4 truss)
4	Screw Type C – Slider to rack (M6-1.0 X 16 PH PAN SST)
1	Cat 5 Ethernet Cable
2	Serial Console Cable
2	Power Cables
2	SATA Drive bay key

4.2.2 BL300 Rack Installation

The appliance is designed for installation in a standard 19 in server rack; and it occupies two rack units (2U). Mounting hardware is included for rack installation. Follow the steps below and refer to the Figure 6 to complete the installation.

Installation should be performed by qualified personnel

It is recommended for two people to perform the installation to aid in positioning the appliance on the rack.


INSTALL AFTER MOUNTING FRONT EARS TO RACK
3
2
1
INSTALL AFTER MOUNTING FRONT EARS TO RACK
3
2
5
1
4
6

ITEM NO.	PART NUMBER	DESCRIPTION	QTY.
1	001-IM3382-E1	2U, EAR, FRONT MOUNTING	2
2	001-IM3385-E2	2U, SLIDER 32-38 INCHES	2
3	001-IM3384-E2	2U, EAR, REAR MOUNTING	2
4	#A	8-32 X 1/4 X PHIL FLAT 100° SST	8
5	#B	8-32 X 1/4 PHIL TRUSS STL ZN	8
6	#C	10-32 X 5/16 PHIL TRUSS STL ZN	8

Figure 6: Black Lantern Installation

1. Install the mounting ears (#1) to the chassis. Use screw type A (#4) to secure.
2. Install the slider rail (#2) to the chassis. Use screw type B (#5) to secure.
3. Install the rear mounting bracket (#3) to the rear of the rack. Use screw type C (#6) or the appropriate cage nuts/screws for your rack (not included) to secure.
4. Guide the chassis into the rack and align the slider onto the rear bracket. The rear bracket should slide into the slider. Push the chassis into the rack until the front mounting ears are flush with the front of the rack.

A second person is helpful at this step to help support the chassis and align the sliding rails.

5. Secure the front mounting ear to the rack using screw type C (#6) or the appropriate cage nuts/screws for your rack (not included).

4.2.3 BL400 Rack Installation

The appliance is designed for installation in a standard 19 in server rack; and it occupies one rack unit (1U). Mounting hardware is included for rack installation.

> ⚠ Installation should be performed by qualified personnel
>
> It is recommended for two people to perform the installation to aid in positioning the appliance on the rack.

1. Remove inner slide from rail by extending and compressing clip.
2. Attach the inner slide to the chassis (Screw type B)
3. Align and attach the outer rail to the rack (Screw type C)
4. Attach mounting ears to the chassis (Screw type A)
5. Guide the chassis into the rack and align the sliders. Push the chassis into the rack until the front mounting ears are flush with the front of the rack.

> ⓘ A second person is helpful at this step to help support the chassis and align the sliding rails.

6. Secure the front mounting ear to the rack using screw type C (#6) or the appropriate cage nuts/screws for your rack (not included).

4.3 Connectivity

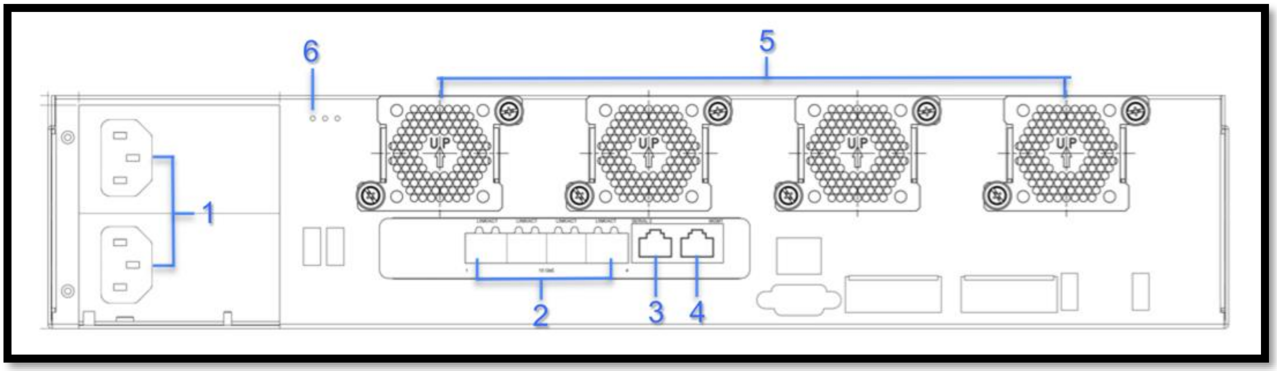


Figure 7: Black Lantern 300 Port Connectivity

1. Redundant Power Supplies (2)
2. SFP+ Service Ports (1-4)
3. Serial Console RS232 (RJ45)
4. Management Port (RJ45)
5. Redundant Fans (4)
6. Reset/Power Button

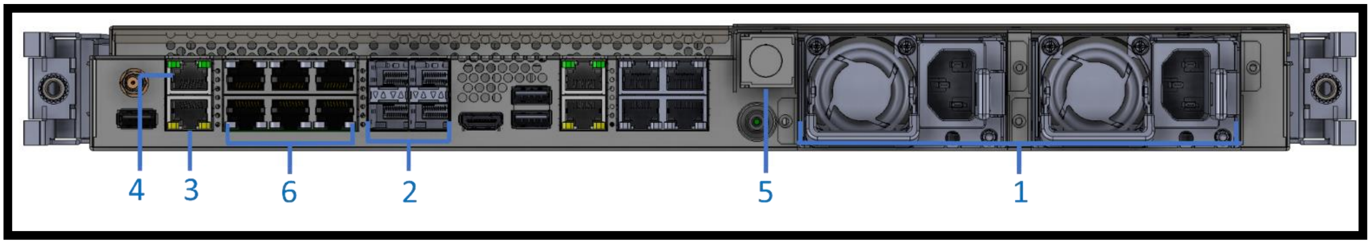


Figure 8: Black Lantern 400 Port Connectivity

1. Redundant Power Supplies (2)
2. SFP+ Service Ports (1-4)
3. Serial Console RS232 (RJ45)
4. Management Port (RJ45)
5. Reset/Power Button (under flip open cover)
6. 6 x 1G BASE-T Service Ports (RJ45)

For operation of the Black Lantern, please connect the following ports:

- Management Port - The Black Lantern provides an Out-of-Band management interface which allows administration of the unit over the network.
- Serial Console - The Black Lantern provides an RJ45 serial port as a console management interface for local administration of the unit. This interface can be accessed using a third-party terminal emulation application from a directly connected terminal (e.g. PC).
- Service Ports - These interfaces (RJ45, SFP+) provide flexible network access for remote management (via RESTful APIs), support services (DNS, NTP, Remote Logging), and KSI services.

⚠ The Black Lantern unit will power on when power cables are connected. Connect all other cables first before connecting power.

4.4 Network Configuration

Once the unit has been installed in the rack and connectors have been plugged in, you will need to configure the network settings to enable communication on your network.

The Black Lantern has the following available network ports identified below:

Table 5: Black Lantern Network Ports States at Factory Reset

Logical Name	Physical Port (BL300)	Physical Port (BL400)	Factory Reset State
eth0	1Gb Ethernet Management Port	1Gb Ethernet Management Port	Enable
eth1	10Gb SFP+ Service Port 1	1Gb Ethernet Service Port 1	Disable
eth2	10Gb SFP+ Service Port 2	1Gb Ethernet Service Port 2	Disable

Logical Name	Physical Port (BL300)	Physical Port (BL400)	Factory Reset State
eth3	10Gb SFP+ Service Port 3	1Gb Ethernet Service Port 3	Disable
eth4	10Gb SFP+ Service Port 4	1Gb Ethernet Service Port 4	Disable
eth5	n/a (PCIe Virtual Port)	1Gb Ethernet Service Port 5	Disable
eth6	n/a	1Gb Ethernet Service Port 6	Disable
eth7	n/a	10Gb SFP+ Service Port 1	Disable
eth8	n/a	10Gb SFP+ Service Port 2	Disable
eth9	n/a	10Gb SFP+ Service Port 3	Disable
eth10	n/a	10Gb SFP+ Service Port 4	Disable
eth11	n/a	n/a (Internal Ethernet Port)	Disable

The following guidelines need to be followed when configuring the above network interfaces for Black Lantern:

- Typically, the management port (eth0) should be used when provisioning the Black Lantern.
- Once Black Lantern has been provisioned, use ifconfig or setconfig SCI commands to configure the rest of the interfaces.
- When using multiple interfaces, each interface needs to be on its own subnet. Unexpected behavior can occur if more than one interface is on the same subnet.
- Interface(s) not being used should be disabled using either ifconfig or setconfig

When the Black Lantern is powered on for the first time, by default eth0 is enabled while the rest of the interfaces are disabled. At this point, setting up the remaining interfaces is not required. Using ifconfig command you can either enable DHCP to get a dynamic IP assignment or you can manually set the Gateway, DNS, IP, and Netmask if a static IP is assigned to this Black Lantern. It is recommended not to use DHCP assignment; or use DHCP only to perform Black Lantern initial network configuration.

4.4.1 Network Configuration Setup Procedure

As an example of configuring the Black Lantern, the following will be used as the network configurations needed:

- Management port (eth0) is assigned IP 192.168.1.100 on subnet 192.168.1.x
- Gateway for subnet 192.168.1.x is 192.168.1.254
- default gateway is set to 192.168.1.254 and DNS is set to 192.168.1.1
- Interface ports 1, 2, 3 and 4 are not being used

The following procedure will perform the network configuration of the Black Lantern:

1) Apply power to the Black Lantern.

```
pre-init
*********************************************************
  Boot Loaded....
 Build 0x00080000 Thu Apr  8 17:26:50 2021
*********************************************************
Begin Built-In-Test...
Press 'Enter' key to abort...
100% Complete...

Loading OS image...
OS prepared..

********************************************************************************
* This setup menu will walk you through setting up your Black Lantern.
* - Step 1: Configure the network interface to communicate with management host
*           by running <ifconfig> command. Use <ifconfig --help> for help.
* - Step 2: Run <setupbl> command to download setup file from management host
*           Use <setupbl --help> for help.
*******************************************************************************

[blshell]>
```

2) Use the ifconfig command to view initial network interface settings.

```
[blshell]>ifconfig
-------------------------------------------------------------------
Default Gateway                      = 192.168.0.254
Primary DNS                          = 192.168.0.1
Secondary DNS                        = 192.168.0.1
-------------------------------------------------------------------
Network Interface Name               = eth0
Network Interface Enable             = true
Network Interface IPv4               = 192.168.0.2
Network Interface MAC                = 00:0c:bd:08:f4:20
Network Interface Netmask            = 255.255.255.0
Network Interface DHCP               = 0
-------------------------------------------------------------------
-------------------------------------------------------------------
Network Interface Name               = eth1
Network Interface MAC                = 00:0c:bd:08:f4:21
Network Interface Enable             = false
-------------------------------------------------------------------
-------------------------------------------------------------------
Network Interface Name               = eth2
Network Interface MAC                = 00:0c:bd:08:f4:22
Network Interface Enable             = false
-------------------------------------------------------------------
-------------------------------------------------------------------
Network Interface Name               = eth3
Network Interface MAC                = 00:0c:bd:08:f4:23
Network Interface Enable             = false
-------------------------------------------------------------------
-------------------------------------------------------------------
Network Interface Name               = eth4
Network Interface MAC                = 00:0c:bd:08:f4:24
Network Interface Enable             = false
-------------------------------------------------------------------
-------------------------------------------------------------------
Network Interface Name               = eth5
Network Interface MAC                = 00:0c:bd:08:f4:25
Network Interface Enable             = false
-------------------------------------------------------------------
```

3) Use ifconfig command to enable or disable the network ports in the event that they don’t match the state listed in Table 5.

```
[blshell]>ifconfig eth0 up
Success: ifconfig completed.
[blshell]>ifconfig eth1 down
Success: ifconfig completed.
[blshell]>ifconfig eth2 down
Success: ifconfig completed.
[blshell]>ifconfig eth3 down
Success: ifconfig completed.
[blshell]>ifconfig eth4 down
Success: ifconfig completed.
```

4) Use ifconfig to configure the IP and netmask.

```
[blshell]>ifconfig eth0 ip 192.168.0.100
Success: ifconfig completed.
[blshell]>ifconfig eth0 netmask 255.255.255.0
Success: ifconfig completed.
```

5) Use ifconfig to configure default the system gateway and DNS.

```
[blshell]>ifconfig sys1 gateway 192.168.0.254
Success: ifconfig completed.
[blshell]>ifconfig sys1 dns 192.168.0.1
Success: ifconfig completed.
```

6) Use ifconfig to verify the updated network settings.

```
[blshell]>ifconfig
------------------------------------------------------------------
Default Gateway                     = 192.168.0.254
Primary DNS                         = 192.168.0.1
Secondary DNS                       = 192.168.0.1
------------------------------------------------------------------
Network Interface Name              = eth0
Network Interface Enable            = true
Network Interface IPv4              = 192.168.0.100
Network Interface MAC               = 00:0c:bd:08:f4:20
Network Interface Netmask           = 255.255.255.0
Network Interface DHCP              = 0
------------------------------------------------------------------
------------------------------------------------------------------
Network Interface Name              = eth1
Network Interface MAC               = 00:0c:bd:08:f4:21
Network Interface Enable            = false
------------------------------------------------------------------
------------------------------------------------------------------
Network Interface Name              = eth2
Network Interface MAC               = 00:0c:bd:08:f4:22
Network Interface Enable            = false
------------------------------------------------------------------
------------------------------------------------------------------
Network Interface Name              = eth3
Network Interface MAC               = 00:0c:bd:08:f4:23
Network Interface Enable            = false
------------------------------------------------------------------
------------------------------------------------------------------
Network Interface Name              = eth4
Network Interface MAC               = 00:0c:bd:08:f4:24
Network Interface Enable            = false
------------------------------------------------------------------
```

```
------------------------------------------------------------------
Network Interface Name              = eth5
Network Interface MAC               = 00:0c:bd:08:f4:25
Network Interface Enable            = false
------------------------------------------------------------------
```

With the network configurations above, the Black Lantern is now connected to your network.

5 Initial Configuration

Black Lantern allows local login through SCI or remote access through its RESTful Interface. This section describes the necessary steps the Security Administrator must perform to configure both login methods.

5.1 Local Login

Local login is performed by using the Serial Console Interface (SCI) of the Black Lantern and a terminal emulator (e.g., Putty). However, before using the SCI, the Security Administrator must configure the Black Lantern using the Initial Configuration File, which contains a Security Administrator account.

When a Black Lantern is delivered, Guardtime Federal also delivers an encrypted Initial Configuration File and the credentials for the Initial Security Administrator account. The credentials and the configuration file are delivered using different delivery channels agreed upon by Guardtime Federal and the customer at the time of contract signing. The following figure depicts Guardtime Federal delivery items and how the customer must use each one.

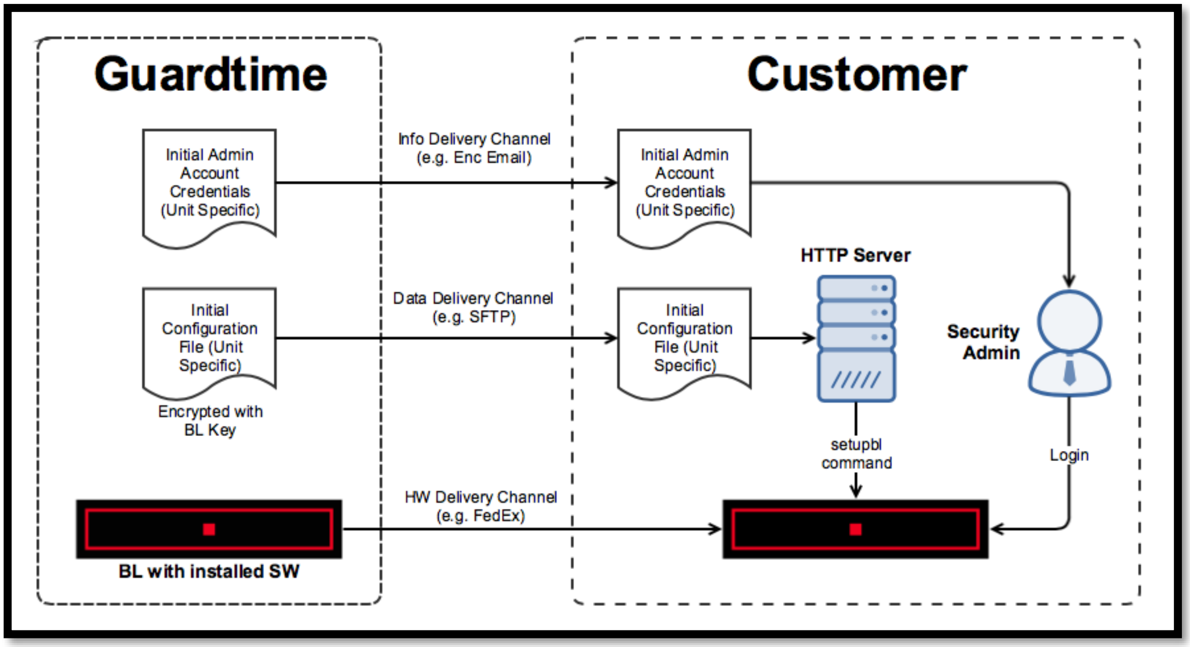

Guardtime
Customer
Initial Admin Account Credentials (Unit Specific)
Info Delivery Channel (e.g. Enc Email)
Initial Admin Account Credentials (Unit Specific)
HTTP Server
Initial Configuration File (Unit Specific)
Data Delivery Channel (e.g. SFTP)
Initial Configuration File (Unit Specific)
Security Admin
Encrypted with BL Key
setupbl command
Login
HW Delivery Channel (e.g. FedEx)
BL with installed SW

Figure 9: Guardtime Federal Delivery Process

The Black Lantern is delivered in Factory Reset state without any user accounts in its local user database. The Initial Configuration File contains the Black Lantern's user database, which in this case, is only the Initial Security Administrator account. Initial configuration files are unique to a specific Black Lantern. They are encrypted with a key residing within its associated Black Lantern and must be hosted on an HTTP server. During the configuration process, the Security Administrator will command the Black Lantern to fetch this file from the HTTP server. At which point, the Black Lantern will configure itself with the Initial Security Administrator account. The credentials for the Initial Security Administrator account are also provided to the customer via a different channel.

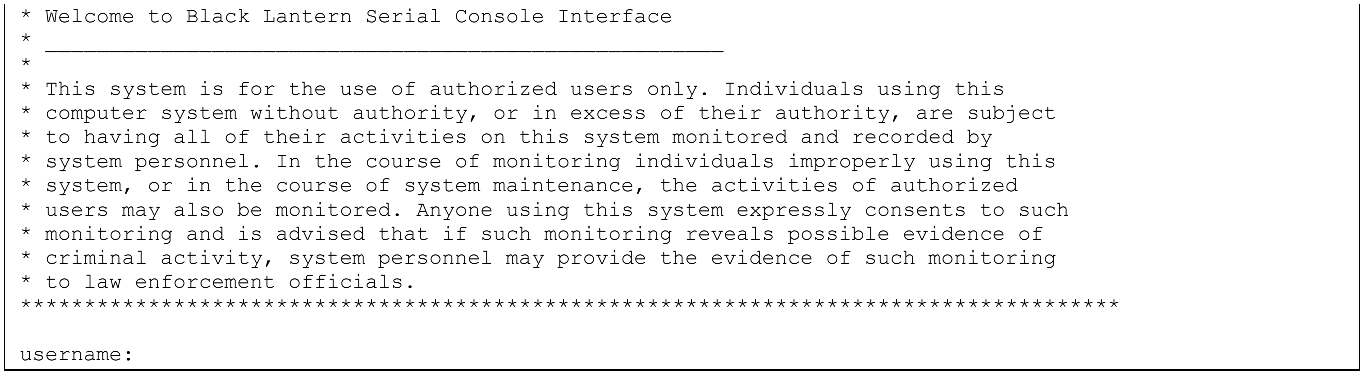
Before using the Black Lantern, the customer should create a *new* Security Administrator account, and the initial account must be deleted. The new Security Administrator account can be then used to create additional user accounts for other admins. Each account created must be associated with a role supported by the Black Lantern. Although multiple roles may be associated with one account, Guardtime Federal advises to separate roles between different accounts. Reference Table 2 for definitions of the various roles. Each type of role grants the administrator access to certain parts of the system. Commands and views will also be restricted to the type of role.

5.1.1 Configuring Local Login

To configure the Black Lantern for local login, the Security Administrator must perform the following steps. These steps assume that the HTTP server has been set up and is hosting the Initial Configuration File, the customer has received the credentials for the Initial Security Administrator account, and the Network Configuration Setup Procedure has been performed (refer to Section 4.4.1).

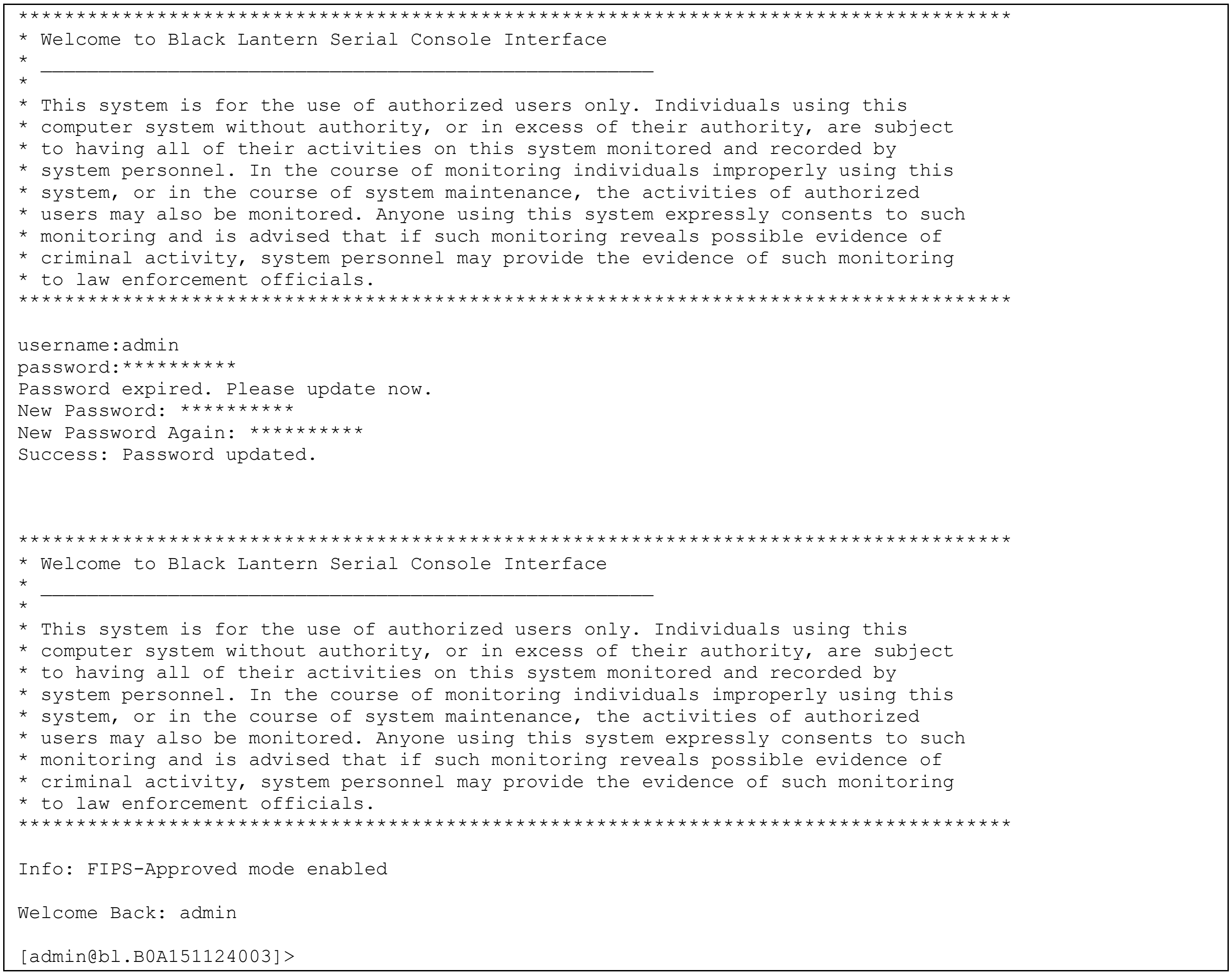
1) To configure the Black Lantern with the Initial Configuration File, use the setupbl command.

```
[blshell]>setupbl http://my.httpserver.net/activationFile.enc
Info: Setup in progress...
Success: Done
Info: Rebooting now...completed

Attempting to unmount SATA...Done
Attempting to unmount RAMDisk...Done
Info: Attempting to reboot high side...

pre-init
********************************************************
  Boot Loaded....
 Build 0x00080000 Thu Apr  8 17:26:50 2021
********************************************************
Begin Built-In-Test...
Press 'Enter' key to abort...
100% Complete...

Loading OS image...
OS prepared..
Services initializing (this may take a minute)...Done



**************************************************************************************
```



```
* Welcome to Black Lantern Serial Console Interface
* ______________________________________________________
*
* This system is for the use of authorized users only. Individuals using this
* computer system without authority, or in excess of their authority, are subject
* to having all of their activities on this system monitored and recorded by
* system personnel. In the course of monitoring individuals improperly using this
* system, or in the course of system maintenance, the activities of authorized
* users may also be monitored. Anyone using this system expressly consents to such
* monitoring and is advised that if such monitoring reveals possible evidence of
* criminal activity, system personnel may provide the evidence of such monitoring
* to law enforcement officials.
**************************************************************************************

username:
```

2) When prompted for credentials, enter the Initial Security Administrator account credentials. If successfully authenticated, the SCI will prompt it. Otherwise, the system will reject the login, and prompt to try again. Password data is obfuscated while it is being entered and only generic success/failure messages are provided. There are no preparatory steps required to ensure authentication data is not revealed while entering login information.



```
**************************************************************************************
* Welcome to Black Lantern Serial Console Interface
* ______________________________________________________
*
* This system is for the use of authorized users only. Individuals using this
* computer system without authority, or in excess of their authority, are subject
* to having all of their activities on this system monitored and recorded by
* system personnel. In the course of monitoring individuals improperly using this
* system, or in the course of system maintenance, the activities of authorized
* users may also be monitored. Anyone using this system expressly consents to such
* monitoring and is advised that if such monitoring reveals possible evidence of
* criminal activity, system personnel may provide the evidence of such monitoring
* to law enforcement officials.
**************************************************************************************

username:admin
password:**********
Password expired. Please update now.
New Password: **********
New Password Again: **********
Success: Password updated.



**************************************************************************************
* Welcome to Black Lantern Serial Console Interface
* ______________________________________________________
*
* This system is for the use of authorized users only. Individuals using this
* computer system without authority, or in excess of their authority, are subject
* to having all of their activities on this system monitored and recorded by
* system personnel. In the course of monitoring individuals improperly using this
* system, or in the course of system maintenance, the activities of authorized
* users may also be monitored. Anyone using this system expressly consents to such
* monitoring and is advised that if such monitoring reveals possible evidence of
* criminal activity, system personnel may provide the evidence of such monitoring
* to law enforcement officials.
**************************************************************************************

Info: FIPS-Approved mode enabled

Welcome Back: admin

[admin@bl.B0A151124003]>
```

3) To add a new user into the Black Lantern, use the adduser command. The Black Lantern will require the Security Administrator to re-enter password to re-authenticate the Security Administrator.

4) Enter <yes> when prompted to have the New User to change password on next login.

5) When prompted for New User's Password, enter a temporary password for the New User.

6) If the command was successful, the Black Lantern will display a message that the New User has been successfully added. The following is an example of adding a new user secadmin with role of security.

```
[admin@bl.B0A151124003]>adduser secadmin security
Logged-In User's Password: **********
Do you want user to change password on next login?
Enter <yes> to continue or any key otherwise.
yes
New User's Password: **********
New User's Password Again: **********
Success: User secadmin added.
```

7) Verify that the New User has been added to the local Black Lantern database by entering getuser command in the SCI.

```
[admin@bl.B0A151124003]>getuser
------------------------------------------------------------------------------------------------------------------------------------------------------
|                                       ||                                      ||                          || last pwd   || last good  || last bad   || authentication |
| user name                             || role                                 || status                   || changed    || login      || login      || failures       |
------------------------------------------------------------------------------------------------------------------------------------------------------
| admin                                 || security                             || active                   || 2018-04-17 || 2018-04-21 || no login   || 0              |
| secadmin                              || security                             || pwd-reset                || 2018-04-21 || no login   || no login   || 0              |
------------------------------------------------------------------------------------------------------------------------------------------------------
```

8) Use the exit command in the SCI to log out of the session initiated by the Initial Security Administrator.

9) Log in using the credential for recently created New User account and follow the instructions to change the password for the account.

10) Delete the Initial Security Administrator account from the Black Lantern user database, with the deluser command.

11) Follow the directions to re-authenticate the Security Administrator and confirm the deletion of the user account.

12) If the command was successful, the Black Lantern will display a message confirming the deletion of the user account. The following is an example of deleting a user account admin.

```
[admin@bl.B0A151124003]>deluser admin
Logged-In User's Password:
Are you sure you want to delete user?
Enter <yes> to continue or any key otherwise.
yes
Success: User admin deleted.
```

13) Verify that the user account has been deleted from the local Black Lantern database by entering getuser command in the SCI.

5.2 Remote Login

For the Black Lantern to enable remote management, the Security Administrator must configure the settings as described in Section 5.3.2.1.

The Black Lantern is designed to provide a RESTful Interface for the purposes of remote management. The nature of this type of interface does not allow the administrator to initiate remote login sessions to the Black Lantern. Instead, when the administrator needs to remotely manage the Black Lantern, the administrator sends a RESTful request to the Black Lantern. This request is accompanied with authentication credentials, associated with local accounts on the Black Lantern. Once the authentication credentials are authenticated, the Black Lantern processes the RESTful request, and terminates any communication with the administrator.

5.2.1 Configuring Remote Login

The Black Lantern supports secure communication when communicating through the HTTPS-protected RESTful interface (during remote management) and when sending logs to a remote logging server. Both cases require the establishment of server certificates and a Black Lantern private key along with initial configuration. The certificate type supported in the Black Lantern is X.509 encoded in PEM format. In addition, to support certificate status checking (e.g. revoked certificates), the Online Certificate Status Protocol (OCSP) server is queried during a TLS connection when the certificate contains the specified URI. Within revocation checking, if the OCSP server does not respond or if the certificate is invalid, the Black Lantern does not establish the connection (i.e. the certificate is not accepted).

Note that certificates are not used for trusted updates or executable code integrity. Therefore, the Black Lantern does not support the rules for validating certificates with the Code Signing purpose in the extendedKeyUsage field, and this part of the requirement is trivially satisfied.

The Black Lantern allows for the following possible scenarios to set up TLS / SSL certificates and keys:

1. Importing a certificate and Certificate Authority (CA) chain for identity of the Black Lantern (localhost), where the private key is already on the system.
2. Importing the CA chain that signed the certificate of an Authorized IT Entity (remotehost). This is used for connecting to a remote management client and/or a logging server.

The following figure provides an overview of the certificates that must be stored in the Black Lantern and those that must be interchanged between the Black Lantern and the remotehost:

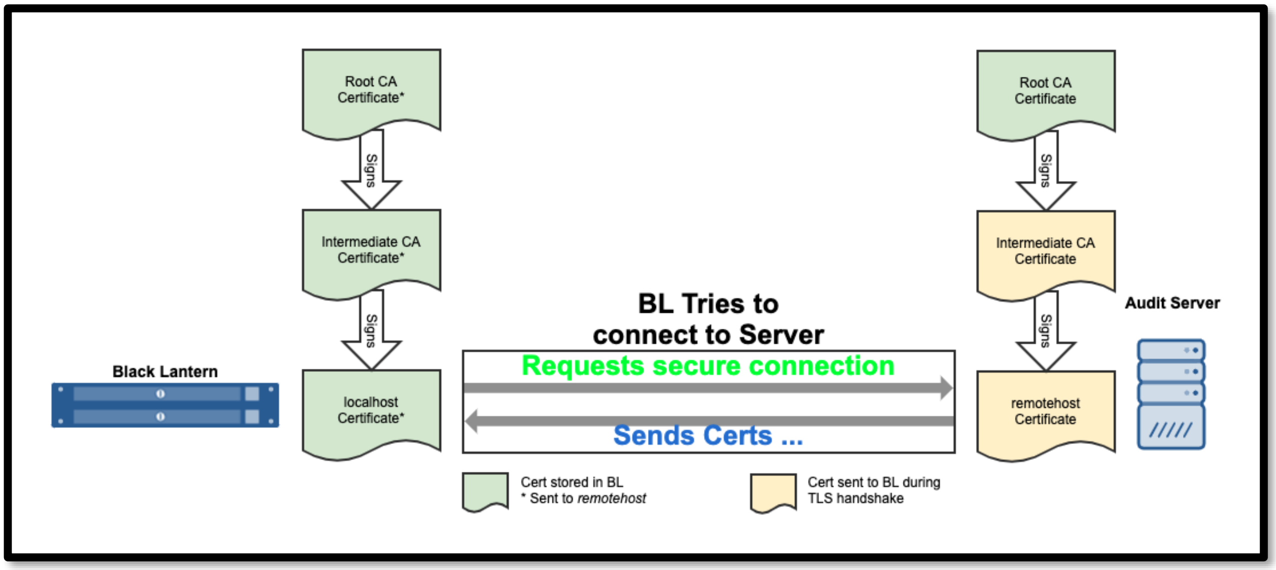


Figure 10: Required Certificate Storage and Interchange for TLS Communication

All certificates are verified at import time; Black Lantern's certificate chain is verified up to the Root CA. When importing certificates, the Security Administrator must enter them in reverse order of signing, with the Root CA certificate inputted last as shown in the following figure:

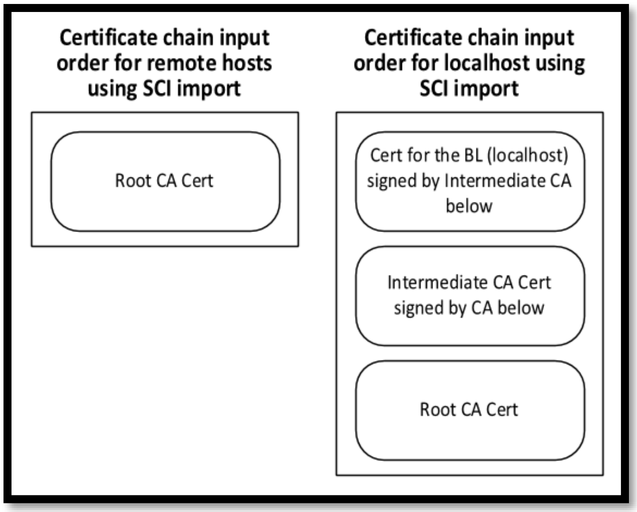

Certificate chain input order for remote hosts using SCI import
Root CA Cert
Certificate chain input order for localhost using SCI import
Cert for the BL (localhost) signed by Intermediate CA below
Intermediate CA Cert signed by CA below
Root CA Cert

Figure 11: Black Lantern Certificate Loading Order

5.2.1.1 Importing Localhost Certificate and Certificate Authority (CA) Chain (as identity of the Black Lantern)

In this scenario, the Security Administrator will generate a key pair and CSR on the Black Lantern, export the Certificate Signing Request (CSR) and sign it using a CA. The Security Administrator then imports the resulting certificate into the Black Lantern. For this scenario, the Security Administrator pastes in the *localhost* certificate, followed by all the parents' Intermediate CA certificates, up to the Root CA certificate.

5.2.1.1.1 Key Generation

The Black Lantern allows the Security Administrator to generate RSA and ECC key pairs using the genkey command. The Black Lantern supports the following keys sizes for the two types of schemes:

Table 6: Black Lantern Supported Asymmetric Key Sizes

Algorithm	Key Lengths Supported
RSA	2048 4096
ECDSA	256 384 521

Keys generated by the Black Lantern can be used for Black Lantern certificate (localhost) generation only and not for other devices. This is because the Black Lantern does not allow displaying or exporting private keys in plaintext. Consider the CSfC constraints mentioned in Section 1.2 when selecting the appropriate algorithms and key sizes for key generation.

The following captures the SCI when the Security Administrator generates an RSA key pair with the length of 2048 and an ECC key pair with curve P-384.

```
[admin@bl.B0A151124003]>genkey -a RSA -s 2048 "RSA_Key"
Generating RSA-2048 key(s). Operation may take minutes depending on selected key/curve size...
Success: Key(s) generated and stored. Please use the key-name "rsa_key" to reference it in the system.
[admin@bl.B0A151124003]>genkey -a EC -s 384 "ec384"
Generating EC-384 key(s). Operation may take minutes depending on selected curve/key/seed size...
Success: Key(s) generated and stored. Please use the key-name "ec384" to reference it in the system.
[admin@bl.B0A151124003]>
```

5.2.1.1.2 Certificate Signing Request (CSR) generation

The Black Lantern allows the Security Administrator to generate CSRs using the gencsr command. The Black Lantern uses one of the previously generated key pairs when generating a CSR. A CSR generated and stored by the system can be displayed on the terminal; the Security Administrator must send the CSR to a trusted CA for signing. The public key, common name, device specific information, organization, organizational unit, and country fields are established when invoking the gencsr command. Public key and common name are mandatory fields, while the rest are optional requiring their respective flag.

The following captures the SCI when the Security Administrator generates a CSR with a key name of "rsa_key" and a CN of "blacklantern.com", and several CSR attributes.

```
[admin@bl.B0A151124003]>gencsr rsa_key blacklantern.com --country US --state California --locality
    Irvine --org GT --unit BL
Success: CSR generated and stored. Please use "gencsr --show rsa_key" to display.
[admin@bl.B0A151124003]>gencsr --show rsa_key
Certificate signing request for key-name rsa_key:

-----BEGIN CERTIFICATE REQUEST-----
MIIC9jCCAd4CAQIwYzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQ8wDQYDVQQH
DAZJcnZpbmUxCzAJBgNVBAoMAkdUMQswCQYDVQQLDAJCTDEcMBoGA1UEAwwTa2V5
X2dlbmVyYXRlZF9vbl9ibDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANJi9Vdh6LZWUiTlEOgNa06Zl6eV85FARlRQiGC74CT8p/m/LWrotkH80rEaXad1
50zq8CK0LdQiqDNAQtWl7H7o7iDiSqlUhsLiwxtKVZWdAklSNHNdtRcuYeI7eCn/
ttdMjwPtjE6phW0WtKLZYtq8+De0V6HGlpLm2vT/X4QyZmd+GIvjKNX3npD9lqlH
Dz2FloXNOWw9M0TzPFnl+6Ps7N64K3htjeZelYW8vi6zZc0/un1Wj/OG2F1nTFD1
FiQeVeGmum961tlGs/NWFzR1BIRosg0cV4DpP1+dnSmF+QSlCgxxgc+zJf/Jwi2W
UauSuqcWMRzjkkYYrSMQiKsCAwEAAaBOMEwGCSqGSIb3DQEJDjE/MD0wDAYDVR0T
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMA0GCSqGSIb3DQEBCwUAA4IBAQAg+GQfpcYF6gxhfbf1bXJjIdcdc6kH
Z0R1NOEpZeCKqtRz/Xx/xATTrs76hlU8gxh62NWxUoMFlRFne7cxdkxzAARNaoXD
9rD6X9oZhExIVkadJ05RmFih8J8Ma/Bxm6Cye2B/Bca3InoebOs52ZGo4wc0NhwB
7ppDirHskQIw23EIUcDrc0Dksf+anNqzBYdSX+FxmvJCcVCFzZKUbMR1f5ZCwZkl
bF9fBcBY/8q3K4nBZE/zm8YXnkggkGHTVpx/CDcyYCajfVG6cSjTXuBka6C1DMTQ
9PWLiBttMe3p86wpOF1Yv4rh0igeVGnbUAJ1PUqdzQAyR2gpkoKiooCp
-----END CERTIFICATE REQUEST-----
```

To import the certificate (after having the CA process the CSR) for this scenario, the Security Administrator must follow the following convention:

```
[admin@bl.B0A151124003]>import --cert localhost

When:
    1. Prompted for key, enter the name of the key associated with the certificate.
    2. Prompted for certificate of the localhost, paste the entire certificate chain for the
    localhost.
    3. Completed pasting, press <CTRL + S> to save the local host certificate and certificate chain.
```

The following captures the SCI when the Security Administrator imports the certificate and certificate chain for *localhost* using a key name of "rsa_key".

```
[admin@bl.B0A151124003]>import --cert localhost
Importing localhost certificate is requested.
Enter key name if key was generated by Black Lantern or hit Enter to import key using serial console:
    rsa_key
Please input certificate for hostname = localhost:
-------------------------------------------------------------------------------------
<CTRL+C to CANCEL> <CTRL+S to SAVE>
-------------------------------------------------------------------------------------
-----BEGIN CERTIFICATE-----
MIIEpjCCA46gAwIBAgICEA0wDQYJKoZIhvcNAQELBQAweDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgMAkNBMQswCQYDVQQKDAJHVDELMAkGA1UECwwCQkwxIDAeBgNVBAMM
F2RlZmF1bHRfaW50ZXJtZWRpYXRlX2NuMSAwHgYJKoZIhvcNAQkBFhFkZWZhdWx0
QGdtYWlsLmNvbTAeFw0xODA5MTQxOTI3NDVaFw0xODEyMjMxOTI3NDVaMGMxCzAJ
BgNVBAYTAlVTMQswCQYDVQQIDAJDQTEPMA0GA1UEBwwGSXJ2aW5lMQswCQYDVQQK
DAJHVDELMAkGA1UECwwCQkwxHDAaBgNVBAMME2tleV9nZW5lcmF0ZWRfb25fYmww
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDSYvVXYei2VlIk5RDoDWtO
mZenlfORQEZUUIhgu+Ak/Kf5vy1q6LZB/NKxGl2ndedM6vAitC3UIqgzQELVpex+
6O4g4kqpVIbC4sMbSlWVnQJJUjRzXbUXLmHiO3gp/7bXTI8D7YxOqYVtFrSi2WLa
vPg3tFehxpaS5tr0/1+EMmZnfhiL4yjV956Q/ZapRw89hZaFzTlsPTNE8zxZ5fuj
7OzeuCt4bY3mXpWFvL4us2XNP7p9Vo/zhthdZ0xQ9RYkHlXhprpvetbZRrPzVhc0
dQSEaLINHFeA6T9fnZ0phfkEpQoMcYHPsyX/ycItllGrkrqnFjEc45JGGK0jEIir
AgMBAAGjggFNMIIBSTAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDAzBglg
```

```
hkgBhvhCAQ0EJhYkT3BlblNTTCBHZW5lcmF0ZWQgU2VydmVyIENlcnRpZmljYXRl
MB0GA1UdDgQWBBRETI0wFEW+PjBY0z5jCT6gp/8/kjCBrwYDVR0jBIGnMIGkgBTH
0AbNehIOg+jItBlV6Z/eeBwcUKGBh6SBhDCBgTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgMAkNBMQ8wDQYDVQQHDAZJcnZpbmUxCzAJBgNVBAoMAkdUMQswCQYDVQQLDAJC
TDEYMBYGA1UEAwwPZGVmYXVsdF9yb290X2NuMSAwHgYJKoZIhvcNAQkBFhFkZWZh
dWx0QGdtYWlsLmNvbYICEBAwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsG
AQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQANWZrFZJKn6LhJZmmuUG0k9R1g9zQ0
Y+oHzBhoonlpihTu4ThF3QdlMiDF+4d3m6V5Nd4LO1M3CorIGk5JTzwmT+d9LpXY
I/u7WiIq8ENTUePJ1pX3nm+1jAnHi6ljKi1EVHXSSq9UdsFimPlzPPiDA/784zlK
DtDf9K/MSt2yqWIn4ti5lYCDkX8rYVWBS2YAj5455GWm8BGLgOE4F5JTGdudiK4E
dj7oUl6lGbwaR82BkI7cyDEdmQ99k8nfTgNWMQ2Lrk95CMeCdt3GV+nyw0vWaysQ
lDR014r48n4QzvQkYw9S8jpQwvsFDOI/SeSpQUgsE8Rfv0+9czPtjAOs
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID3DCCAsSgAwIBAgICEBAwDQYJKoZIhvcNAQELBQAwgYExCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UEBwwGSXJ2aW5lMQswCQYDVQQKDAJHVDELMAkG
A1UECwwCQkwxGDAWBgNVBAMMD2RlZmF1bHRfcm9vdF9jbjEgMB4GCSqGSIb3DQEJ
ARYRZGVmYXVsdEBnbWFpbC5jb20wHhcNMTgwOTE0MTkyNzMxWhcNMjgwOTExMTky
NzMxWjB4MQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExCzAJBgNVBAoMAkdUMQsw
CQYDVQQLDAJCTDEgMB4GA1UEAwwXZGVmYXVsdF9pbnRlcm1lZGlhdGVfY24xIDAe
BgkqhkiG9w0BCQEWEWRlZmF1bHRAZ21haWwuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA3C3+usPlRidxsMlWELP29oDCF8T8EpBzB3X4xjQqFLlP
8oYsk+kG0x7glTQplJJtNFEdFWMGopDtQPeveoV6/wLZq3q65sCM37/S0TxFri9o
B9wNUASYOyFdW1M6d6BeeA+l6xWB/zI1Tmbj4J1fNAW/oNSzfP8S8ekzCTpMzuYa
pxhhZK/kXrqpJhw+BU7GBRJnoSMKbyObnI0z9x8x4dMHSNMtgxwh+FgvZkGfHdC0
8ivs84x0lACbJS8BMUyNiuIiRlc+JvI95PCI5saYVLhHFSSIpohXZ7KnAjzgibvL
A1W0wRDoPKAfMIT4iy+k1Epj4cYSh8QYrSV7PR2alQIDAQABo2YwZDAdBgNVHQ4E
FgQUx9AGzXoSDoPoyLQZVemf3ngcHFAwHwYDVR0jBBgwFoAUmE4mZ1JeMvtMEqjC
4JfGsuVvNQUwEgYDVR0TAQH/BAgwBgEB/wIBATAOBgNVHQ8BAf8EBAMCAYYwDQYJ
KoZIhvcNAQELBQADggEBABfWx0IIEjQDHVIHCMEt0SQEjZ5Prz5hI/caAvwl02ZB
3wHA6w/zkCwt63MSLmW/NoWu7gV+UNV6f+I103pgQfZvwAmV8xyyfmrKYTC9kW8v
xzrRlBuU6wrpW2rRI2bFXrVMAchEvrqsXzNna5WpPEizwzWTD2DqQY7uzioszDyE
J0rJGgkyA6et1R2NlQT+o+tBpA9q52ReHQ3F0A+Vf4ZPNmoUhbfyaC1BIgDC7o7J
U+n9dcWwbZL+khfd6r9cUHS0Ewq84v6w5i9VVM13SWzYyaTz4beAWuy9q+bQaDPa
t6k/FXy/psD1tiASz3A7wWZ2pkPy7srAsWmCDONiUko=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID6jCCAtKgAwIBAgIJAMil9q7EEZK0MA0GCSqGSIb3DQEBCwUAMIGBMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExDzANBgNVBAcMBklydmluZTELMAkGA1UECgwC
R1QxCzAJBgNVBAsMAkJMMRgwFgYDVQQDDA9kZWZhdWx0X3Jvb3RfY24xIDAeBgkq
hkiG9w0BCQEWEWRlZmF1bHRAZ21haWwuY29tMB4XDTE4MDkxNDE5MjczMVoXDTM4
MDkwOTE5MjczMVowgYExCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEPMA0GA1UE
BwwGSXJ2aW5lMQswCQYDVQQKDAJHVDELMAkGA1UECwwCQkwxGDAWBgNVBAMMD2Rl
ZmF1bHRfcm9vdF9jbjEgMB4GCSqGSIb3DQEJARYRZGVmYXVsdEBnbWFpbC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5kQzTGvxuctYpQDlFrpov
Rzet/JUzRVHM6ic9oFI7Fl6KoF/bHCK2ua+AxiTMGjgXS16eUNrcHjy/4UM12uV9
SFgm9fN3MBzB6fqBtJtz5SWsV6Ydr/VuCGGcvBtr61JFXOmKJTQRc2eRiOMqhphR
AsTAe+4BxTs7xzMmvab8RakHOMWS5oRMqd8DQni3Joj10WUf2z6VHKLpPpQIgP9q
wd1ctKWWuIFBGejr28rouW7zVMBsUb875EPLKqs+eF4sH3doUNmzXztZoVRbeQB3
FdmNNv8e260O9SkdOMbxgXiElm7FHwvqvqQ+VAZNzhVnf/EnyFBKTQcZ+A0ndU+/
AgMBAAGjYzBhMB0GA1UdDgQWBBSYTiZnUl4y+0wSqMLgl8ay5W81BTAfBgNVHSME
GDAWgBSYTiZnUl4y+0wSqMLgl8ay5W81BTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAQEAa0UlgIgbKt+5n7MLdFErbBhc
ZRvUpZyWKPvszwq+nhjYlVrJcb7s7wCJ7msB7N/IJtDcEDO5lWYTDYMXc/7U5W5M
EiQUqlm8F1EmpDKP64u+pPPJt6LPQwXPwE1fXGZOinEzpyVFxOUtFkzypXCjveS5
iUgwXA9JGuDV1I/dA02KuPiiMaB/U6lzzYPjhAdS+H9Cwa0JHRk09ZKsZX2Mn1AW
C8Cdrax6ZJ45v8DUZHoNHmOtjs3gitLVNlFV4OafwakwG87JKr3zt5GCbAUFerA0
wEkB84RIIYGpBnroEBHyoPHjJuD0qv5gTEK6DliygLM6SSc4yJDb0S5p/SDjQQ==
-----END CERTIFICATE-----


Success: Certificate and private key imported for host localhost.
```

5.2.1.2 Importing Remote Host CA Chain

In this scenario, to communicate with remote hosts, such as a remote logging server or remote client, the Black Lantern must have the entire CA chain that signed the certificates of each *remotehost*. To associate the CA chain with a *remotehost*, the Security Administrator must import it into the Black Lantern. Consider the CSfC constraints mentioned in Section 1.2 when importing the appropriate CA chain containing certificates generated from specific algorithms and key sizes.

To import the CA chain for this scenario, the Security Administrator must follow the following convention:

```
[admin@bl.B0A151124003]>import --cert <hostname>

Where:
    <hostname> is an identifier (typically certificate CN or SAN) for the CA chain of the remotehost.
When:
    1. Prompted for CA chain of the <hostname>, paste the CA chain.
    2. Completed pasting, press <CTRL + S> to save the CA chain associated with <hostname>.
```

The following figure captures the SCI when the Security Administrator imports the CA chain for *remotehost*.

```
[admin@bl.B0A151124003]>import --cert root-ca.com
Please input certificate for hostname = root-ca.com:
--------------------------------------------------------------------------------------
<CTRL+C to CANCEL> <CTRL+S to SAVE>
--------------------------------------------------------------------------------------
-----BEGIN CERTIFICATE-----
MIID6jCCAtKgAwIBAgIJAOtOc36d0F6dMA0GCSqGSIb3DQEBCwUAMIGBMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExDzANBgNVBAcMBklydmluZTELMAkGA1UECgwC
R1QxCzAJBgNVBAsMAkJMMRgwFgYDVQQDDA9kZWZhdWx0X3Jvb3RfY24xIDAeBgkq
hkiG9w0BCQEWEWRlZmF1bHRAZ21haWwuY29tMB4XDTE4MDkxNDE5MjY1OVoXDTM4
MDkwOTE5MjY1OVowgYExCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEPMA0GA1UE
BwwGSXJ2aW5lMQswCQYDVQQKDAJHVDELMAkGA1UECwwCQkwxGDAWBgNVBAMMD2Rl
ZmF1bHRfcm9vdF9jbjEgMB4GCSqGSIb3DQEJARYRZGVmYXVsdEBnbWFpbC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDDEu5PQ4dDVm8ieyr+4GYT
+IJRFTfcZ/KqKuGl1YiL2GbDz3aMnhKyQQu2dtldqL82ecoK0Bs4KqMpO6hbmA2L
bsYmHbG3KN5OIJNmrJgklLNzfmkTuPSLSwafVZBuThCAfJPwyxCuQX5R6B5VWaFw
sU77bZ/IL5Qc8ppccLn2cUKlRDwL/EhaKXuY7PoZhF78xskzH0xjT55bAwiWoIWE
2RBriKDEOFBrXEg96ZJ4edHDQquN5hv19Qv7I7LqTXgu1LaoRqKBHOq+vBd3mqGT
AN2nBQ0TWvy3MbBeEmDPInLselZ4+2WdlLSLC5bFupI8h31LZSyD2IYaW43GAcl7
AgMBAAGjYzBhMB0GA1UdDgQWBBQAMneIjzbq+jYZrlP0tT1n/rIAizAfBgNVHSME
GDAWgBQAMneIjzbq+jYZrlP0tT1n/rIAizAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAQEAv8uxkKIPrRT962R2a/hioOrO
+tdhHxTBtHY9zjfmCBiavdpulSjSQqfztguQcby5lMdB2cJZMZejeD+ZzM5Cpwf4
8XN2R9ijPSltGTA3b/ZxGO/1TmkRaTAVsXc+uOMwkcSDoYclThammxQDXBkNq8J6
yPaBMmEC4OAKi9+u3y1rPPGkC5Yign/4+1+SQdFUFwkW/EZ30LjDCslgCHwHuxWM
GPnKRhmnlEDhpZlqtF8pzwiB1+S+uvmd8mKMOfDdrBjKfSiCMxrEk6dIawy0TNo4
7qpATSRbuoZZpikfEdCA9Xu/AkBB6GOLuh48J/OK+Goj15l5g6I58VHHJH5+dg==
-----END CERTIFICATE-----


Success: Certificate imported for host root-ca.com.
```

5.3 Secure Communication

TLS is the explicit mechanism for establishing secure communication with the Black Lantern. There exists both a client and a server mode of configuration to appropriately set up a TLS connection. Note that for both TLS client and server modes, session resumption and session tickets are not supported, and no additional configuration is necessary to ensure this.

5.3.1 Client Mode Configuration

The Black Lantern supports the capability of having trusted communication channels between itself and a remote logging server. The Black Lantern uses the Transport Security Layer (TLS) protocol, version 1.2, with mutual authentication to provide privacy and data integrity between itself and the trusted IT Entities it communicates with.

Only Security Administrators are permitted to manage all the configurations necessary for the Black Lantern to establish secure channels to communicate with Authorized IT Entities. This section outlines the Black Lantern's behaviors and steps required to configure the Black Lantern using the SCI.

5.3.1.1 Trusted Communication Channel with a Remote Logging Server

The Black Lantern uses the TLS protocol to establish a trusted communication channel with a remote logging server. In this trusted communication channel, the Black Lantern acts a TLS client while the remote logging server acts as a TLS server.

As part of establishing a trusted channel between the Black Lantern and the logging server, a TLS 1.2 handshake is required without the need for additional configuration. During this handshake, the Black Lantern requests the logging server's certificate and certificate chain. Once received, the Black Lantern validates the certificate and certificate chain to the certificate of a trusted known Root Certificate Authority (CA). Therefore, the Black Lantern must have the CA chain that the logging server's certificate is linked against.

The Black Lantern is designed to use reference identifiers per RFC 6125 section 6 and IPv4 addresses in the certificate's Subject Alternative Name (SAN) or Common Name (CN) as the key for certificate lookup. If the SAN field is not present, the Black Lantern uses the CN as the key for certificate lookup. The SAN (or CN) is the identifier of the remote machine where it hosts the logging server.

To display the list of available certificates in the Black Lantern certificate store/database, the Security Administrator can type the getcert command on the SCI.

```
[admin@bl.B0A151124003]>getcert

Hostname: 192.168.1.2
Hostname: 192.168.1.3
Hostname: 192.168.1.4
Hostname: localhost
Hostname: externalhost1.localdomain.net
Hostname: externalhost2.localdomain.net
```

If the logging server's CA chain does not appear in the list, the Security Administrator can import it into the Black Lantern with the import command.

The Security Administrator must configure the Black Lantern's management settings. To view these configuration settings, use the getconfig command on the SCI.

```
[admin@bl.B0A151124003]>getconfig -f management
|==============================================================
| Key Name                            || Key Value
|==============================================================
| management.authserver               ||
| management.enablelocallogging       || 1
| management.enableremotelogging      || 1
| management.locallogkeepnewest       || 1
| management.locallogstoragesize      || 2048
| management.remoteclient.0           || myremoteclient.com
| management.remoteclient.1           ||
| management.remoteclient.2           ||
| management.remoteclient.3           ||
| management.remoteclient.4           ||
| management.remoteclient.5           ||
| management.remoteclient.6           ||
| management.remoteclient.7           ||
| management.remoteclient.8           ||
| management.remoteclient.9           ||
| management.serviceport              || 8001
| management.tcplogging.enabletls     || 1
| management.tcplogging.host          || myloggingserver.com
| management.tcplogging.port          || 6514
| management.udplogging.host          || 0.0.0.0
| management.udplogging.port          || 514
|==============================================================
```

Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
management.enableremotelogging	Commands Black Lantern to initiate a TLS channel with logging server (1 = True; 0 = False)
management.tcplogging.enabletls	Commands Black Lantern to utilize TLS channel if communicating with logging server (1 = True; 0 = False). Set to 1 to enable secure channel.
management.tcplogging.host	Remote logging server hostname or IP address
management.tcplogging.port	Remote logging server listening port

To view the TLS connection status with the remote logging server, use the getstatus command.

```
[admin@bl.B0A151124003]>getstatus
|-------------------------------------------------------|
|-------------------BL Status-Summary-------------------|
|-------------------------------------------------------|
|               Status Code :                          0|
|            Overall Status :                    Healthy|
|              Model Number :                      BL400|
|             Serial Number :               B0A151124003|
|        Primary Version Id :                   BL.x.x.x|
|      Secondary Version Id :                   BL.x.x.x|
|         Last Startup Time :    2021-06-10 12:31:47 UTC|
|        FIPS-Approved Mode :                    Enabled|
|          On-Board Battery :                        99%|
|        System Temperature :                      35.6C|
|-------------------------------------------------------|
|-------------------------------------------------------|
|                      Boot :                         Ok|
|                       DTB :                         Ok|
|                        OS :                         Ok|
|        Power-On Self Test :                         Ok|
|    Periodic Built-In Test :                         Ok|
|          Crypto Self Test :                         Ok|
|                   Network :                         Ok|
|                   Storage :                         Ok|
|                 Local Log :                         Ok|
|                       NTP :                         Ok|
|    Log Server Certificate :                         Ok|
|  Log Server Communication :                         Ok|
|-------------------------------------------------------|
```

If the Log Server Communication Status indicates Ok, log entries will be forwarded to the remote logging server. In case when the Log Server Communication Status indicates Fail, the Security Administrator can view the local logs (if enabled) to find out more details on the failed TLS connection event. If local logging is enabled, use viewlog command to view the local log entries.

In the event of the connection between the Black Lantern and the remote logging server is broken, the Black Lantern will retry the TLS connection periodically. If the connection continues to be broken, the Security Administrator may re-verify configuration is valid and perform a reboot of the system.

5.3.2 Server Mode Configuration

The Black Lantern supports the capability of allowing trusted communication path between a remote Security Administrator and itself, for the purpose of remote management of the Black Lantern. Remote management capabilities are done through the Black Lantern's RESTful Interface over HTTPS. The Black Lantern is, by default, configured to use TLS 1.2 with mutual authentication to provide confidentiality and data integrity for the trusted path between remote client and itself. The Black Lantern rejects client connection attempts that use SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1. In addition, in accordance with RFC 6960 during TLS Server connection establishment, the Online Certificate Status Protocol (OCSP) is queried for revoked certificates when the certificate contains the specified URI.

As part of the TLS handshake, both the remote client entity and the Black Lantern must have the appropriate certificates installed and perform the correct exchange of certificates. The Black Lantern must have the client's CA chain installed and the proper configurations must be performed.

Only Security Administrators are permitted to manage all the configurations necessary for the Black Lantern to support a trusted path for remote management. This section outlines the Black Lantern's behaviors and steps required to configure the Black Lantern using the SCI. Furthermore, this section does not cover any configurations on the remote client, as the customer may choose to use any client that can communicate with the Black Lantern using the RESTful Interface. Therefore, coverage of client settings is outside the scope of this document.

5.3.2.1 Trusted Communication Path with Remote Management Client

To set up the Black Lantern to be capable of supporting a secure communication path with a remote client, the Security Administrator must set the remote client and the Black Lantern's

RESTful API service port configuration. Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
management.remoteclient.{i}	Remote management client hostname/FQDN or IP address. Note that multiple clients can be authorized for remote management.
management.serviceport	Black Lantern RESTful API service interface (IP address) and (listening) port

For using the local user database as the authentication server, use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
management.authserver	Authentication server to authenticate remote requests against. Set to "localhost" to authenticate against local account credentials (username/password).

Note that account disabling for remote access applies on consecutive login failures when this local authentication is enabled, and the number of allowed consecutive login failures is configurable as well.

The Black Lantern logs the authenticated connection status for both passes and fails. If local logging is enabled, the Security Administrator can use the local log entries to look for the failure reasons via the viewlog command. In the event of a failed authenticated connection attempt, the Security Administrator can re-verify configuration and retry the authenticated connection attempt or perform a reboot of the system.

5.3.3 Additional Related Information

This section provides the Security Administrator with additional information relevant to configure the establishment of secure communication channels and paths for the Black Lantern.

5.3.3.1 Random Number Generation

The Black Lantern implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions". No configuration is necessary for the Random Number Generation (RNG) functionality.

5.3.3.2 Key Generation

In addition to supporting the key algorithms and key sizes for digital signature generation during TLS communication listed in Table 6, the Black Lantern also supports AES 256 bits for encryption and decryption. Consider the CSfC constraints mentioned in Section 1.2 when selecting the appropriate algorithms and key sizes for key generation.

For TLS communication, the ciphersuite is restricted to AES-256-GCM and no other configuration is necessary.

5.3.3.3 Key Establishment

Black Lantern performs key establishment during TLS communication and supports the following scheme: Elliptic Curve-based. The key establishment scheme is directly associated with the type of ciphersuite used when establishing a TLS connection.

5.3.3.3.1 Elliptic Curve-based Key Establishment

The Black Lantern is designed to support two ciphersuites for TLS communication. Elliptic Curve-based key establishment is used when the Black Lantern and its peer communicate using either of the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To ensure the use of Elliptic Curve-based key establishment for TLS communication, the Security Administrator must load RSA-based or ECDSA-based key certificates on the Black Lantern and the peer as described in Section 5.2.

The Black Lantern provides support for the following Elliptic Curve Extensions: secp256r1, secp384r1, or secp521r1. No additional configuration is required.

5.3.3.4 Key Destruction

There are no configurations or circumstances that do not conform to the plaintext key zeroized destruction method.

5.3.3.5 Hash Algorithms

Hash algorithm configuration is available when configuring authenticated NTP. See Section 7.5.1 on how to configure.

To establish a TLS communication channel, the hashing function is specified by cryptographic criteria and as such, the Black Lantern can support SHA-256, SHA-384, or SHA-512. There is no configuration necessary to further restrict this.

5.3.3.6 Keyed Hashing (HMAC)

No configuration is required to ensure HMAC functionality.

6 Audit Functionality

The Black Lantern provides local and remote audit storage capabilities. Management of these facilities is limited to users with the Security Administrator role. Local and remote logging are independent capabilities and do not have behavioral impact on one another. When both capabilities are enabled, audit data is logged locally and then remotely in real-time as generated. Log data is buffered in memory and flushed into file whenever the buffer is exceeded or when the user issues the “--flush” option with the viewlog command on the SCI.

The content of remote and local audit data is identical. When local logging is enabled, audit data will be logged and stored locally on filesystem. When remote logging is enabled, audit data will be sent externally to a remote entity, as configured. Remote logging is performed using TLS over a TCP channel. Note that audit data is considered read-only, and no interface exists to modify audit records.

The Black Lantern follows the "Syslog Protocol", as specified in RFC 5424, to format each of its audit records. The following is an example of an audit record and its mapping to the RFC:

```
<109>1 2017-03-30T22:04:03.0Z bldevice1 DeviceMgr 0 - - Ev: Generate key item (Success), ID: admin,
     Src: Serial, Rsn: [no error], Item: testrsa.prv.enc
```

Table 7: Syslog Protocol Mapping

Priority Value	<109>
Version	1
Timestamp	2017-03-30T22:04:03.0Z
Hostname	bldevice1
App Name	DeviceMgr
Process ID	0
Message ID	-
Structure Data	-
MSG	Ev: Generate key item (Success), ID: admin, Src: Serial, Rsn: [no error], Item: testrsa.prv.enc

In addition, each MSG contains the following fields:

- Ev: - the type of audit event.
- ID: - the identity who caused the event.
- Rsn: - contains the outcome (success or failure) of the event.

6.1 Configuring Remote Audit Storage

See Section 5.3.1.1 for instructions on configuring the trusted communication channel to a remote logging server to enable remote audit storage.

6.2 Configuring Local Audit Storage

Configuration of Audit Storage is limited to users with the Security Administrator role. Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
management.enablelocallogging	Enables local audit logging (1 = Enabled; 0 = Disabled)
management.locallogkeepnewest	Allows oldest log entries to be overwritten when local storage is full. Otherwise, drop newest entries.
management.locallogstoragesize	Size of local storage in megabytes. Range: 500MB - 2048MB

Care should be taken when decreasing the local log storage size parameter. If the parameter is set to a size smaller than the actual size of the stored logs, some stored logs will be deleted from the system to accommodate the smaller defined log storage size.

6.2.1 Low Local Storage Space Warnings

The Black Lantern warns the Security Administrator once there is 25% local storage space remaining by issuing local log storage warning audit records. Additional warnings are issued when the remaining capacity reaches 15%, 10%, 5%, 4%, 3%, 2%, and 1%. An example of this audit record is shown below.

```
03-24T13:37:32.024 [20:37:31.0Z bldevice1 LogDistService[0]audit.war:Ev: Local logging (Success), ID:
    [SYSTEM], 25 percent storage remaining
```

Once local logging storage is full, old local log data is, by default, overwritten with the newest and a counter of all overwritten log entries will begin incrementing to track these entries. This overwritten counter value will be available as a warning whenever the viewlog command is invoked. In addition, this overwrite log entry behavior can be changed to drop log entry behavior (and maintaining a dropped count) by disabling overwriting through configuration.

```
[admin@bl.B0A151124003]>viewlog -n 2
Flushing local logging buffer...Done
<109>1 2022-05-19T19:13:20.404Z bldevice1 DeviceManager 0 - - Ev: Authentication (Success), ID: admin
    Src: Serial, Rsn: No error
<109>1 2022-05-19T19:13:20.404Z bldevice1 DeviceManager 0 - - Ev: Login (Success), ID: admin Src:
    Serial

Warning: Detected 0 dropped and 1024 overwritten log entries.
Local log storage may be full and need to be expanded/purged.

[admin@bl.B0A151124003]>
```

6.2.2 Clearing Local Log Data

The entire local storage can be cleared by using the following rm command. Note that this operation cannot be reversed and that all locally stored audit data will be permanently removed from Black Lantern.

```
[admin@bl.B0A151124003]>rm -r -f log/
Success: Removed 1 matching item(s).
[admin@bl.B0A151124003]>
```

Optionally, a subset of the local log data may be cleared. Local log data is stored in individual files and can be deleted on a file-by-file basis. To remove log data, perform the ls command to display the list of log filenames, followed by the rm command to remove individual log files or the entire log directory. Wildcards are also permitted.

```
[admin@bl.B0A151124003]>ls log/
DIR            - Tue May 16 15:45:17 2017 ./
DIR            - Mon May 15 22:13:47 2017 ../
              27 Tue May 16 20:52:13 2017 logIndex.txt
          262037 Tue Jan 31 05:23:39 2017 log_1485823840.txt
          262024 Tue Jan 31 09:15:52 2017 log_1485840219.txt
          262028 Tue Jan 31 10:40:23 2017 log_1485854152.txt
          262133 Tue Jan 31 14:40:10 2017 log_1485859223.txt

[admin@bl.B0A151124003]>rm log/log_1485823840.txt
Remove 'log_1485823840.txt'?
Enter <yes> to continue or any key otherwise.
yes
Success: Removed 1 matching item(s).
[admin@bl.B0A151124003]>
```

The overwritten log entries counter will be cleared either by removing the entire log directory or by removing the “logIndex.txt” file in the log directory where this counter is being tracked.

Clearing any log files or the “logIndex.txt” file will be logged in an audit record such as the following.

```
<109>1 2017-05-16T23:33:56.0Z bldevice1 DeviceMgr 0 - - Ev: Remove item (Success), ID: secadmin, Src:
    Serial, Rsn: [no error], Item: /log/log_1494792613.txt
```

The Black Lantern protects itself against unauthorized modification and deletion of local audit logs by only permitting administrator users with Security Administrator role to manage the logging functionalities, which includes the clearing of local logs.

6.3 Viewing local audit records

Local logs can be viewed using the viewlog command on the SCI. Because of the large number of logs often in the system, filtering commands are provided.

Example. View the last two entries in the local log.

```
[admin@bl.B0A151124003]>viewlog -n 2
```

```
Flushing local logging buffer...Done
<109>1 2022-05-19T19:13:20.404Z bldevice1 DeviceManager 0 - - Ev: Authentication (Success), ID: admin
     Src: Serial, Rsn: No error
<109>1 2022-05-19T19:13:20.404Z bldevice1 DeviceManager 0 - - Ev: Login (Success), ID: admin Src:
     Serial
```

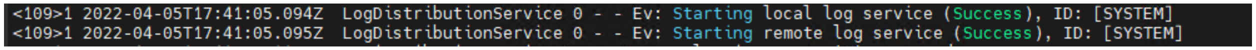
6.4 Audit Events

Table 8 summarizes a list of audit events being logged. Each audit record will record at least this information: date/time of event, type of event, identity who caused the event, and outcome (success or failure). Some logs require more information, as noted for each event below.

Sample audit records for each auditable action.

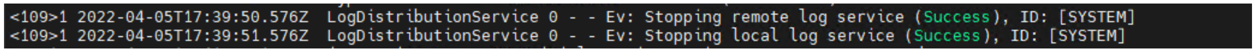
a) Start-up and shut-down of the audit functions;

Start of Audit Functions:



```
<109>1 2022-04-05T17:41:05.094Z  LogDistributionService 0 - - Ev: Starting local log service (Success), ID: [SYSTEM]
<109>1 2022-04-05T17:41:05.095Z  LogDistributionService 0 - - Ev: Starting remote log service (Success), ID: [SYSTEM]
```

Stop of Audit Functions:

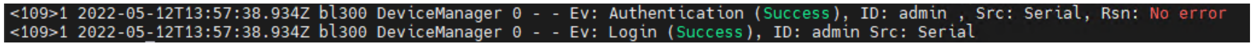


```
<109>1 2022-04-05T17:39:50.576Z  LogDistributionService 0 - - Ev: Stopping remote log service (Success), ID: [SYSTEM]
<109>1 2022-04-05T17:39:51.576Z  LogDistributionService 0 - - Ev: Stopping local log service (Success), ID: [SYSTEM]
```

b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:

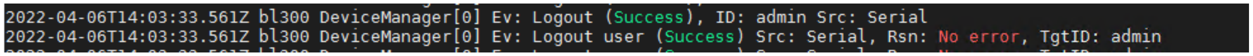
• Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).

Administrator interactive Login:



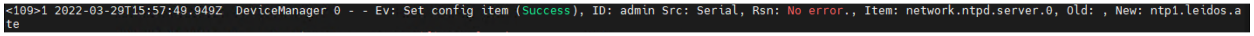
```
<109>1 2022-05-12T13:57:38.934Z bl300 DeviceManager 0 - - Ev: Authentication (Success), ID: admin , Src: Serial, Rsn: No error
<109>1 2022-05-12T13:57:38.934Z bl300 DeviceManager 0 - - Ev: Login (Success), ID: admin Src: Serial
```

Administrator interactive logout:



```
2022-04-06T14:03:33.561Z bl300 DeviceManager[0] Ev: Logout (Success), ID: admin Src: Serial
2022-04-06T14:03:33.561Z bl300 DeviceManager[0] Ev: Logout user (Success) Src: Serial, Rsn: No error, TgtID: admin
```

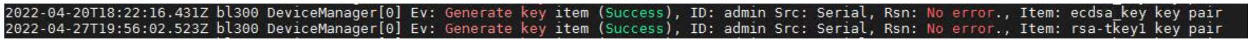
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).



```
<109>1 2022-03-29T15:57:49.949Z  DeviceManager 0 - - Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.ntpd.server.0, Old: , New: ntp1.leidos.a
te
```

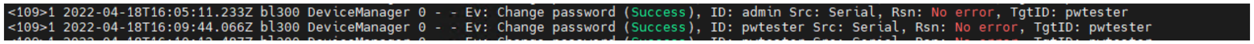
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).

Note: the TOE only allows for internal generation of key pairs.



```
2022-04-20T18:22:16.431Z bl300 DeviceManager[0] Ev: Generate key item (Success), ID: admin Src: Serial, Rsn: No error., Item: ecdsa_key key pair
2022-04-27T19:56:02.523Z bl300 DeviceManager[0] Ev: Generate key item (Success), ID: admin Src: Serial, Rsn: No error., Item: rsa-tkey1 key pair
```

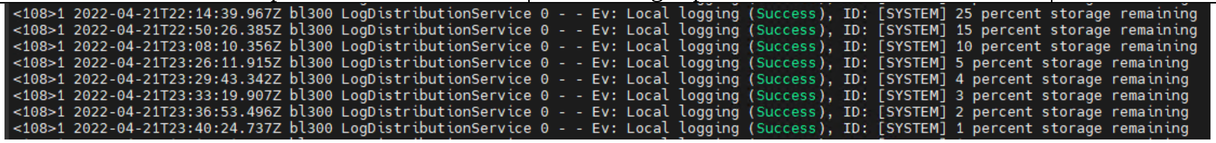
- Resetting passwords (name of related user account shall be logged).



```
<109>1 2022-04-18T16:05:11.233Z bl300 DeviceManager 0 - - Ev: Change password (Success), ID: admin Src: Serial, Rsn: No error, TgtID: pwtester
<109>1 2022-04-18T16:09:44.066Z bl300 DeviceManager 0 - - Ev: Change password (Success), ID: pwtester Src: Serial, Rsn: No error, TgtID: pwtester
```

Table 8: Black Lantern Audit Events

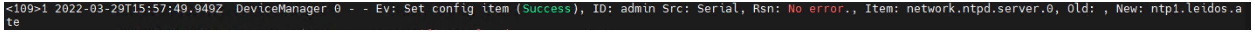
Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.2/LocSpace	None.	None.
FAU_STG_EXT.3/LocSpace	Low storage space for audit events.	None.



```
<108>1 2022-04-21T22:14:39.967Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 25 percent storage remaining
<108>1 2022-04-21T22:50:26.385Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 15 percent storage remaining
<108>1 2022-04-21T23:08:10.356Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 10 percent storage remaining
<108>1 2022-04-21T23:26:11.915Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 5 percent storage remaining
<108>1 2022-04-21T23:29:43.342Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 4 percent storage remaining
<108>1 2022-04-21T23:33:19.907Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 3 percent storage remaining
<108>1 2022-04-21T23:36:53.496Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 2 percent storage remaining
<108>1 2022-04-21T23:40:24.737Z bl300 LogDistributionService 0 - - Ev: Local logging (Success), ID: [SYSTEM] 1 percent storage remaining
```

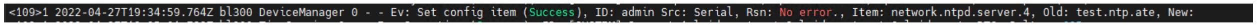
Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
See FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, and FCS_TLSS_EXT.2 audits		
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity of new/removed time server

Configuration:



```
<109>1 2022-03-29T15:57:49.949Z  DeviceManager 0 - - Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.ntpd.server.0, Old: , New: ntp1.leidos.a
te
```

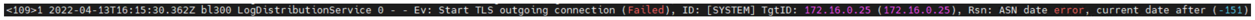
Removal:



```
<109>1 2022-04-27T19:34:59.764Z bl300 DeviceManager 0 - - Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.ntpd.server.4, Old: test.ntp.ate, New:
```

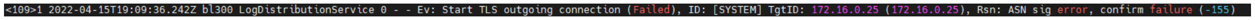
Requirement	Auditable Events	Additional Audit Record Contents
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS session	Reason for failure

Expired Certificate:



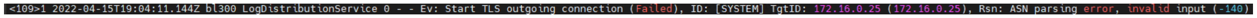
```
<109>1 2022-04-13T16:15:30.362Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: ASN date error, current date after (-151)
```

Certificate Signature issue:



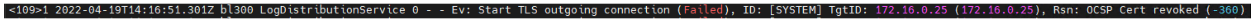
```
<109>1 2022-04-15T19:09:36.242Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: ASN sig error, confirm failure (-155)
```

Certificate Parse Issue:



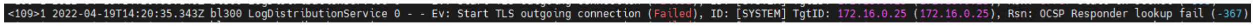
```
<109>1 2022-04-15T19:04:11.144Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: ASN parsing error, invalid input (-140)
```

OCSP Cert Revoked:



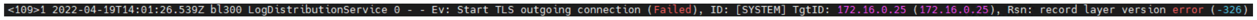
```
<109>1 2022-04-19T14:16:51.301Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: OCSP Cert revoked (-360)
```

OCSP down:



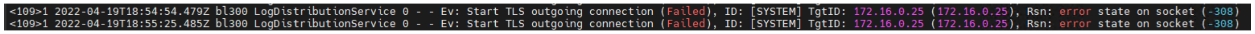
```
<109>1 2022-04-19T14:20:35.343Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: OCSP Responder lookup fail (-367)
```

TLS protocol Version issue:



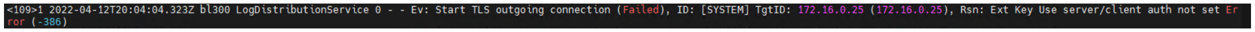
```
<109>1 2022-04-19T14:01:26.539Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: record layer version error (-326)
```

Socket issue:



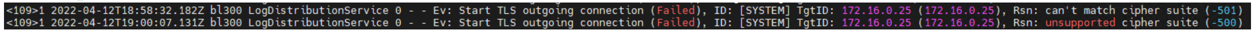
```
<109>1 2022-04-19T18:54:54.479Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: error state on socket (-308)
<109>1 2022-04-19T18:55:25.485Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: error state on socket (-308)
```

Client/Server Auth Error



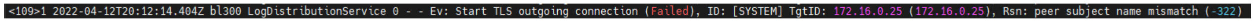
```
<109>1 2022-04-12T20:04:04.323Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: Ext Key Use server/client auth not set Er
ror (-386)
```

TLS CipherSuite Issue



```
<109>1 2022-04-12T18:58:32.182Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: can't match cipher suite (-501)
<109>1 2022-04-12T19:00:07.131Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: unsupported cipher suite (-500)
```

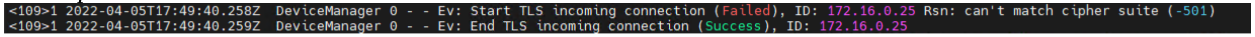
TLS Subject name mismatch



```
<109>1 2022-04-12T20:12:14.404Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Failed), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: peer subject name mismatch (-322)
```

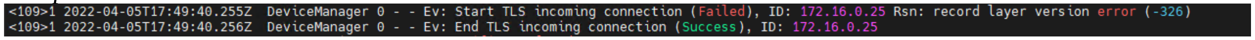
FCS_TLSC_EXT.2	None	None
FCS_TLSS_EXT.1	Failure to establish a TLS session	Reason for failure

TLS CipherSuite Issue:



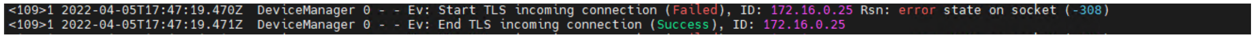
```
<109>1 2022-04-05T17:49:40.258Z  DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: can't match cipher suite (-501)
<109>1 2022-04-05T17:49:40.259Z  DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.0.25
```

TLS protocol Version issue:



```
<109>1 2022-04-05T17:49:40.255Z  DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: record layer version error (-326)
<109>1 2022-04-05T17:49:40.256Z  DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.0.25
```

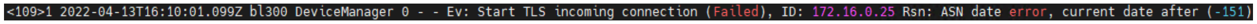
Socket issue:



```
<109>1 2022-04-05T17:47:19.470Z  DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: error state on socket (-308)
<109>1 2022-04-05T17:47:19.471Z  DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.0.25
```

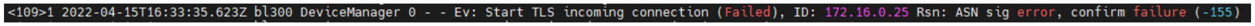
FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure

Expired Certificate:



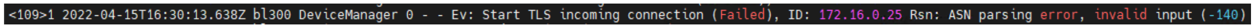
```
<109>1 2022-04-13T16:10:01.099Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: ASN date error, current date after (-151)
```

Certificate Signature issue:



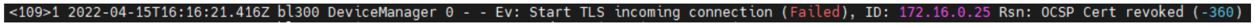
```
<109>1 2022-04-15T16:33:35.623Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: ASN sig error, confirm failure (-155)
```

Certificate Parse Issue:



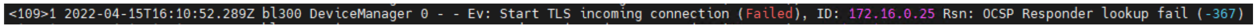
```
<109>1 2022-04-15T16:30:13.638Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: ASN parsing error, invalid input (-140)
```

OCSP Cert Revoked:



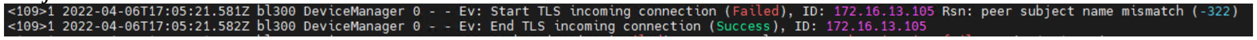
```
<109>1 2022-04-15T16:16:21.416Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: OCSP Cert revoked (-360)
```

OCSP down:



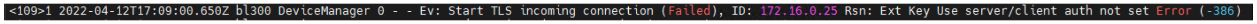
```
<109>1 2022-04-15T16:10:52.289Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: OCSP Responder lookup fail (-367)
```

Subject name mismatch



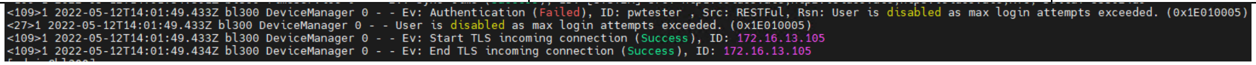
```
<109>1 2022-04-06T17:05:21.581Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.13.105 Rsn: peer subject name mismatch (-322)
<109>1 2022-04-06T17:05:21.582Z bl300 DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.13.105
```

Client/Server Auth Error



```
<109>1 2022-04-12T17:09:00.650Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Failed), ID: 172.16.0.25 Rsn: Ext Key Use server/client auth not set Error (-386)
```

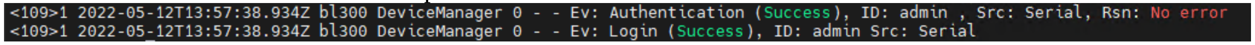
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).



```
<109>1 2022-05-12T14:01:49.433Z bl300 DeviceManager 0 - - Ev: Authentication (Failed), ID: pwtester , Src: RESTFul, Rsn: User is disabled as max login attempts exceeded. (0x1E010005)
<27>1 2022-05-12T14:01:49.433Z bl300 DeviceManager 0 - - User is disabled as max login attempts exceeded. (0x1E010005)
<109>1 2022-05-12T14:01:49.433Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Success), ID: 172.16.13.105
<109>1 2022-05-12T14:01:49.434Z bl300 DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.13.105
```

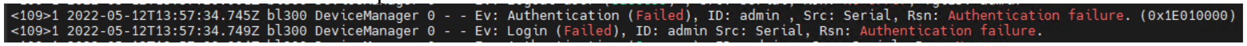
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).

Local Successful Authentication Attempt



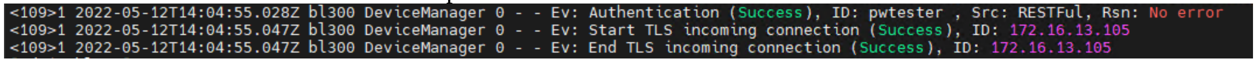
```
<109>1 2022-05-12T13:57:38.934Z bl300 DeviceManager 0 - - Ev: Authentication (Success), ID: admin , Src: Serial, Rsn: No error
<109>1 2022-05-12T13:57:38.934Z bl300 DeviceManager 0 - - Ev: Login (Success), ID: admin Src: Serial
```

Local Failed Authentication Attempt



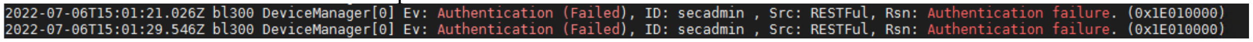
```
<109>1 2022-05-12T13:57:34.745Z bl300 DeviceManager 0 - - Ev: Authentication (Failed), ID: admin , Src: Serial, Rsn: Authentication failure. (0x1E010000)
<109>1 2022-05-12T13:57:34.749Z bl300 DeviceManager 0 - - Ev: Login (Failed), ID: admin Src: Serial, Rsn: Authentication failure.
```

Remote Successful Authentication Attempt



```
<109>1 2022-05-12T14:04:55.028Z bl300 DeviceManager 0 - - Ev: Authentication (Success), ID: pwtester , Src: RESTFul, Rsn: No error
<109>1 2022-05-12T14:04:55.047Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Success), ID: 172.16.13.105
<109>1 2022-05-12T14:04:55.047Z bl300 DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.13.105
```

Remote Failed Authentication Attempt



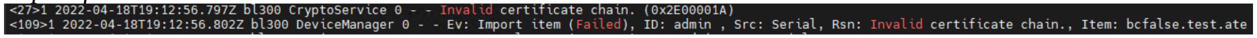
```
2022-07-06T15:01:21.026Z bl300 DeviceManager[0] Ev: Authentication (Failed), ID: secadmin , Src: RESTFul, Rsn: Authentication failure. (0x1E010000)
2022-07-06T15:01:29.546Z bl300 DeviceManager[0] Ev: Authentication (Failed), ID: secadmin , Src: RESTFul, Rsn: Authentication failure. (0x1E010000)
```

FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
See FIA_UIA_EXT.1 audits.		
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement, or removal of trust anchors in the TOE’s trust store	Reason for failure of certificate validation Identification of certificates added, replaced, or removed as trust anchor in the TOE’s trust store

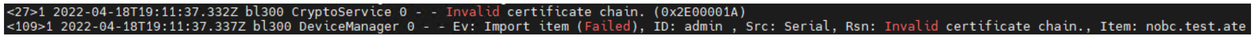
Certificate validation attempts:

Evidence for this can be seen in FCS_TLSS_EXT.2 and FCS_TLSC_EXT.1 audits

Import failures:

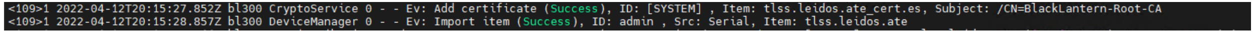


```
<27>1 2022-04-18T19:12:56.797Z bl300 CryptoService 0 - - Invalid certificate chain. (0x2E00001A)
<109>1 2022-04-18T19:12:56.802Z bl300 DeviceManager 0 - - Ev: Import item (Failed), ID: admin , Src: Serial, Rsn: Invalid certificate chain., Item: bcfalse.test.ate
```



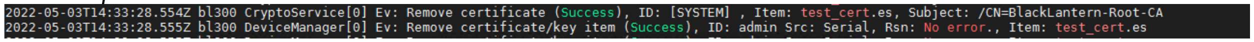
```
<27>1 2022-04-18T19:11:37.332Z bl300 CryptoService 0 - - Invalid certificate chain. (0x2E00001A)
<109>1 2022-04-18T19:11:37.337Z bl300 DeviceManager 0 - - Ev: Import item (Failed), ID: admin , Src: Serial, Rsn: Invalid certificate chain., Item: nobc.test.ate
```

Adding to Trust store, Replacing in Trust Store:



```
<109>1 2022-04-12T20:15:27.852Z bl300 CryptoService 0 - - Ev: Add certificate (Success), ID: [SYSTEM] , Item: tlss.leidos.ate_cert.es, Subject: /CN=BlackLantern-Root-CA
<109>1 2022-04-12T20:15:28.857Z bl300 DeviceManager 0 - - Ev: Import item (Success), ID: admin , Src: Serial, Item: tlss.leidos.ate
```

Removal from Trust Store:

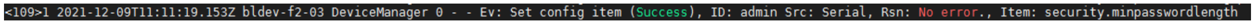


```
2022-05-03T14:33:28.554Z bl300 CryptoService[0] Ev: Remove certificate (Success), ID: [SYSTEM] , Item: test_cert.es, Subject: /CN=BlackLantern-Root-CA
2022-05-03T14:33:28.555Z bl300 DeviceManager[0] Ev: Remove certificate/key item (Success), ID: admin Src: Serial, Rsn: No error., Item: test_cert.es
```

FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
Evidence for this can be seen in FPT_TUD_EXT.1 audits.		

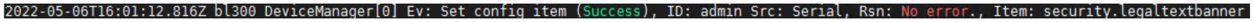
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.

Setting the minimum password length required for user passwords



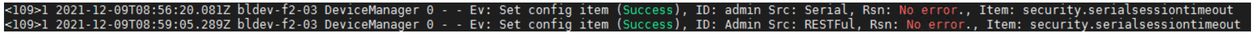
```
<109>1 2021-12-09T11:11:19.153Z bldev-f2-03 DeviceManager 0 - - Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: security.minpasswordlength
```

Configuring the login banner



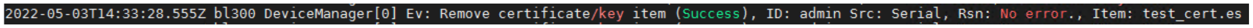
```
2022-05-06T16:01:12.816Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: security.legaltextbanner
```

Configuring inactivity time



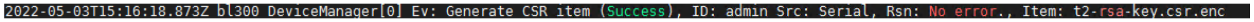
```
<109>1 2021-12-09T08:56:20.081Z bldev-f2-03 DeviceManager 0 - - Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: security.serialsessiontimeout
<109>1 2021-12-09T08:59:05.289Z bldev-f2-03 DeviceManager 0 - - Ev: Set config item (Success), ID: Admin Src: RESTFul, Rsn: No error., Item: security.serialsessiontimeout
```

Deleting a certificate private key



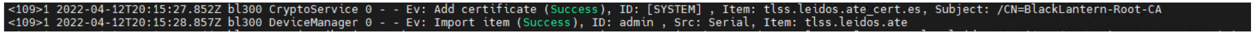
```
2022-05-03T14:33:28.555Z bl300 DeviceManager[0] Ev: Remove certificate/key item (Success), ID: admin Src: Serial, Rsn: No error., Item: test_cert.es
```

Generating a CSR



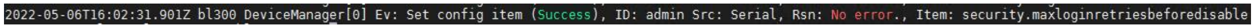
```
2022-05-03T15:16:18.873Z bl300 DeviceManager[0] Ev: Generate CSR item (Success), ID: admin Src: Serial, Rsn: No error., Item: t2-rsa-key.csr.enc
```

Importing a certificate



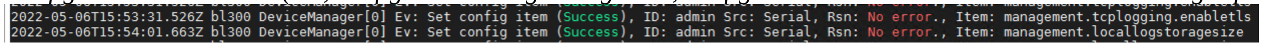
```
<109>1 2022-04-12T20:15:27.852Z bl300 CryptoService 0 - - Ev: Add certificate (Success), ID: [SYSTEM] , Item: tlss.leidos.ate_cert.es, Subject: /CN=BlackLantern-Root-CA
<109>1 2022-04-12T20:15:28.857Z bl300 DeviceManager 0 - - Ev: Import item (Success), ID: admin , Src: Serial, Item: tlss.leidos.ate
```

Configure the authentication failure parameters

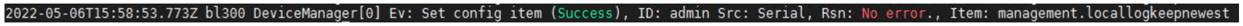


```
2022-05-06T16:02:31.901Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: security.maxloginretriesbeforedisable
```

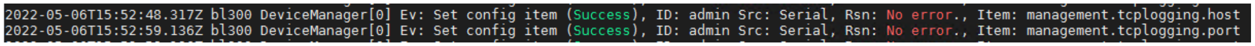
Configure audit behavior (i.e., configure local log storage size, configure TOE behavior when local audit storage space is full)



```
2022-05-06T15:53:31.526Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: management.tcplogging.enabletls
2022-05-06T15:54:01.663Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: management.locallogstoragesize
```

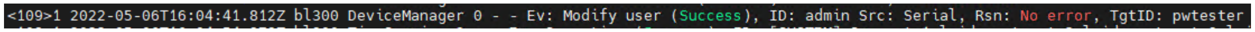


```
2022-05-06T15:58:53.773Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: management.locallogkeepnewest
```



```
2022-05-06T15:52:48.317Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: management.tcplogging.host
2022-05-06T15:52:59.136Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: management.tcplogging.port
```

Re-enable an administrator account



```
<109>1 2022-05-06T16:04:41.812Z bl300 DeviceManager 0 - - Ev: Modify user (Success), ID: admin Src: Serial, Rsn: No error, TgtID: pwtester
```

Ability to Update the TOE
Evidence for this can be seen in FPT_TUD_EXT.1 audits.

Ability to set the time used for timestamps
Evidence for this can be seen in FTP_STM_EXT.1 audits and FCS_NTP_EXT.1 audits.

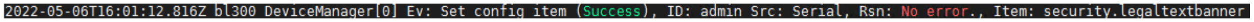
Ability to configure NTP

Evidence for this can be seen in FCS_NTP_EXT.1 audits.

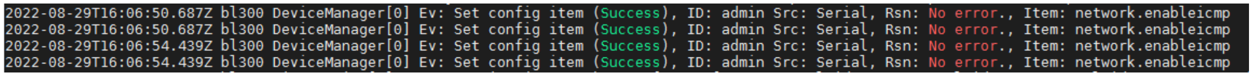
Ability to manage the trust store and designate certificates as trust anchors

Evidence for this can be seen in FIA_X509_EXT.1/Rev audits

Ability to configure the list of TOE-provided services before an entity is authenticated



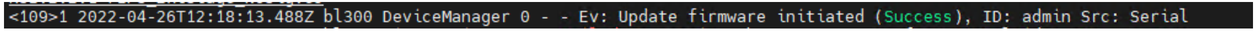
```
2022-05-06T16:01:12.816Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: security.legaltextbanner
```



```
2022-08-29T16:06:50.687Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.enableicmp
2022-08-29T16:06:50.687Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.enableicmp
2022-08-29T16:06:54.439Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.enableicmp
2022-08-29T16:06:54.439Z bl300 DeviceManager[0] Ev: Set config item (Success), ID: admin Src: Serial, Rsn: No error., Item: network.enableicmp
```

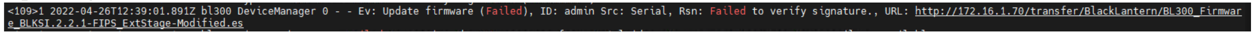
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.

Initiate Update:

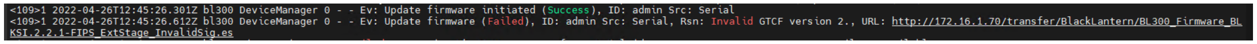


```
<109>1 2022-04-26T12:18:13.488Z bl300 DeviceManager 0 - - Ev: Update firmware initiated (Success), ID: admin Src: Serial
```

Update failed:

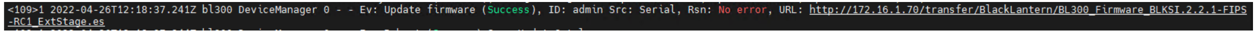


```
<109>1 2022-04-26T12:39:01.891Z bl300 DeviceManager 0 - - Ev: Update firmware (Failed), ID: admin Src: Serial, Rsn: Failed to verify signature., URL: http://172.16.1.70/transfer/BlackLantern/BL300_Firmwar
e_BLKSI.2.2.1-FIPS_ExtStage-Modified.es
```



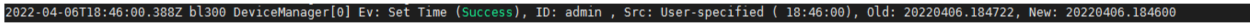
```
<109>1 2022-04-26T12:45:26.301Z bl300 DeviceManager 0 - - Ev: Update firmware initiated (Success), ID: admin Src: Serial
<109>1 2022-04-26T12:45:26.612Z bl300 DeviceManager 0 - - Ev: Update firmware (Failed), ID: admin Src: Serial, Rsn: Invalid GTCF version 2., URL: http://172.16.1.70/transfer/BlackLantern/BL300_Firmware_BL
KSI.2.2.1-FIPS_ExtStage_InvalidSig.es
```

Update Success:



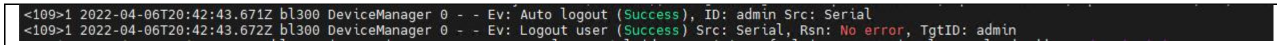
```
<109>1 2022-04-26T12:18:37.241Z bl300 DeviceManager 0 - - Ev: Update firmware (Success), ID: admin Src: Serial, Rsn: No error, URL: http://172.16.1.70/transfer/BlackLantern/BL300_Firmware_BLKSI.2.2.1-FIPS
-RC1_ExtStage.es
```

FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).



```
2022-04-06T18:46:00.388Z bl300 DeviceManager[0] Ev: Set Time (Success), ID: admin , Src: User-specified ( 18:46:00), Old: 20220406.184722, New: 20220406.184600
```

FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.

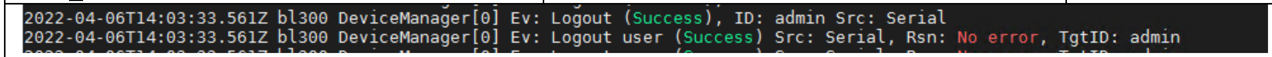


```
<109>1 2022-04-06T20:42:43.671Z bl300 DeviceManager 0 - - Ev: Auto logout (Success), ID: admin Src: Serial
<109>1 2022-04-06T20:42:43.672Z bl300 DeviceManager 0 - - Ev: Logout user (Success) Src: Serial, Rsn: No error, TgtID: admin
```

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.

N/A, The TOE does not implement remote sessions in a manner where session locking can occur, and this is requirement has been vacuously met.

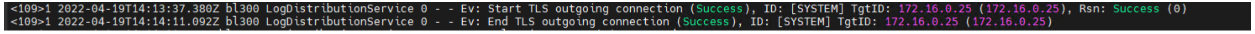
FTA_SSL.4	The termination of an interactive session.	None.



```
2022-04-06T14:03:33.561Z bl300 DeviceManager[0] Ev: Logout (Success), ID: admin Src: Serial
2022-04-06T14:03:33.561Z bl300 DeviceManager[0] Ev: Logout user (Success) Src: Serial, Rsn: No error, TgtID: admin
```

FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

Start/End of Trusted channel

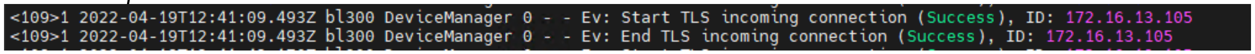


```
<109>1 2022-04-19T14:13:37.380Z bl300 LogDistributionService 0 - - Ev: Start TLS outgoing connection (Success), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25), Rsn: Success (0)
<109>1 2022-04-19T14:14:11.092Z bl300 LogDistributionService 0 - - Ev: End TLS outgoing connection (Success), ID: [SYSTEM] TgtID: 172.16.0.25 (172.16.0.25)
```

Failures of Trusted channel
These can be seen in the FCS_TLSC_EXT.1 audits

FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

Start/End of Trusted Path



```
<109>1 2022-04-19T12:41:09.493Z bl300 DeviceManager 0 - - Ev: Start TLS incoming connection (Success), ID: 172.16.13.105
<109>1 2022-04-19T12:41:09.493Z bl300 DeviceManager 0 - - Ev: End TLS incoming connection (Success), ID: 172.16.13.105
```

Failures of Trusted Path
These can be seen in the FCS_TLSS_EXT.1 and FCS_TLSS_EXT.2 audits.

7 Management

7.1 TSF Data

7.1.1 User Roles

The TOE implements a role-based access control model with the following defined roles:

- Security Administrator — manages all security-related functionality of the Black Lantern
- Network Administrator — manages all network-related configuration of the Black Lantern
- Application Administrator — manages all application-related (e.g. KSI) configuration of the Black Lantern
- Recovery Agent — specialized role associated with backup and recovery of TOE root key

Note that the Application Administrator and Recovery Agent roles are not relevant to the management of TSF data and as such, will not be covered throughout this document.

The ability to manage TSF data is restricted to the Security Admin and Network Admin roles. This includes the ability to manage the TOE's trust store by uploading X.509 v3 certificates and CA certificates.

The following table lists the SCI commands TOE administrators can use to manage (i.e., create, view, modify, delete, clear, etc.) TSF data and identifies the roles permitted to invoke each command.

Table 9: Functions for Managing TSF Data

Command	Purpose	Roles
addrole	Adds a security management role to a user	Security Admin
adduser	Create new user account on TOE	Security Admin
banner	Configure TOE login banner	Security Admin
delrole	Remove a security management role from a user	Security Admin
deluser	Delete a user account from the TOE	Security Admin
gencsr	Generate certificate signing request	Security Admin
genkey	Generate a cryptographic key	Security Admin
getcert	View certificate information	Security Admin
getconfig	View TOE configuration information	Security Admin Network Admin
gettime	View the system time	Security Admin Network Admin
getuser	View information about TOE user accounts	Security Admin
import	Import configuration information; manage the TOE's trust store by uploading X.509 v3 certificates and CA certificates	Security Admin
moduser	Enable or disable user account	Security Admin
passwd	Change password on user account	Security Admin Network Admin
rm	Remove directories or files from TOE, including keys and local audit logs	Security Admin
setconfig	Modify TOE configuration information	Security Admin

Command	Purpose	Roles
		Network Admin
settime	Set the system time	Network Admin

In addition to these commands, one command available to any entity connected to the serial console at the login prompt is the factoryReset command. This command has the capability to restore the appliance into its original factory condition, removing any user data and configuration generated post-provisioned state. See example below:

```
**************************************************************************************
* Welcome to Black Lantern Serial Console Interface
* _____________________________________________________
*
* This system is for the use of authorized users only. Individuals using this
* computer system without authority, or in excess of their authority, are subject
* to having all of their activities on this system monitored and recorded by
* system personnel. In the course of monitoring individuals improperly using this
* system, or in the course of system maintenance, the activities of authorized
* users may also be monitored. Anyone using this system expressly consents to such
* monitoring and is advised that if such monitoring reveals possible evidence of
* criminal activity, system personnel may provide the evidence of such monitoring
* to law enforcement officials.
**************************************************************************************

username:factoryReset
Do not remove power or reset the system until this operation has finished.
This can take up to several minutes. Are you sure you want to perform a factory reset?
Enter <yes> to continue or any key otherwise.
yes
Do you want to format SATA?
Enter <yes> to continue or any key otherwise.
yes
All user data will be deleted. This will take several minutes. Are you sure you want to format SATA?
Enter <yes> to continue or any key otherwise.
yes
Performing factory reset now....
Info: Attempting to reboot high side...



pre-init
********************************************************
  Boot Loaded....
 Build 0x00080000 Thu Apr  8 17:26:50 2021
********************************************************
Begin Built-In-Test...
Press 'Enter' key to abort...
100% Complete...

Loading OS image...
OS prepared..



*******************************************************************************
* This setup menu will walk you through setting up your Black Lantern.
* - Step 1: Configure the network interface to communicate with management host
*           by running <ifconfig> command. Use <ifconfig --help> for help.
* - Step 2: Run <setupbl> command to download setup file from management host
*           Use <setupbl --help> for help.
******************************************************************************


[blshell]>
```

7.2 Security Settings

This section provides information for available configuration of security policy on the Black Lantern and guidance for best practices for passwords generation and storage.

7.2.1 Configuration

Available security configuration can be viewed using the getconfig command. Below is an example to view all security-related configuration:

```
[admin@bl.B0A151124003]>getconfig -f security
|===================================================================
| Key Name                                         || Key Value
|===================================================================
| security.degradecapabilitiesonlocallogfailed     || 0
| security.dormantaccountdisableperiod             || 0
| security.maxloginretriesbeforedisable            || 5
| security.maxpasswordhistorysize                  || 0
| security.maxpasswordlifetimedays                 || 0
| security.minpasswordchangepercentage             || 0
| security.minpasswordlength                       || 8
| security.minpasswordlifetimedays                 || 0
| security.serialsessiontimeout                    || 300
|===================================================================
| Count: 9
|===================================================================
[admin@bl.B0A151124003]>
```

Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
security.degradecapabilitiesonlocallogfailed	When enabled, on local log failure, degrades some services (e.g. KSI) from running.
security.dormantaccountdisableperiod	Time (in days) of inactive user account before disabling.
security.maxloginretriesbeforedisable	Number of allowed authentication or login failures before user account disabling.
security.maxpasswordhistorysize	Number of passwords to story in history to ensure new password change is different.
security.maxpasswordlifetimedays	Password expiration time (in days).
security.minpasswordchangepercentage	Minimum percentage to differ from old password on password change.
security.minpasswordlength	Minimum password character length.
security.minpasswordlifetimedays	Minimum password period (in days) where user cannot change password.
security.serialsessiontimeout	SCI session timeout (in minutes) before logging out due to inactivity.

Changes to security configuration will not take effect for the logged-in Security Administrator until after the administrator changing the parameter has logged out. For all other accounts, the updated policy will take effect the next time they log in or change their passwords. Note that security configuration relevant to disabling accounts do not apply to administrator accounts with Security role, so Security Administrators can never be disabled from local management SCI access. However, remote management access disabling applies to all administrator accounts.

Below is an example of setting configuration using the setconfig command:

```
[admin@bl.B0A151124003]>setconfig -kp security.minpasswordlength 16
Success: setconfig completed.
[admin@bl.B0A151124003]>
```

New password requirements may be enforced immediately by resetting the password of all users with the moduser command; the command will force users to update their passwords on the next login. In addition, the moduser command can also re-enable a previously disabled administrator account from a security configuration policy violation. Below is an example of re-enabled an administrator account and forcing a password reset on the next SCI login:

```
[admin@bl.B0A151124003]>moduser netadmin --enable
Logged-In User's Password: **********
Success: 1 user(s) updated.
[admin@bl.B0A151124003]>moduser netadmin --reset
Logged-In User's Password: **********
Success: 1 user(s) updated.
[admin@bl.B0A151124003]>
```

Note that remote management of the Black Lantern is done via the RESTful Interface. The TOE does not maintain an interactive session over the RESTful API as each request is a self-contained, identified, and authenticated request. As such, the TOE does not establish an authenticated state that is preserved across multiple commands.

7.2.2 Password Guidance

Passwords are never stored in the Black Lantern in plain text, instead they are stored as salted hashes, utilizing Password-Based Key Derivation Function 2 (PBKDF2) with HMAC-SHA-256. No additional configuration is required. The Black Lantern manages password parameters as configuration settings, which only Security Administrators can manage.

A strong password policy is essential to the security of the Black Lantern. Users should follow their own password management policy. This section provides general guidance for users for password management within the Black Lantern.

Password Recommendations
• Users should not share system user accounts. Each user should have their own account. • Avoid storing passwords on other media. If a password must be stored on other media, it should be stored in a secure manner in which only authorized individuals can access it. • Passwords should be unique, never reuse passwords used in other systems, or by other users. • Passwords should not be easily guessable.

Password Recommendations

- Ideally passwords should be randomly generated, containing no full or partial words.
- Passwords should be changed periodically.

The Black Lantern has some basic password requirements, which help enforce a good password policy. The table below specifies the system password requirements.

Black Lantern password requirements

- minimum of 8 characters
- maximum of 32 characters
- must contain at least 1 digit
- must contain at least 1 lowercase character
- must contain at least 1 uppercase character
- must contain at least 1 special character
- valid characters:
  - “a” to “z”
  - “A” to “Z”
  - “0” to “9”
  - special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, “?”, “_”, “<”, “>”, “.”, “,”, “~”, “|”

7.3 Login Banner

For the SCI, there exists a configurable login banner display that can be customized from the default legal login text. Use the banner command to set a custom legal login text as shown:

```
[admin@bl.B0A151124003]>banner set
Please input your login banner message:
--------------------------------------------------------------------------------
<CTRL+C to CANCEL>   <CTRL+S to SAVE>
--------------------------------------------------------------------------------
This is my custom legal text banner to be displayed at SCI login.
Success: Login banner has been set.
[admin@bl.B0A151124003>
```

7.4 Internet Control Message Protocol (ICMP)

ICMP echo requests are supported in the Black Lantern by default and is available prior to requiring identification or authentication for any non-TOE entity. Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
network.enableicmp	When enabled, respond to ICMP echo requests (e.g. ping).

7.5 Time Synchronization

7.5.1 NTP Settings

The Black Lantern supports the use of NTP servers to synchronize the system/local clocks. Having accurate time on the Black Lantern is critical for proper operations of its services. For this reason, it is recommended to configure multiple NTP servers to protect against attacks on time synchronization. More specifically, configuring more authenticated NTP servers over unauthenticated NTP servers will provide more assurance of accurate time simply because it will guarantee authenticated NTP servers outweigh unauthenticated NTP servers in the time sync algorithm.

The Black Lantern supports NTP v4 as specified in RFC 5905 without any additional configuration. It authenticates the timestamps it receives from NTP servers using SHA-1, SHA-256, SHA-384, or SHA-512 when the configured NTP servers support and are configured for authentication as described below. Note that the Black Lantern does not update its real-time clock based on timestamps received from broadcast or multicast addresses and no additional configuration is required for this behavior.

Use the setconfig command to set the following configuration appropriately:

Key Name	Description (Refer to Section 10)
network.ntpd.server.{i}	NTP server hostname or IP address. Note that multiple servers can be configured.
network.ntpd.server.{i}.auth	Authenticated NTP parameters (in the form of "KeyID DigestAlgorithm Key" with fields separated by whitespace) corresponding to each NTP server (e.g. "1 sha1 0123456789ABCDEF0123456789ABCDEF").
network.ntpd.tsclockdrifttolerance	Time syncing with NTP servers must fall within bounds of this set drift tolerance (in seconds). Otherwise, no time sync occurs with system time.
network.ntpd.tsupdateinterval	Dictates frequency period (in seconds) of time syncing events.

7.5.2 Setting Time Manually

Setting time manually is typically needed in the case where there exists a significantly large drift on the Black Lantern system clock that NTP synchronization is too slow to correct or when NTP servers are unavailable. To force a set time manually on the SCI, use the settime command with either a specific timestamp or NTP server as input to sync with:

```
[admin@bl.B0A151124003]>settime -n time.nist.gov
Warning: Adjusting the clock time may have an impact on applications and services and cause
service interruptions. It is highly recommended to shut down services before making changes.
Event logs, user account expirations, and time-dependent data may also be affected.
Are you sure you would like to continue?
Enter <yes> to continue or any key otherwise.
yes
```

```
Success: settime completed.
Previous Date: 2022-05-24
Previous Time: 22:34:30 UTC
Date: 2022-05-24
Time: 22:34:30 UTC
[admin@bl.B0A151124003]>
```

7.6 Self Test

The TOE performs primary and secondary firmware loads. These images are encrypted and signed while they are at rest. The keys to verify the digital signature and decrypt the firmware images are stored in the TOE. During initial start-up of the TOE, each firmware image is verified prior to executing its code, to ensure it has not been modified. If either of the images does not verify correctly, then the TOE reports this as a fault. If neither image verifies correctly, the TOE does not boot up.

In addition to performing verification and decryption of the firmware files, the extended boot also performs a series of Power On Self Tests (POSTs). The TOE performs the following POSTs:

- RAM March Test—verifies RAM by writing an incrementing integer value and a decrementing integer value into every memory cell. After each write, it reads the value back and compares it to the expected value.

- Error-correcting Code Memory Test—consists of two parts: single-bit error correction; and multi-bit error detection. For the single-bit error correction test, one bit error is injected into each DDR SRAM device. Once the single-bit error is injected, the test confirms the error is detected and corrected. Similarly for the multi-bit error detection test, a multi-bit error is injected into each DDR SRAM device and the test confirms the multi-bit error is detected (note, correction cannot be done on a multi-bit error).

- Special Purpose Register Test—verifies each bit can be read and written in the Special Purpose Registers (SPRs), except for those bits that may put the processor into an unstable state. The SPRs verified by this test comprise the Core SPRs, Processor SPRs, Exception SPRs, Interrupt Vector SPRs, Configuration SPRs, and Debug SPRs. In addition to those SPRs that may put the processor into an unstable state, SPRs that are read-only, write-only, write-once, and read-clear are also excluded from this test.

- General Purpose Register Test—verifies each bit in each general purpose register can be read and written correctly. The test starts by filling the general purpose register under test with 1s. Next, it loops to shift a 0 into each bit position and verifies the data read back matches the expected value.

- Condition Register Test—verifies the Condition Registers (CRs) are working correctly. It first sets certain bits in each CR and reads back the CR to verify that the bits were written. Next, it performs instructions that set bits in the CRs as a side effect and verifies the associated bits were set with the expected value.

- Branch Test—verifies the processor’s branch instructions are functioning as expected. It performs each branch instruction and verifies the program counter ends up at the expected location. In addition, it also verifies the state of the link and counter registers for each branch instruction test. This test does not verify the branch absolute instruction (which branches to an absolute address).

- Integer Math Test—verifies every integer arithmetic instruction to make sure the instruction functions correctly. It executes every integer arithmetic instruction (including compares and shifts) using test patterns that utilize all the data paths and functional operations of the integer arithmetic unit.
- Integer Load and Store Test—verifies the load and store instructions are functioning as expected. It performs loads and stores between the General Purpose Registers and RAM using variations of load and store instructions with different data patterns.
- Floating Point Unit Register Test—verifies the functioning of the floating point registers. It writes multiple patterns to each floating point register and verifies the value read back matches the written pattern.
- Floating Point Unit Load and Store Test—verifies the floating point load and store instructions are working as expected. It uses the floating point registers as well as the floating point instructions to load and store data from/to memory.
- Floating Point Unit Math Test—verifies every floating point math instruction functions correctly. It executes every floating point math instruction and verifies that the floating point status register and the observed result value match the expected values.
- Timebase and Decrementer Test—verifies the Timebase and Decrementer Registers are functioning as expected. First, it writes and verifies each bit of the Timebase and Decrementer registers. Next, it checks for rollover in each bit of the Timebase and Decrementer registers. Finally, it measures the Timebase and Decrementer increment/decrement rate to make sure it is at the expected rate.
- Data Cache Test—verifies the Data Cache is functioning as expected. With memory coherency enabled, it verifies that the written test data pattern is flushed from the cache into memory when the data cache is invalidated. With memory coherency disabled, it verifies the written test data pattern is not written to memory.
- RNG Test—consists of four tests from FIPS 140: Monobit; Poker; Runs; and Repetition Count.
- AES CBC Test—verifies the hardware AES engine in CBC mode is functioning as expected. First it populates a test buffer with random data, and feeds the test buffer, along with a known Key and Initial Vector (IV), to the AES engine to be encrypted using CBC mode. Next, it verifies the AES engine can decrypt correctly by feeding it with the encrypted buffer received from the Encrypt operation with the same known Key and IV.
- AES GCM Test—verifies the hardware AES engine in Galois/Counter Mode (GCM) is functioning as expected. First, it populates a test buffer with random data, and feeds the test buffer, with a known Key and Initial Vector (IV), to the AES engine to be encrypted using GCM. Next, it verifies the AES engine can decrypt correctly by feeding it with the encrypted buffer received from the Encrypt operation with the same known Key and IV.

- Sign and Verification Test—verifies the RSA and ECDSA modes by signing data with a known key and then verifying that the correct signature was generated.
- SHA Test—verifies the hardware SHA engine is functioning as expected. It performs SHA-1, SHA-256, SHA-384 and SHA-512 on a sample data buffer and compares the returned hash with known hashes to make sure they are the same.
- HMAC Test—verifies the hardware HMAC engine is functioning as expected. It performs HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 on a sample data buffer and compares the returned results with known answers to make sure they are the same.

If all these tests pass, the overall status on the POST will indicate “OK”. Otherwise, any failed POST will trigger the TOE to display “Failure” on its “Power On Self Test” status. In addition, any errors encountered are printed out at bootup.

The combination of firmware verifications and POSTs performed during bootup, along with the approach taken, enables the TOE to convey to the Administrator that the TOE is operating properly. Furthermore, in the event of catastrophic failures, errors output during bootup will provide the Administrator adequate information to diagnose the issue.

For faults encountered from these tests, it is recommended to perform a reset of the system using the reboot command to force a re-run of self-tests and possible recovery. This is especially relevant when observing cryptographic self test failures, which will enter an error state, disabling cryptographic services and consequently management functions.

The following is a Black Lantern getstatus sample view:

```
[admin@bl.B0A151124003]>getstatus
|-------------------------------------------------------|
|-------------------BL Status-Summary-------------------|
|-------------------------------------------------------|
|               Status Code :                          0|
|            Overall Status :                    Healthy|
|              Model Number :                      BL400|
|             Serial Number :               B0A151124003|
|        Primary Version Id :                   BL.x.x.x|
|      Secondary Version Id :                   BL.x.x.x|
|         Last Startup Time :    2021-06-10 12:31:47 UTC|
|        FIPS-Approved Mode :                   Disabled|
|          On-Board Battery :                        99%|
|        System Temperature :                      35.6C|
|-------------------------------------------------------|
|-------------------------------------------------------|
|                      Boot :                         Ok|
|                       DTB :                         Ok|
|                        OS :                         Ok|
|        Power-On Self Test :                         Ok|
|    Periodic Built-In Test :                         Ok|
|          Crypto Self Test :                         Ok|
|                   Network :                         Ok|
|                   Storage :                         Ok|
|                 Local Log :                         Ok|
|                       NTP :                         Ok|
|    Log Server Certificate :                         Ok|
|  Log Server Communication :                         Ok|
|-------------------------------------------------------|
```

7.7 Software Updates

Both the current executing version and the most recently installed version of the Black Lantern firmware can be viewed using the getconfig command. See example below:

```
[admin@bl.B0A151124003]>getconfig -f info
|==================================================================
| Key Name                          || Key Value
|==================================================================
| info.cfgdbversion                 || 1.14
| info.installedsoftwareversion     || BLKSI.2.2.1-FIPS
| info.lastconfigchangedate         || 2022-03-17 19:58:09 UTC
| info.lastconfigchangeuser         || admin
| info.overallstatus                || Healthy
| info.runningsoftwareversion       || BLKSI.2.2.1-FIPS
| info.serialnumber                 || B0A151124003
| info.softwarebuilddate            || 2022-03-12 19:29 UTC
|==================================================================
```

The Black Lantern supports the ability to update its firmware using the SCI and an HTTP server. This functionality is restricted to Security Administrators. When performing a firmware update, the Security Administrator will command the Black Lantern to obtain the update image from a specific URL address. The customer is responsible for setting an HTTP server to host the update image. Guardtime Federal is responsible for generating the update image and providing it to the customer. The update image is encrypted and signed by Guardtime Federal. The Black Lantern uses pre-installed keys to verify signature authenticity and decrypt the update image. If the verification or the decryption process of the update image fails, the target Black Lantern will reject the firmware update.

To update the Black Lantern, use the updatebl command. After commanding the Black Lantern to perform an update, the Security Administrator must provide confirmation of the update for the Black Lantern to proceed. After the Black Lantern receives confirmation about the update, it proceeds with the firmware update process. This process takes two steps, and the Black Lantern reboots itself after each step. During the firmware update and reboots, the Black Lantern will temporarily cease to operate until the update is completed. The following is an example of what the Black Lantern displays to the SCI during the update process:

```
[admin@bl.B0A151124003]>updatebl http://my.domain.net/repo/bl/updates/BL_Firmware.es
Firmware update can take up to 10 minutes.
Are you sure you want to perform firmware update at this time?
Do not remove power or reset the system until this operation has finished.
Enter <yes> to continue or any key otherwise.
yes
Info: Firmware update step 1 of 2 starting...
Info: Firmware download in progress...
Success: Done
Info: Firmware verification in progress...
Success: Done
Info: Firmware writing in progress...
Success: Done
Info: Rebooting now...
Attempting to unmount SATA...Done
Attempting to unmount RAMDisk...Done
Info: Attempting to reboot high side...

pre-init
********************************************************
```

```
  Boot Loaded....
 Build 0x00080000 Thu Apr  8 17:26:50 2021
*********************************************************
Begin Built-In-Test...
Press 'Enter' key to abort...
100% Complete...

Loading OS image...
OS prepared..



Info: Firmware update step 2 of 2 starting...
Info: Firmware writing in progress....
Success: Done
Info: Rebooting now...
Attempting to unmount SATA...Done
Attempting to unmount RAMDisk...Done
Info: Attempting to reboot high side...

pre-init
*********************************************************
  Boot Loaded....
 Build 0x00080000 Thu Apr  8 17:26:50 2021
*********************************************************
Begin Built-In-Test...
Press 'Enter' key to abort...
100% Complete...

Loading OS image...
OS prepared..
Services initializing (this may take a minute)...Done



***************************************************************************************
* Welcome to Black Lantern Serial Console Interface
* ______________________________________________________
*
* This system is for the use of authorized users only. Individuals using this
* computer system without authority, or in excess of their authority, are subject
* to having all of their activities on this system monitored and recorded by
* system personnel. In the course of monitoring individuals improperly using this
* system, or in the course of system maintenance, the activities of authorized
* users may also be monitored. Anyone using this system expressly consents to such
* monitoring and is advised that if such monitoring reveals possible evidence of
* criminal activity, system personnel may provide the evidence of such monitoring
* to law enforcement officials.
***************************************************************************************

username:
```

If the firmware update fails, the Black Lantern aborts the firmware update process and outputs an error message to the serial console. The following is an example of what the Black Lantern displays to the SCI if a failure occurs:

```
[admin@bl.B0A151124003]>updatebl http://my.domain.net/repo/bl/updates/BL_Invalid_Firmware.es
Firmware update can take up to 10 minutes.
Are you sure you want to perform firmware update at this time?
Do not remove power or reset the system until this operation has finished.
Enter <yes> to continue or any key otherwise.
yes
Info: Firmware update step 1 of 2 starting...
Info: Firmware download in progress...
Success: Done
Info: Firmware verification in progress...
Error (-1): Failed
Error (503382060): Crypto verification error.
```

8 Appendix A: Serial Console Interface Command Reference

This section details the serial console interface commands and their usages, according to role, for local management.

8.1 Security Admin

```
|----------------------------------------------------------------------|
|------------------------ BLSHELL COMMANDS ----------------------------|
|----------------------------------------------------------------------|
| addrole      : Adds role to user.                                    |
| adduser      : Adds new user.                                        |
| banner       : Sets/Displays the security banner.                    |
| clear        : Clears current screen.                                |
| delrole      : Removes role from user.                               |
| deluser      : Deletes user.                                         |
| exit         : Log out, <quit> and <logout> also work                |
| export       : Exports (print) data files.                           |
| gencsr       : Generates certificate signing request.                |
| genkey       : Generates keys.                                       |
| getcert      : Gets certificate information.                         |
| getconfig    : Gets configuration settings.                          |
| getstatus    : Gets Black Lantern status.                            |
| gettime      : Prints current UTC time.                              |
| getuser      : Gets user information.                                |
| help         : Help menu, <?> also works                             |
| history      : Prints out the history buffer.                        |
| import       : Imports data files.                                   |
| keyceremony  : Enforces key ceremony for key backup and recovery.    |
| ls           : Lists directory contents.                             |
| moduser      : Modifies user.                                        |
| passwd       : Changes password of user.                             |
| ping         : Pings the specified host.                             |
| reboot       : Reboots the system.                                   |
| rm           : Removes directories or files.                         |
| setconfig    : Sets configuration settings.                          |
| shutdown     : Shuts down the system.                                |
| updatebl     : Updates system with firmware files.                   |
| viewlog      : View local log.                                       |
| whoami       : Prints current login user.                            |
|----------------------------------------------------------------------|



------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  addrole [OPTION] USERNAME ROLE...

DESCRIPTION
  Adds ROLE to USERNAME, or multiple ROLE(s) to USERNAME. The USERNAME must exist in the user database. No more than 3
  ROLE(s) can be given, and the ROLE(s) can be: security, network, or application.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display addrole usage.
    addrole --help
  Add security and network role to bluser.
    addrole bluser security network

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  adduser [OPTION] USERNAME ROLE...

DESCRIPTION
  Adds USERNAME with ROLE to user database, or USERNAME with multiple ROLE(s) to user database. ROLE(s) can be
  security, network, application, or recovery-agent. Recovery-agent role cannot be given with any other role.

OPTIONS
  --help, -h, ?
```

```
    Display the usage.

EXAMPLES
  Display adduser usage.
    adduser --help
  Add bluser with security role to user database.
    adduser bluser security

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  banner [OPTION] ACTIONTYPE

DESCRIPTION
  Sets or displays the login banner that appears when a user logs on the system. ACTIONTYPE can be either set or
  display. When setting the login banner, the length of the banner cannot contain more than 16,383 characters. If no
  characters are given while setting the login banner, the login banner will be set to the default text.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display banner usage.
    banner --help
  Set banner.
    banner set
  Display banner.
    banner display

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  clear [OPTION]

DESCRIPTION
  Clears the screen.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display clear usage.
    clear --help
  Clear the screen.
    clear

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  delrole [OPTION] USERNAME ROLE...

DESCRIPTION
  Removes ROLE from USERNAME or remove multiple ROLE(s) from USERNAME. The USERNAME must exist in the user database.
  The ROLE(s) can be security, network, or application.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display delrole usage.
    delrole --help
  Remove roles from bluser.
    delrole bluser security network

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  deluser [OPTION] USERNAME

DESCRIPTION
  Deletes USERNAME from the user database. The USERNAME must exist in the user database.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display deluser usage.
    deluser --help
  Delete bluser from user database.
    deluser bluser
```

```
------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  export [OPTION]... PATH
  export --file FILENAME PATH

DESCRIPTION
  Displays the exported data file via the serial console. Only keys and configuration files can be exported. Export to
  serial is limited to printing 16KB or less. Security admin users are allowed to export data files via FTP and can
  create local backups of configurations. Non-public keys and configuration files require an encryption key.

OPTIONS
  -e KEY_PATH
    Secure export of file using key to encrypt.
  --file FILENAME
    Create local backup of configuration.
  --help, -h, ?
    Display the usage.
  --url URL
    Export to url destination via FTP.

EXAMPLES
  Display export usage.
    export --help
  Export file via serial.
    export keys/key.pub.enc
  Export file via serial.
    export keys/key.enc -e keys/kek.enc
  Create local backup of configuration.
    export configurationDB/config.enc --file snapshot
  Export file via serial.
    export configurationDB/snapshots/config.es -e keys/key.pub.enc
  Export file via FTP.
    export configurationDB/config.enc -e keys/key.pub.enc --url ftp://anon:anon@ftpServer.com/config.enc

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  gencsr [OPTION]... KEYNAME COMMON_NAME
  gencsr --show KEYNAME

DESCRIPTION
  Generates a Certificate Signing Request (CSR) to be exported and signed by a Certificate Authority (CA). The output
  of this CSR can be referenced using KEYNAME. KEYNAME is the key identifier given from genkey command. COMMON_NAME is
  the common name of certificate.

OPTIONS
  --country COUNTRY
    Country of issued certificate. Maximum of 2 chars are allowed.
  --digest ALG
    Digest algorithm type. Can be either sha256 (default) or sha512.
  --display
    Outputs CSR to serial console once it is generated.
  --email EMAIL
    Email address to reference. Maximum of 255 chars are allowed.
  --help, -h, ?
    Display the usage.
  --locality LOCALITY
    Local city of issued certificate. Maximum of 128 chars are allowed.
  --org ORGANIZATION
    Company or organization name. Maximum of 64 chars are allowed.
  --san SAN_LIST
    Subject Alternative Name list. Only DNS type is supported. Hostname and IP address can be used. Use quotes if more
    than one name and separated with "," A maximum of 32 entries are allowed and each entry can have up to a maximum
    of 64 chars.
  --show
    Output a previously generated CSR to serial console.
  --state STATE
    State or province of issued certificate. Maximum of 128 chars are allowed.
  --unit ORG_UNIT
    Group or team within organization. Maximum of 64 chars are allowed.

EXAMPLES
  Display gencsr usage.
    gencsr --help
  Generate csr with algo option and display.
    gencsr mykey myhost.com --digest sha512 --display
  Show a CSR that was previously generated.
    gencsr --show mycsr
  Generate csr with --san option.
    gencsr mykey myhost.com --san "host1.com,host2.com"

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
```

```
SYNOPSIS
  genkey [OPTION]... [KEYNAME]
  genkey [--combine | --split NUM [-t THRESHOLD]] KEYNAME

DESCRIPTION
  Generates cryptographic keys for use such as TLS or secure data exchange. Key generation algorithms that are
  accepted: AES, EC (formerly ECDSA), RSA (default), seed. If key generation algorithm is AES, supported key sizes
  are: 128, 192, 256 (default). If key generation algorithm is EC, supported curve sizes are: 256, 384, 521 (default).
  If key generation algorithm is RSA, supported key sizes are: 2048 (default) and 4096. If key generation algorithm is
  seed, supported seed sizes must be multiple of 8 ranging from 8 to 16K bits (default: 512). KEYNAME must contain at
  least 1 character and at most 128 characters. Must contain at least 1 alphanumeric character. Special characters
  available are: '_-.@'

OPTIONS
  -a ALG
    Generate key using specified algorithm.
  --combine
    Combine key splits into a single key material. Only supported with AES
  --help, -h, ?
    Display the usage.
  -s SIZE
    Generate key using specified curve/key/seed sizes.
  --split NUM
    Divide key material into NUM key splits. Only supported with AES.
  -t THRESHOLD
    Specify minimum NUM of key splits required to reconstruct the original key. Must be used with --split option.

EXAMPLES
  Display genkey usage.
    genkey --help
  Generate AES key with key size 256.
    genkey -a AES -s 256 "AES_Key"
  Generate EC key pair with curve size 521.
    genkey -a EC -s 521 "EC_Key"
  Generate RSA key pair with key size 2048.
    genkey -a RSA -s 2048 "RSA_Key"
  Generate 512 bit seed.
    genkey -a seed -s 512 "Random_Seed"
  Split testkey into 5 parts/sub-keys.
    genkey testkey --split 5
  Split testkey into 5 sub-keys with a threshold of 3.
    genkey testkey --split 5 -t 3
  Combine testkey using the available key splits.
    genkey --combine testkey

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getcert [OPTION]
  getcert --info HOSTNAME [--fingerprint HASH_ALGO]

DESCRIPTION
  Displays list of all installed certificates.
  Additional information printed about a hostname's associated CA certificate chain is limited to just the first
  certificate in the chain. Also a certificate's extension information is limited to displaying only the subject
  alternative name and basic constraints extensions.

OPTIONS
  --details
    Print hostnames and certificates.
  --help, -h, ?
    Display the usage.
  --fingerprint HASH_ALGO
    Use HASH_ALGO to create the certificate fingerprint. HASH_ALGO can be: sha1, sha224, sha256, sha384, or sha512. Can
    only be used with --info option.
  --info HOSTNAME
    Print certificate info associated with HOSTNAME. By default uses SHA1 to create the certificate fingerprint.
  -p NUM
    Change the NUM of entries printed per page. Disable paging by using 0.

EXAMPLES
  Display getcert usage.
    getcert --help
  Get certificate hostnames.
    getcert
  Get certificate hostnames and data.
    getcert --details
  Get certificate info associated with hostname 'myhost'.
    getcert --info myhost
  Get certificate info associated with hostname 'myhost' and use SHA-256 to create fingerprint.
    getcert --info myhost --fingerprint sha256

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getconfig [OPTION]...
```

```
DESCRIPTION
  Displays core configurations for the device.

OPTIONS
  -f FILTER
    Filters configuration with matching start pattern.
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 20) of entries printed per page. Disable paging by using 0.

EXAMPLES
  Display getconfig usage.
    getconfig --help
  Show all device core configurations.
    getconfig
  Show core configurations starting with "monitor".
    getconfig -f monitor
  Show core configurations starting with "monitor.logexport".
    getconfig -f monitor.logexport
  Show all core configurations, 10 entries per page.
    getconfig -p 10

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getstatus [OPTION]...

DESCRIPTION
  Prints the status of the device.

OPTIONS
  --details
    Displays detailed failure information for the selected BIT table. Must be used with -t option.
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 25) of entries printed per page.
  -t TABLE
    Display the specified TABLE. TABLE can be either: post, pbit, crypto.

EXAMPLES
  Display getstatus usage.
    getstatus --help
  Get overall status.
    getstatus
  Display the post table results.
    getstatus -t post
  Display the post table results, 35 entries per page.
    getstatus -t post -p 35
  Display the crypto table failure details.
    getstatus -t crypto --details
  Display the pbit table failure detauls, 10 entries per page.
    getstatus -t pbit --details -p 10

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  gettime [OPTION]

DESCRIPTION
  Prints the Black Lantern's current time in Coordinated Universal Time (UTC).

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display gettime usage.
    gettime --help
  Get current time.
    gettime

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getuser [OPTION] [USERNAME]

DESCRIPTION
  Displays information about a USERNAME or all users in the database.

OPTIONS
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 20) of entries printed per page. Disable paging by using 0.

EXAMPLES
  Display getuser usage.
    getuser --help
  Print info about bluser.
    getuser bluser
  Print info about all users.
    getuser
  Print info about all users, 10 per page.
    getuser -p 10

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  import --config [--preview] [--file PATH | --url URL]
  import --key [--url URL]
  import --cert HOSTNAME

DESCRIPTION
  Saves to the system any of the following types of data: certificates, configuration, keys. Certificate and
  configuration import use is limited to only security admin users.
  Importing CA certificate chain of remote host for TLS communication must be in PEM format, contain CA certificates
  only, contain a root CA certificate and must be in the order of intermediates then root certificates.
  Importing CA certificate chain and private key for local host for TLS communication must be in PEM format, must
  contain leaf certificate and entire CA certificate chain up to the root CA certificates, and must be in the order of
  leaf then intermediates then root certificates.
  The maximum length of each certificate chain allowed to be imported is 16KB. An existing certificate with the same
  hostname will be replaced with the most recently imported.

OPTIONS
  --cert HOSTNAMAE
    Enable certificate chain import. To import a Black Lantern certificate, use "localhost" as HOSTNAME.
  --config
    Enable configuration import.
  --file PATH
    Import configuration snapshot using local path to snapshot file.
  --help, -h, ?
    Display the usage.
  --key
    Enable key import.
  --preview
    Display a table of the configuration being imported. Can only be used when importing configuration.
  --url URL
    Use a URL source via FTP. Cannot be used when importing certificate.

EXAMPLES
  Display import usage.
    import --help
  Import a certificate chain.
    import --cert host.com
  Import localhost certificate and private key.
    import --cert localhost
  Import configuration.
    import --config
  Import configuration snapshot and preview.
    import --config --preview --file /configurationDB/snapshots/temp.es
  Import configuration via FTP.
    import --config --url ftp://anon:anon@ftpServer.com/config.enc
  Import key previously exported from a Black Lantern.
    import --key

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  keyceremony [--status | --open | --close]
  keyceremony --key KEYNAME [--assign USERNAME... | --unassign]

DESCRIPTION
  Establishes and enforces the key ceremony process for key backup and recovery. Recovery agents may only query for the
  key ceremony status, while security admin users may query for key ceremony status, open, close, assign and unassign
  key splits to/from users. It is HIGHLY recommended to close ceremony immediately after key backup or if no key
  backup is required.

OPTIONS
  --assign USERNAME...
    Assign key-splits to key recovery agents. Must be used with --key option.
  --close
    Validate all key holders are assigned and backup keys have been exported and permanently restrict export of any
    plaintext keys.
  --help, -h, ?
    Display the usage.
  --key KEYNAME
    Specify the KEYNAME where its associated key-splits are to be assigned or unassigned. Must be used with --assign or
    --unassign option.
  --open
    Initiate the key ceremony process.
  --status
    Print key ceremony status table, which lists all assigned backup keys and its export status.
  --unassign
    Remove existing backup key assignments for specific key. Must be used with --key option.

EXAMPLES
  Display keyceremony usage.
    keyceremony --help
  Print key ceremony status table.
    keyceremony --status
  Initiate key ceremony.
    keyceremony --open
  Assign backup keys.
    keyceremony --key secretkey --assign agent1 agent2
  Unassign backup keys.
    keyceremony --key secretkey --unassign
  Close key ceremony.
    keyceremony --close

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  ls [OPTION]... [PATH]

DESCRIPTION
  Displays directory contents of user/customer data. Wildcarding ("*") is supported to filter on files. PATH is
  case-sensitive.

OPTIONS
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 100) of entries printed per page. Disable paging by using 0.
  -r
    Reverses the listing (sort) order.

EXAMPLES
  Display ls usage.
    ls --help
  List contents in current directory.
    ls
  List contents in current directory in reverse order.
    ls -r
  List contents in log directory, 10 per page.
    ls /log -p 10
  List contents in log directory ending with ".txt".
    ls /log/*.txt

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  moduser [USERNAME | -a] POLICY

DESCRIPTION
  Applies the policy change to the identified user or users. The USERNAME must exist in the user database. POLICY can
  be one of the following policies: --disable (disable user account), --enable (enable user account), --enable-remote
  (allow remote management for user account), --read (permit user read commands), --read-write (permit user read/write
  commands), --reset (force user to reset password at next login).

OPTIONS
  -a
    Apply policy change to all non-security users.
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display moduser usage.
    moduser --help
  Modify policy to disable bluser.
    moduser bluser --disable
  Modify policy to enable bluser.
    moduser bluser --enable
  Modify policy to permit remote management for bluser.
    moduser bluser --enable-remote
  Modify policy to permit read commands for bluser.
    moduser bluser --read
  Modify policy to permit read/write commands for bluser.
    moduser bluser --read-write
  Modify policy to reset bluser's password.
    moduser bluser --reset
  Modify policy to disable all non-security users.
    moduser -a --disable
  Modify policy to enable all non-security users.
    moduser -a --enable
  Modify policy to reset all non-security user's passwords.
    moduser -a --reset

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  passwd [OPTION] [USERNAME]

DESCRIPTION
  Changes passwords for user accounts. Non-security users may only change the password for their own account, while
  security users may change the password for any account. The password must contain a minimum of 8 characters and have
  no more than 32 characters. Passwords must also contain one or more characters from each of the following sets:lower
  case alphabetics, upper case alphabetics, digits 0 thru 9, and special characters _!@#$%^&*()?<>.,~|

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display passwd usage.
    passwd --help
  Change own password.
    passwd
  Change password for bluser.
    passwd bluser

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  ping [OPTION]... DESTINATION

DESCRIPTION
  Sends an ICMP request to elicit an ICMP response from the specified hostname or IP address.

OPTIONS
  -c COUNT
    Stop after sending COUNT (default: Continuous) request packets.
  -i INTERVAL
    Wait INTERVAL (default: 1) seconds between sending each packet.
  --help, -h, ?
    Display the usage.
  -w TIMEOUT
    Time to wait for a response, in seconds (default: 5).

EXAMPLES
  Display ping usage.
    ping --help
  Ping the host continuously.
    ping www.host.com
  Ping the host 5 times.
    ping www.host.com -c 5
  Ping the host in 2 second intervals.
    ping www.host.com -i 2
  Ping the host and timeout request in 2 seconds.
    ping www.host.com -w 2

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  reboot [OPTION]

DESCRIPTION
  Puts the system in a safe state and issues a software reset.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display reboot usage.
    reboot --help
  Reboot system.
    reboot

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  rm [OPTION]... PATH

DESCRIPTION
  Removes directories/files from the file system. Wildcarding ("*") is supported to filter on files. PATH is
  case-sensitive.

OPTIONS
```

```
  -f
    Removal without confirmation.
  --help, -h, ?
    Display the usage.
  -r
    Remove directories and their contents recursively.

EXAMPLES
  Display rm usage.
    rm --help
  Remove local log directory.
    rm -r /log
  Remove key.pub.es file with confirmation.
    rm /keys/key.pub.es
  Remove key.pub.es without confirmation.
    rm -f /keys/key.pub.es
  Remove contents in keys directory ending with ".pub.es".
    rm /keys/*.pub.es

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  setconfig [OPTION] --kp KEY VALUE...

DESCRIPTION
  Sets the configuration KEY to the corresponding VALUE. Multiple keys can be set in a single command.

OPTIONS
  --help, -h, ?
    Display the usage.
  -p PREFIX
    Prepend all keys with PREFIX, where PREFIX has to be full configuration block name.

EXAMPLES
  Display setconfig usage.
    setconfig --help
  Prepend keys with management configuration block name and set values.
    setconfig -p management --kp tcplogging.host host.com tcplogging.port 4545
  Set keys to their specified values.
    setconfig --kp management.tcplogging.host host.com management.tcplogging.port 4545

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  shutdown [OPTION]

DESCRIPTION
  Puts the system in a safe state to be powered off.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display shutdown usage.
    shutdown --help
  Shut down system.
    shutdown

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  updatebl [OPTION] LOCATION

DESCRIPTION
  Gets firmware from the location provided and initiates the update process according to parameters specified. The
  location can either be a URL or local filepath.

OPTIONS
  --download
    Download and save firmware to download directory.
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display updatebl usage.
    updatebl --help
  Download and save firmware locally from URL.
    updatebl --download https://hostname.net:8080/firmware.es
  Update firmware from local file.
    updatebl downloads/firmware.es
  Update firmware from URL.
    updatebl https://hostname.net:8080/firmware.es

------------------------------------------------------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  viewlog [OPTION]...

DESCRIPTION
  Prints to the serial console all local log messages, 25 log entries printed at a time. By default, the local log is
  searched from its tail.
  If filtering the log using --facility and/or --severity, refer to RFC5424 to find the expected syslog facility values
  and syslog severity values.
  When filtering for logs between a specified time range, TIMESTAMP can be given in the following formats:
  YYYYMMDD.HHMMSS or YYYY-MM-DDTHH:MM:SS. If 0's are substituted for any date component set (year, month, day), the
  current date for that component set will default as the value. For example, if 0000 is the value used for the year
  component of the date the current year will be used.

OPTIONS
  -f FILTER
    Use FILTER as a regex-supported search string with appropriately formatted regex escape characters (e.g. \\d = \d,
    \\\\ = \\). With the -n option, will only filter against the subset of entries requested.
  --facility NUM
    Use NUM for the syslog facility filter.
  --from TIMESTAMP
    Use TIMESTAMP as UTC start timestamp for the time range filter.
  --head
    View from the head of the log.
  --help, -h, ?
    Display the usage.
  -i
    Ignore case sensitivity in FILTER. Must be used with -f option.
  -n NUM
    Output the specified NUM of logs.
  -p NUM
    Change the NUM (default: 25) of log entries printed per page. Disable paging by using 0.
  --severity NUM
    Use NUM for the syslog severity filter.
  --to TIMESTAMP
    Use TIMESTAMP as UTC end timestamp for the time range filter.

EXAMPLES
  Display viewlog usage.
    viewlog --help
  Filter for logs within a specified time range.
    viewlog --from 20160101.120102 --to 20160101.130102
  View the last 100 log entries.
    viewlog -n 100
  View the last 100 log entries, 10 entries per page.
    viewlog -n 100 -p 10
  View the first 100 log entries.
    viewlog -n 100 --head
  View local0 entries from the last 100 log entries.
    viewlog -n 100 --facility 16
  View warning entries from the last 100 log entries.
    viewlog -n 100 --severity 4
  View log entries that contain the string "abc" from the last 100 log entries.
    viewlog -n 100 -f "abc"

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  whoami [OPTION]

DESCRIPTION
  Prints to the serial console the current login user.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display whoami usage.
    whoami --help
  Display current login user.
    whoami

------------------------------------------------------------------------------------------------------------------------
```

8.2 Network Admin

```
|----------------------------------------------------------------------|
|------------------------ BLSHELL COMMANDS ----------------------------|
|----------------------------------------------------------------------|
| clear        : Clears current screen.                                |
| exit         : Log out, <quit> and <logout> also work                |
| getconfig    : Gets configuration settings.                          |
| getstatus    : Gets Black Lantern status.                            |
| gettime      : Prints current UTC time.                              |
| help         : Help menu, <?> also works                             |
| history      : Prints out the history buffer.                        |
| ifconfig     : Gets and sets network configuration                   |
| netstat      : Displays network connectivity information.            |
| passwd       : Changes password of user.                             |
| ping         : Pings the specified host.                             |
| route        : Gets and sets route table.                            |
| setconfig    : Sets configuration settings.                          |
| settime      : Sets system time.                                     |
| whoami       : Prints current login user.                            |
|----------------------------------------------------------------------|



------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  clear [OPTION]

DESCRIPTION
  Clears the screen.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display clear usage.
    clear --help
  Clear the screen.
    clear

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getconfig [OPTION]...

DESCRIPTION
  Displays core configurations for the device.

OPTIONS
  -f FILTER
    Filters configuration with matching start pattern.
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 20) of entries printed per page. Disable paging by using 0.

EXAMPLES
  Display getconfig usage.
    getconfig --help
  Show all device core configurations.
    getconfig
  Show core configurations starting with "monitor".
    getconfig -f monitor
  Show core configurations starting with "monitor.logexport".
    getconfig -f monitor.logexport
  Show all core configurations, 10 entries per page.
    getconfig -p 10

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  getstatus [OPTION]...

DESCRIPTION
  Prints the status of the device.

OPTIONS
  --details
    Displays detailed failure information for the selected BIT table. Must be used with -t option.
  --help, -h, ?
    Display the usage.
  -p NUM
    Change the NUM (default: 25) of entries printed per page.
  -t TABLE
    Display the specified TABLE. TABLE can be either: post, pbit, crypto.

EXAMPLES
  Display getstatus usage.
    getstatus --help
  Get overall status.
    getstatus
  Display the post table results.
    getstatus -t post
  Display the post table results, 35 entries per page.
    getstatus -t post -p 35
  Display the crypto table failure details.
    getstatus -t crypto --details
  Display the pbit table failure detauls, 10 entries per page.
    getstatus -t pbit --details -p 10

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  gettime [OPTION]

DESCRIPTION
  Prints the Black Lantern's current time in Coordinated Universal Time (UTC).

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display gettime usage.
    gettime --help
  Get current time.
    gettime

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  ifconfig [OPTION]
  ifconfig TYPE [SETTING] [VALUE]

DESCRIPTION
  Queries the network interface information and set network configurations. TYPE can be one of the following: sys1 or
  ethX (with X being the interface index). SETTING can be one of the following: gateway, dns, dns2, ip, netmask, dhcp,
  up, down. Up and down settings do not require additional arguments. Gateway, dns, and dns2 are only for sys1. VALUE
  is what the SETTING will be set to. To enable dhcp use 1, to disable use 0.

OPTIONS
  -a
    Display network info of all interfaces.
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display ifconfig usage.
    ifconfig --help
  Get all interface info.
    ifconfig
  Get all interface info.
    ifconfig -a
  Set ip of eth0.
    ifconfig eth0 ip 192.168.1.100
  Bring down eth0.
    ifconfig eth0 down
  Set primary dns for system.
    ifconfig sys1 dns 192.168.1.1
  Set secondary dns for system.
    ifconfig sys1 dns2 192.168.1.1
  Set gateway for system.
    ifconfig sys1 gateway 192.168.1.254

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  netstat [OPTION]

DESCRIPTION
  Displays network connectivity information. Each connection is described in following details:
    Index: Socket descriptor.
    Family: IP address family.
    Recv-Q: Receive queue of bytes received or ready to be received.
    Send-Q: Send queue of bytes ready to be sent.
    LocalAddress: IP address/port of the local end of the socket.
    ForeignAddress: IP address/port of the remote end of the socket.
    Refs: Number of attached processes to this socket.
    State/Backlog: State of the local socket.
    RTO: Retransmission timeout.

OPTIONS
  --help, -h, ?
    Display the usage.
```

```
EXAMPLES
  Display netstat usage.
    netstat --help
  Display network connectivity.
    netstat

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  passwd [OPTION] [USERNAME]

DESCRIPTION
  Changes passwords for user accounts. Non-security users may only change the password for their own account, while
  security users may change the password for any account. The password must contain a minimum of 8 characters and have
  no more than 32 characters. Passwords must also contain one or more characters from each of the following sets:lower
  case alphabetics, upper case alphabetics, digits 0 thru 9, and special characters _!@#$%^&*()?<>.,~|

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display passwd usage.
    passwd --help
  Change own password.
    passwd
  Change password for bluser.
    passwd bluser

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  ping [OPTION]... DESTINATION

DESCRIPTION
  Sends an ICMP request to elicit an ICMP response from the specified hostname or IP address.

OPTIONS
  -c COUNT
    Stop after sending COUNT (default: Continuous) request packets.
  -i INTERVAL
    Wait INTERVAL (default: 1) seconds between sending each packet.
  --help, -h, ?
    Display the usage.
  -w TIMEOUT
    Time to wait for a response, in seconds (default: 5).

EXAMPLES
  Display ping usage.
    ping --help
  Ping the host continuously.
    ping www.host.com
  Ping the host 5 times.
    ping www.host.com -c 5
  Ping the host in 2 second intervals.
    ping www.host.com -i 2
  Ping the host and timeout request in 2 seconds.
    ping www.host.com -w 2

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  route [OPTION]
  route add DESTINATION NETMASK GATEWAY
  route del DESTINATION NETMASK

DESCRIPTION
  Displays routing table, adds static routes to routing table and deletes static routes from routing table. When given
  with no arguments the routing table will be displayed. The DESTINATION is the IP address of the host. The NETMASK is
  not the netmask string and is a value in the range0-32. The GATEWAY is the gateway for the route.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display route usage.
    route --help
  Get route table.
    route
  Delete static route.
    route del 192.168.1.0 24
  Add static route.
    route add 192.168.1.0 24 192.168.1.1
```

```
--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  setconfig [OPTION] --kp KEY VALUE...

DESCRIPTION
  Sets the configuration KEY to the corresponding VALUE. Multiple keys can be set in a single command.

OPTIONS
  --help, -h, ?
    Display the usage.
  -p PREFIX
    Prepend all keys with PREFIX, where PREFIX has to be full configuration block name.

EXAMPLES
  Display setconfig usage.
    setconfig --help
  Prepend keys with management configuration block name and set values.
    setconfig -p management --kp tcplogging.host host.com tcplogging.port 4545
  Set keys to their specified values.
    setconfig --kp management.tcplogging.host host.com management.tcplogging.port 4545

--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  settime [OPTION]...
  settime -n NTP_SERVER

DESCRIPTION
  Sets the system time immediately to the specified date and/or time.

OPTIONS
  -d DATE
    Set the current date on the device to DATE. DATE expected to be in the format: YYYY-MM-DD.
  -f
    Set time without confirmation.
  --help, -h, ?
    Display the usage.
  -n NTP_SERVER
    Synchronize the current date and time on the device with the remote timestamp retrieved from NTP_SERVER. NTP_SERVER
    can be IP address or hostname.
  -t TIME
    Set the current time on the device to TIME. TIME is assumed to be in Coordinated Universal Time (UTC) and expected
    to be in the format: HH:MM:SS.

EXAMPLES
  Display  settime usage.
    settime --help
  Set date on device to July 5th, 2017 without confirmation prompt.
    settime -f -d 2017-07-05
  Set date on device to July 5th, 2017.
    settime -d 2017-07-05
  Set time on device to 23hr 43min 38sec in UTC.
    settime -t 23:43:38
  Set date on device to July 5th, 2017 and time to 23hr 43min 38sec in UTC.
    settime -d 2017-07-05 -t 23:43:38
  Set date and time on device to values retrieved from the time.nist.gov NTP server.
    settime -n time.nist.gov

--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  whoami [OPTION]

DESCRIPTION
  Prints to the serial console the current login user.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display whoami usage.
    whoami --help
  Display current login user.
    whoami

--------------------------------------------------------------------------------------------------------------------------
```

8.3 Recovery-Agent

```
|-----------------------------------------------------------------------|
|------------------------ BLSHELL COMMANDS -----------------------------|
|-----------------------------------------------------------------------|
| clear        : Clears current screen.                                 |
| exit         : Log out, <quit> and <logout> also work                 |
| export       : Exports (print) data files.                            |
| gettime      : Prints current UTC time.                               |
| help         : Help menu, <?> also works                              |
| history      : Prints out the history buffer.                         |
| import       : Imports data files.                                    |
| keyceremony  : Enforces key ceremony for key backup and recovery.     |
| passwd       : Changes password of user.                              |
| ping         : Pings the specified host.                              |
| whoami       : Prints current login user.                             |
|-----------------------------------------------------------------------|



------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  clear [OPTION]

DESCRIPTION
  Clears the screen.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display clear usage.
    clear --help
  Clear the screen.
    clear

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  export [OPTION]... PATH
  export --file FILENAME PATH

DESCRIPTION
  Displays the exported data file via the serial console. Only keys and configuration files can be exported. Export to
  serial is limited to printing 16KB or less. Security admin users are allowed to export data files via FTP and can
  create local backups of configurations. Non-public keys and configuration files require an encryption key.

OPTIONS
  -e KEY_PATH
    Secure export of file using key to encrypt.
  --file FILENAME
    Create local backup of configuration.
  --help, -h, ?
    Display the usage.
  --url URL
    Export to url destination via FTP.

EXAMPLES
  Display export usage.
    export --help
  Export file via serial.
    export keys/key.pub.enc
  Export file via serial.
    export keys/key.enc -e keys/kek.enc
  Create local backup of configuration.
    export configurationDB/config.enc --file snapshot
  Export file via serial.
    export configurationDB/snapshots/config.es -e keys/key.pub.enc
  Export file via FTP.
    export configurationDB/config.enc -e keys/key.pub.enc --url ftp://anon:anon@ftpServer.com/config.enc

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  gettime [OPTION]

DESCRIPTION
  Prints the Black Lantern's current time in Coordinated Universal Time (UTC).

OPTIONS
  --help, -h, ?
```

```
    Display the usage.

EXAMPLES
  Display gettime usage.
    gettime --help
  Get current time.
    gettime

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  import --config [--preview] [--file PATH | --url URL]
  import --key [--url URL]
  import --cert HOSTNAME

DESCRIPTION
  Saves to the system any of the following types of data: certificates, configuration, keys. Certificate and
  configuration import use is limited to only security admin users.
  Importing CA certificate chain of remote host for TLS communication must be in PEM format, contain CA certificates
  only, contain a root CA certificate and must be in the order of intermediates then root certificates.
  Importing CA certificate chain and private key for local host for TLS communication must be in PEM format, must
  contain leaf certificate and entire CA certificate chain up to the root CA certificates, and must be in the order of
  leaf then intermediates then root certificates.
  The maximum length of each certificate chain allowed to be imported is 16KB. An existing certificate with the same
  hostname will be replaced with the most recently imported.

OPTIONS
  --cert HOSTNAMAE
    Enable certificate chain import. To import a Black Lantern certificate, use "localhost" as HOSTNAME.
  --config
    Enable configuration import.
  --file PATH
    Import configuration snapshot using local path to snapshot file.
  --help, -h, ?
    Display the usage.
  --key
    Enable key import.
  --preview
    Display a table of the configuration being imported. Can only be used when importing configuration.
  --url URL
    Use a URL source via FTP. Cannot be used when importing certificate.

EXAMPLES
  Display import usage.
    import --help
  Import a certificate chain.
    import --cert host.com
  Import localhost certificate and private key.
    import --cert localhost
  Import configuration.
    import --config
  Import configuration snapshot and preview.
    import --config --preview --file /configurationDB/snapshots/temp.es
  Import configuration via FTP.
    import --config --url ftp://anon:anon@ftpServer.com/config.enc
  Import key previously exported from a Black Lantern.
    import --key

------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  keyceremony [--status | --open | --close]
  keyceremony --key KEYNAME [--assign USERNAME... | --unassign]

DESCRIPTION
  Establishes and enforces the key ceremony process for key backup and recovery. Recovery agents may only query for the
  key ceremony status, while security admin users may query for key ceremony status, open, close, assign and unassign
  key splits to/from users. It is HIGHLY recommended to close ceremony immediately after key backup or if no key
  backup is required.

OPTIONS
  --assign USERNAME...
    Assign key-splits to key recovery agents. Must be used with --key option.
  --close
    Validate all key holders are assigned and backup keys have been exported and permanently restrict export of any
    plaintext keys.
  --help, -h, ?
    Display the usage.
  --key KEYNAME
    Specify the KEYNAME where its associated key-splits are to be assigned or unassigned. Must be used with --assign or
    --unassign option.
  --open
    Initiate the key ceremony process.
  --status
    Print key ceremony status table, which lists all assigned backup keys and its export status.
  --unassign
```

```
    Remove existing backup key assignments for specific key. Must be used with --key option.

EXAMPLES
  Display keyceremony usage.
    keyceremony --help
  Print key ceremony status table.
    keyceremony --status
  Initiate key ceremony.
    keyceremony --open
  Assign backup keys.
    keyceremony --key secretkey --assign agent1 agent2
  Unassign backup keys.
    keyceremony --key secretkey --unassign
  Close key ceremony.
    keyceremony --close

--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  passwd [OPTION] [USERNAME]

DESCRIPTION
  Changes passwords for user accounts. Non-security users may only change the password for their own account, while
  security users may change the password for any account. The password must contain a minimum of 8 characters and have
  no more than 32 characters. Passwords must also contain one or more characters from each of the following sets:lower
  case alphabetics, upper case alphabetics, digits 0 thru 9, and special characters _!@#$%^&*()?<>.,~|

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display passwd usage.
    passwd --help
  Change own password.
    passwd
  Change password for bluser.
    passwd bluser

--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  ping [OPTION]... DESTINATION

DESCRIPTION
  Sends an ICMP request to elicit an ICMP response from the specified hostname or IP address.

OPTIONS
  -c COUNT
    Stop after sending COUNT (default: Continuous) request packets.
  -i INTERVAL
    Wait INTERVAL (default: 1) seconds between sending each packet.
  --help, -h, ?
    Display the usage.
  -w TIMEOUT
    Time to wait for a response, in seconds (default: 5).

EXAMPLES
  Display ping usage.
    ping --help
  Ping the host continuously.
    ping www.host.com
  Ping the host 5 times.
    ping www.host.com -c 5
  Ping the host in 2 second intervals.
    ping www.host.com -i 2
  Ping the host and timeout request in 2 seconds.
    ping www.host.com -w 2

--------------------------------------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------------------------------------
SYNOPSIS
  whoami [OPTION]

DESCRIPTION
  Prints to the serial console the current login user.

OPTIONS
  --help, -h, ?
    Display the usage.

EXAMPLES
  Display whoami usage.
    whoami --help
  Display current login user.
```

```
    whoami
-----------------------------------------------------------------------------------------------------------------------------
```

9 Appendix B: RESTful APIs

9.1 Overview

RESTful APIs are available for secure remote management.

Black Lantern RESTful endpoints conform to the following format:

- https://[BL FQDN or IP address]:[ServicePort]/blrest/{APIVersion}/{function}

In the above format,

- “blrest” is a keyword and serving as the main context switch for all Black Lantern REST endpoints
- {APIVersion} is a variable string that refers to available API version. The format of the API version String is always upper case “V” follow by the API integer version number, e.g., “V1”, “V2”, etc.
- {function} is a variable that references the actual endpoint function that this API version provides

With the appropriate endpoint in the format above, along with any required HTTP headers and payload specific to each endpoint, a remote RESTful request can be made programmatically to the Black Lantern.

9.2 Additional Error Handling

9.2.1 Error Response

In addition to returning HTTP status code, Black Lantern returns customized details error code in the JSON status payload that can be interpreted by client.

```
{
  "error": "FFFABCD"
}
```

9.2.2 Error Code

The error code is a 32-bit value expressed as a hexadecimal number (upper-case). The first 8 bits is a domain prefix that classifies the code a "generic" or "device-specific". The remaining 24 bits represent the specific response to the client request

9.2.2.1 Domain Prefix

The first 8 bits gives contextual information about the device where the error code comes from. For example, error codes with a prefix of FE will only come from Black Lantern devices, while error codes with a prefix of FD will only come from the remote device management service. The prefix FF is a general purpose prefix that can appear before error codes coming from many different devices.

9.2.2.2 Error Codes

The following outlines the error codes within the system.

General Error Codes (FFxxxxxx)

Error Code	Description
FFFFABCD	Missing required header parameter(s)
FFFFABCE	User authentication failure
FFFFABCF	Unauthorized user
FFFFABF0	Unrecognized payload format
FFFFABF1	Endpoint not defined
FFFFABF2	Unrecognized metric key
FFFFABF3	Method not supported
FFFFABF4	Payload too big
FFFFABF5	Device internal time out
FFFFABF6	Device internal error
FFFFABF7	Configuration validation failure
FFFFABF8	HTTP version not supported
0	Success, application completed operation normally

9.3 Config RESTful Endpoint

9.3.1 Purpose

The config endpoint provides programmatic access to read and write configuration data on Black Lantern device. This endpoint supports both GET and PUT, and payload is exchanged via JSON document.

9.3.2 URI

The URI for API version 1 config endpoint is

- /blrest/V1/config

9.3.3 GET Method

GET method is used to retrieve configurations on the device.

9.3.3.1 Request

9.3.3.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.3.3.1.2 Query Options

Query Options	Config Type Being Queried	Example URI	Note
config=info	Info Configuration Block	/blrest/V1/config?config=info	return configuration info block to caller
config=network	Network Configuration Block	/blrest/V1/config?config=network	return configuration network block to caller
config=management	Management Server Configuration Block	/blrest/V1/config?config=management	return configuration management block to caller
config=security	Security Configuration Block	/blrest/V1/config?config=security	return configuration security block to caller
config=monitor	Monitor Configuration Block	/blrest/V1/config?config=monitor	return configuration monitor block to caller

9.3.3.2 Response

The config endpoint for GET request returns a HTTP status code to indicate success/failure and a JSON payload.

9.3.3.2.1 Payload Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "settings": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "key": {
            "description": "See Black Lantern Configuration appendix for supported config keys.",
            "type": "string"
          },
          "value": {
            "description": "See Black Lantern Configuration appendix for supported config values.",
            "type": "string"
          }
        },
        "required": [
          "key",
          "value"
        ]
      },
      "required": [
        "0"
      ]
    }
  },
  "required": [
    "settings"
  ]
}
```

9.3.3.2.2 Payload Example

```
{
  "settings": [
    {
      "key": "monitor.logexport.exportmethod",
      "value": "5"
    },
    {
      "key": "monitor.logexport.level",
      "value": "6"
    }
  ]
}
```

9.3.4 PUT Method

This method is used to update the configurations on the device.

9.3.4.1 Request

9.3.4.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)

Header	Type	Required	Description
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.3.4.1.2 Payload Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "settings": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "key": {
            "description": "See Black Lantern Configuration appendix for supported config keys.",
            "type": "string"
          },
          "value": {
            "description": "See Black Lantern Configuration appendix for supported config values.",
            "type": "string"
          }
        },
        "required": [
          "key",
          "value"
        ]
      },
      "required": [
        "0"
      ]
    }
  },
  "required": [
    "settings"
  ]
}
```

9.3.4.1.3 Payload Example

```
{
  "settings": [
    {
      "key": "management.authserver",
      "value": "localhost"
    },
    {
      "key": "security.maxloginretriesbeforedisable",
      "value": "5"
    }
  ]
}
```

9.3.4.2 Response

The config endpoint for SET request returns a HTTP status code to indicate success/failure.

9.4 Status RESTful Endpoint

9.4.1 Purpose

The service endpoint provides programmatic access to manage hosted application services on Black Lantern device. This endpoint supports both GET and PUT, and payload is exchanged via JSON document.

9.4.2 URI

The URI for API version 1 service endpoint is

- /blrest/V1/service

9.4.3 GET Method

GET method is used to retrieve service status on the device.

9.4.3.1 Request

9.4.3.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.4.3.1.2 Query Options

Query Options	Example URI	Note
status	/blrest/V1/service?status	Returns status of each hosted application service.

9.4.3.2 Response

The service endpoint for GET request returns a HTTP status code and a JSON payload.

9.4.3.2.1 Payload Schema

```
{
  "type": "object",
  "properties": {
    "services": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "name": {
            "description" : "Service name",
            "type": "string"
          },
          "status": {
            "description" : "'unknown', 'active' or 'inactive'",
            "type": "string"
          }
        }
      }
    }
  }
}
```

9.4.3.2.2 Payload Example

```
{
  "services": [
    {
      "name": "service1",
      "status": "active"
    },
    {
      "name": "service2",
      "status": "inactive"
    }
  ]
}
```

9.4.4 PUT Method

This method is used to signal (reload config, (re)start, stop) the hosted application services on the device.

9.4.4.1 Request

9.4.4.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.4.4.1.2 Payload Schema

```
{
  "type": "object",
  "properties": {
    "services": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "name": {
            "description" : "Service name",
            "type": "string"
          },
          "signal": {
            "description" : "'reload' to reload configuration, 'restart' to (re)start service, or
     'stop' to stop service",
            "type": "string"
          }
        }
      }
    }
  }
}
```

9.4.4.1.3 Payload Example

```
{
  "services": [
    {
      "name": "service1",
      "signal": "reload"
    },
    {
      "name": "service2",
      "signal": "restart"
    }
  ]
}
```

9.4.4.2 Response

The service endpoint for SET request returns a HTTP status code.

9.5 User RESTful Endpoint

9.5.1 Purpose

The user endpoint provides a method to retrieve users from the device and to add, update, and delete users on the device. This endpoint supports PUT and GET method. The request and response are exchanged in JSON format.

9.5.2 URI

The URI for API version 1 service endpoint is

- /blrest/V1/user/

9.5.3 GET Method

The GET method is used to get user information. The GET method returns list of all users on the device.

9.5.3.1 Request

9.5.3.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.5.3.2 Response

The user endpoint for GET request returns a HTTP status code and a JSON payload.

9.5.3.2.1 Payload Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "users": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "username": {
            "description": "username",
            "type": "string"
          },
          "password": {
            "description": "password",
            "type": "string"
          },
          "groupID": {
            "description": "groupID",
            "type": "string"
          }
        },
        "required": [
          "username",
          "password",
          "groupID"
        ]
      },
      "id": "users"
    }
  },
  "required": [
    "users"
  ]
}
```

9.5.3.2.2 Payload Example

```
{
    "users": [
      {
         "username": "user1",
         "password": "encryptedPswd",
         "groupID": "1"
      },
      {
         "username": "user2",
         "password": "encryptedPswd",
         "groupID": "1"
      }
    ]
}
```

9.5.4 PUT Method

The PUT method is used to update user accounts on the device. Accounts may be added, removed, or have their data changed.

9.5.4.1 Request

9.5.4.1.1 Additional HTTP Headers

Header	Type	Required	Description
"x_auth_token"	String	No	Authentication token (Required if remote authentication server is defined.)
"x_auth_user"	String	No	Local account username (Required if local authentication server is defined.)
"x_auth_password"	String	No	Local account password (Required if local authentication server is defined.)

9.5.4.1.2 Payload Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "add": {
      "type": "object",
      "properties": {
        "users": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "user": {
                "type": "string"
              },
              "password": {
                "type": "string"
              },
              "group": {
                "type": "string"
              }
            },
            "required": [
              "user",
              "password",
              "group"
            ]
          }
        }
      },
      "required": [
        "users"
      ]
    },
    "remove": {
      "type": "object",
      "properties": {
        "users": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "user": {
                "type": "string"
              }
            },
            "required": [
              "user"
            ]
          }
        }
      },
      "required": [
        "users"
      ]
    },
    "update": {
      "type": "object",
      "properties": {
        "users": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "user": {
                "type": "string"
              },
              "change": {
                "type": "object",
                "properties": {
                  "key": {
                    "type": "string"
                  },
                  "value": {
                    "type": "string"
                  }
                },
                "required": [
                  "key",
                  "value"
                ]
              }
            },
            "required": [
              "user",
              "change"
            ]
          }
        }
      },
      "required": [
        "users"
      ]
    }
  }
}
```

9.5.4.1.3 Payload Example

```
{
    "add": {
        "users": [{
            "user": "user1",
            "password": "4262199c18274d80374cbd39e2b8258ff6dc42b0319f432a733d46f7d0bfa609",
            "group": "7"
        }, {
            "user": "user2",
            "password": "bccb8e54d3e44e8ad9638d1f8f1f102b3397990ff7ce1e05a8e9510318e764e7",
            "group": "7"
        }]
    },
    "remove": {
        "users": [{
            "user": "user4"
        }]
    },
    "update": {
        "users": [{
            "user": "user3",
            "change": {
                "key": "user",
                "value": "jackson"
            }
        }, {
            "user": "user3",
            "change": {
                "key": "group",
                "value": "0"
            }
        }, {
            "user": "user3",
            "change": {
                "key": "group",
                "value": "1"
            }
        }]
    }
}
```

9.5.4.2 Response

The user endpoint for SET request returns a HTTP status code.

10 Appendix C: Black Lantern Configuration

This section outlines the configuration parameters of the Black Lantern. Where applicable:

- A blank line indicates empty string field.
- {i} means there could be 0 or more of that element in a list format.

Table 10: Black Lantern Configuration DB v2.0

Key	Type	Managing Group	Description	Default Value	Range
management	Complex	Security Admin	Management configuration section		
management.authserver	String	Security Admin	Supplemental authentication server to further authenticate a RESTful request against a user account. If defined with a remote authentication server (e.g. ext.authserver.com:4443), an auth token will be required and validated in the RESTful request against the configured server. If a port is not specified, 443 is the default. If defined with the local authentication server keyword "localhost", local user account credentials will be required and validated in the RESTful request. To disable, leave blank.		string
management.csfcmode	Boolean	Security Admin	Enable/Disable Commercial Solutions for Classified (CSfC) compliance	0	0 or 1
management.enablelocallogging	Boolean	Security Admin	Enable/Disable local logging	1	0 or 1
management.enableremotelogging	Boolean	Security Admin	Enable/Disable remote logging	1	0 or 1
management.locallogkeepnewest	Boolean	Security Admin	Allows oldest log entries to be overwritten when local storage is full.	1	0 or 1
management.locallogstoragesize	Integer	Security Admin	Local log storage size allocation (in MB) Valid range: 500MB - 2048MB (2GB)	2048 (2GB)	500 - 2048

Key	Type	Managing Group	Description	Default Value	Range
			Note: Reducing this value when in a storage size full condition will not truncate (delete) the existing local log files to the new smaller configured storage size.		
management.remoteclient.{i}	String	Security Admin	Governing remote/external management client hostname or address (IPv4). Supports up to 10 clients.		string
management.serviceport	String	Security Admin	Black Lantern's Local IP address and listening port for RESTful Service to bind (e.g. 192.168.1.100:443). To disable, leave blank.		string
management.tcplogging.enabletls	Boolean	Security Admin	Enable/Disable TLS for remote logging	1	0 or 1
management.tcplogging.host	String	Security Admin	TCP remote logging hostname or address (IPv4)	0.0.0.0	string
management.tcplogging.port	Integer	Security Admin	TCP remote logging port	1600	0 - 65535
management.udplogging.host	String	Security Admin	UDP remote logging hostname or address (IPv4)	0.0.0.0	
management.udplogging.port	Unsigned Integer	Security Admin	UDP remote logging port	1600	0 - 65535
monitor	Complex	Security Admin	Monitor configuration section		
monitor.logexport	Complex	Security Admin	Log export configuration section		
monitor.logexport.exportmethod	Integer	Security Admin	Method to direct log Disable (0), Reserved (1, 2, or 3), UDP (4), TCP (5)	5	Disable (0), Reserved (1, 2, or 3), UDP (4), TCP (5)
monitor.logexport.level	Integer	Security Admin	(Syslog) Log level filter Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Info (6), Debug (7)	6	Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Info (6), Debug (7)
network	Complex	Network Admin	Network configuration section		
network.defaultgateway	String	Network Admin	Default gateway/route address (IPv4) Note: Shared across all interfaces.	192.168.0.254	0.0.0.0 - 255.255.255.255

Key	Type	Managing Group	Description	Default Value	Range
network.enableicmp	Boolean	Network Admin	Enable/Disable ICMP	1	0 or 1
network.hostname	String	Network Admin	Hostname of the device		
network.interface.{i}	List<Complex>	Network Admin	Network interface list		
network.interface.{i}.enableinterface	Boolean	Network Admin	NIC enable/disable (True/False)	0 (Interface 0 set to 1)	0 or 1
network.interface.{i}.ipv4	Complex	Network Admin	NIC IPv4 settings		
network.interface.{i}.ipv4.dhcp	Boolean	Network Admin	NIC DHCP enable (True/False) Note: Not available for PCIe or other internal interfaces.	0	0 or 1
network.interface.{i}.ipv4.ip	String	Network Admin	NIC address (IPv4)	192.168.0.x (2...7)	0.0.0.0 - 255.255.255.255
network.interface.{i}.ipv4.mask	String	Network Admin	NIC netmask (IPv4)	255.255.255.0	0.0.0.0 - 255.255.255.255
network.ntpd	Complex	Network Admin	NTP daemon configuration section		
network.ntpd.server.{i}	String	Network Admin	NTP server hostname or address (IPv4). Supports up to 10 hosts.		string
network.ntpd.server.{i}.auth	String	Network Admin	NTP server authentication parameters Format: "KeyID DigestAlgorithm Key" with fields separated by whitespace Example: "1 sha1 0123456789ABCDEF0123456789ABCDEF" KeyID: Shared key identifier with NTP server Supported DigestAlgorithm: sha1, sha256, sha384, sha512 Key: 1-20 characters interprets as printable ASCII (e.g., 21-40 interprets as hex-encoded string		string
network.ntpd.tsclockdrifttolerance	Integer	Network Admin	Time update drift tolerance (in seconds)	5	1 - 3600
network.ntpd.tssamplesize	Integer	Network Admin	Time update sample size	1	1 - 5

Key	Type	Managing Group	Description	Default Value	Range
			(No longer supported)		
network.ntpd.tsupdateinterval	Integer	Network Admin	Time update sync interval (in seconds)	1024	1 - 86400
network.primarydns	String	Network Admin	Primary Domain Name Server (DNS) address (IPv4)	192.168.0.1	0.0.0.0 - 255.255.255.255
network.route.{i}.destip	String	Network Admin	Route destination address (IPv4) (Not available to user)		0.0.0.0 - 255.255.255.255
network.route.{i}.gateway	String	Network Admin	Route gateway address (IPv4) (Not available to user)		0.0.0.0 - 255.255.255.255
network.route.{i}.netmasknumber	Integer	Network Admin	Route netmask (32-bit bit integer representation) (Not available to user)		0.0.0.0 - 255.255.255.255
network.secondarydns	String	Network Admin	Secondary Domain Name Server (DNS) address (IPv4)	192.168.0.1	0.0.0.0 - 255.255.255.255
security	Complex	Security Admin	Security configuration section		
security.degradecapabilitiesonlocallogfailed	Boolean	Security Admin	Setting to force Black Lantern to run in degraded mode (i.e no hosted application services) if local log is failed.	0	0 or 1
security.dormantaccountdisableperiod	Integer	Security Admin	Amount of time (in days) before account is disabled due to inactivity. 0 means that an inactive account will never be disabled.	180	0 - 2147483647
security.legaltextbanner	String	Security Admin	Logged in banner security message. Note: This can only be set and displayed through the banner command.	This system is for the use of authorized users only...	string
security.maxloginretriesbeforedisable	Integer	Security Admin	Max consecutive failed login attempts before disabling account. Note that this extends to RESTful requests when local authentication server is configured.	5	1 - 100

Key	Type	Managing Group	Description	Default Value	Range
security.maxpasswordhistorysize	Integer	Security Admin	Number of password history to check against for duplicate password. Valid range: 0-24	5	0-24
security.maxpasswordlifetimedays	Integer	Security Admin	Password expiration period (in days)	60	0 - 2147483647
security.minpasswordchangepercentage	Integer	Security Admin	Minimum percentage to differ from old password on password change. Valid range: 0 - 100	0	0 - 100
security.minpasswordlength	Integer	Security Admin	Minimum password length Valid range: 8 - 32	8	8 - 32
security.minpasswordlifetimedays	Integer	Security Admin	Minimum password life (in days). User can't change their password within this period.	1	0 - 2147483647
security.serialsessiontimeout	Integer	Security Admin	Serial session timeout (in minutes) 0 means that the serial session will never timeout.	300	0 - 2147483647