Hewlett Packard Enterprise Development LP

Integrated Lights-Out 4 v2.11

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 2.2

Prepared for:

Hewlett Packard Enterprise Development LP
20555 State Highway 249
Houston, TX 77070
United States of America

Phone: +1 281 370 0670
Email: info@hpe.com
http://www.hpe.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies and describes the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the HP Integrated Lights-Out 4 v2.11 with an Advanced license, and will hereafter be referred to as the TOE throughout this document. The TOE is a standard component of HP ProLiant Gen8 and Gen9 servers that simplifies initial server setup, server health monitoring, power and thermal optimization, and remote server administration. The TOE is designed to be independent of the host server and its operating system.

1.1 Document Organization

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and EAL package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett Packard Enterprise Development LP Integrated Lights-Out 4 v2.11 Security Target
ST Version	Version 2.2
ST Author	Corsec Security, Inc.
ST Publication Date	March 8, 2016
TOE Reference	HP Integrated Lights-Out 4 v2.11 on the GLP-3, GLP-4, and Sabine Application Specific Integrated Circuits (ASIC) with an Advanced license
FIPS[1] 140-2 Status	FIPS 140-2 Level 1 validated crypto module, certificate No. 2574

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

The HP Integrated Lights-Out 4 (HP iLO 4) built into HP ProLiant Gen8 and Gen9 servers is an autonomous secure management component embedded directly on the server motherboard. iLO helps simplify initial server setup, power and thermal optimization, remote server administration, and provides server health monitoring with the HP Active Health System (AHS). iLO also provides system administrators[2] with true Agentless Management using SNMP[3] alerts from iLO, regardless of the state of the host server. The Embedded Remote Support (ERS) options allow Gen8 and Gen9 servers to use their Insight Remote Support (IRS) server's registration from iLO, regardless of the operating system software and without the need for additional host software, drivers, or agents. The HP AHS monitors and records changes in the server hardware and system configuration. iLO is available whenever the server is connected to a power source, even if the server main power switch is in the Off position. Figure 1 below shows a screenshot of the iLO management interface.

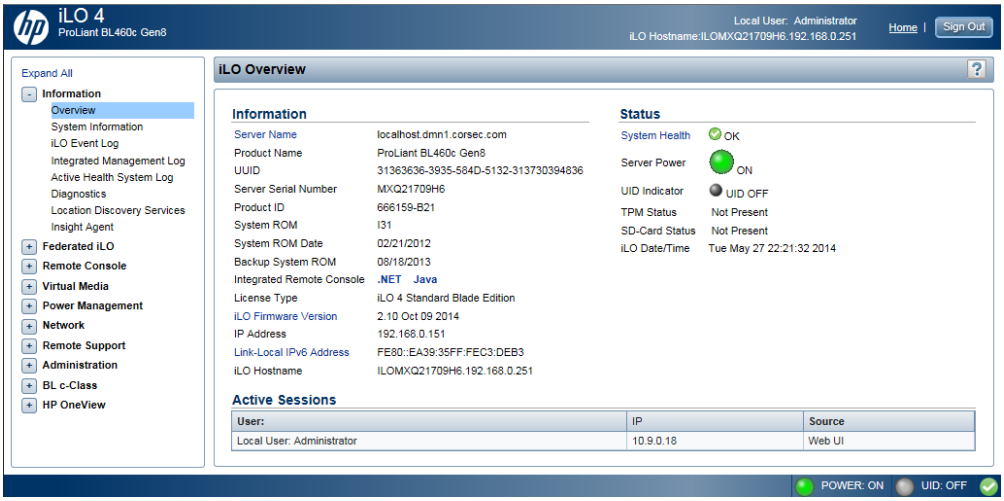

Figure 1 HP iLO (Example Management Screen)

iLO is supported on the following server platforms:

- HP ProLiant Gen8/Gen9 DL Rack Servers
- HP ProLiant Gen8/Gen9 ML Tower Servers
- HP ProLiant Gen8/Gen9 SL/XL Scalable Servers

Rack Servers are complete servers specially designed for an ultra-compact vertical arrangement within a standardized 19-inch mounting rack or cabinet. Tower Servers are upright, free-standing units that contain all the traditional server components: hard disks, motherboards and Central Processing Units (CPU), networking, cabling, power, etc. Scalable Servers are density optimized servers designed for delivering leading-edge performance and efficiency for scale-out environments. The XL series of the Scalable Servers are designed to work with the HP Apollo Systems. No matter the form factor of the server, the iLO hardware and firmware are uniform across all platforms.

Remote access is the key to maximizing efficiency of administration and troubleshooting for enterprise servers. iLO enables remote access to the operating system console, control over the server power and hardware reset functionality, and works with the server to enable remote network booting through a variety of methods. iLO provides Graphical User Interfaces (GUI) and Command Line Interfaces (CLI) that can be accessed by its Internet Protocol (IP) address from either a web browser or third-party software. The common

[2] Note that a system administrator is not a role or privilege level but can refer to any TOE user.
[3] SNMP – Simple Network Management Protocol

method for accessing iLO functionality is mediated by the iLO GUI. Using iLO Federation Management, a system administrator may manage multiple servers from one system running the iLO GUI.

Through iLO, ERS options are available when registered with the IRS server. When configured, information about the server, which iLO is installed on, is sent to HPE either directly or through an IRS centralized hosting device in the local IT[4] environment.

The HP AHS monitors and records changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. The HP AHS does not collect information about operations, finances, customers, employees, partners, or data center (i.e. IP addresses, host names, user names, and passwords).

By sending AHS data to HPE, HPE will use that data for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the HP Privacy Statement. Examples of data that is collected is as follows:

- Server model
- Serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS[5] versions

iLO stores files, such as AHS data, in non-volatile flash memory that is embedded on the system board. This flash memory is called the iLO NAND[6]. HP ProLiant Gen9 servers with a 4GB[7] iLO NAND allow system administrators to use a 1GB non-volatile flash memory partition as if it were an SD[8] card attached to the server, called the Embedded User Partition. By default the Embedded User Partition is disabled.

Advanced features of iLO 4, available via licensing, include (but are not limited to) the following: graphical remote console, multi-user collaboration, power and thermal optimization, health monitoring, virtual media, and console video recording and playback. The advanced features offer sophisticated remote administration of servers in dynamic data center and remote locations. A list of advanced functionality is shown in Table 2.

Table 2 HP iLO 4 Advanced Features

Feature	iLO 4 Advanced
iLO Remote Administration	
Virtual Keyboard, Video, Mouse (KVM[9])	Full text and graphic modes (pre-OS & OS)
Global Team Collaboration (Virtual KVM)	Up to 6 Server Administrators
Console Record and Replay	✓
Virtual Power	✓
Virtual Media	✓

[4] IT – Information Technology
[5] BIOS – Basic Input/Output System
[6] NAND – Negated AND
[7] GB – Gigabyte
[8] SD – Secure Digital
[9] KVM – Keyboard, Video, Mouse

Feature	iLO 4 Advanced
Virtual Folders	✓
Remote Serial Console	SSH Only
Virtual Unit Indicator Display	✓
Simplified Server Setup	
ROM[10]-Based Setup Utility (RBSU)	✓
Option ROM Configuration for Arrays (ORCA)	✓
Power Management & Control	
Present Power Reading	✓
Power Usage Reporting	✓
Ambient Temperature Reporting	✓
Dynamic Power Capping	✓
Power Supply High-Efficiency Mode	✓
Sea of Sensors	✓
Embedded System Health	
Power-On Self Test (POST) and Failure Sequence Replay	✓
iLO and Server Integrated Management Log	✓
Advanced Server Management	✓
Alert Administrator (SNMP Passthrough)	✓
System Health & Configuration Display	✓
Access Security	
Directory Services Authentication	✓
Locally Stored Accounts	✓
Interfaces	
Browser	✓
Command Line	✓
Extensible Markup Language (XML)/Perl Scripting	✓
Integrated Remote Console for Windows Clients	✓
Java Applet Client for Windows and Linux Clients	✓
Security Protocols	
Transport Layer Security (TLS)	✓
Secure Shell	✓
RC4[11]/AES[12] (Virtual KVM)	✓

[10] ROM – Read-Only Memory
[11] RC4 – Rivest Cipher 4
[12] AES – Advanced Encryption Standard

Feature	iLO 4 Advanced
Network Connectivity	
Dedicated Network Interface Controller (NIC)	✓
Shared Network Port	✓

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

HP Integrated Lights-Out 4 v2.11 is a hardware-firmware TOE used to simplify the initial server setup, monitor server health, provide power and thermal optimization, and provide remote server administration. The major features of the TOE include: monitoring server health, access to the Active Health System log, Federation management, secure remote access to the server, controlling the server's virtual media, and controlling server power. iLO is integrated into an HP ProLiant Gen8 or Gen9 DL, ML, SL, or XL server. The TOE functions independently of the server's state of operation by obtaining its power from the auxiliary power plane of the server. This allows the TOE to function as long as the server is plugged into a power source, even if the server is not powered on. HP iLO 4 will be tested on the HP ProLiant Gen8 and Gen9 DL, ML, SL, and XL servers. Figure 2 below depicts the HP iLO Component.

Figure 2 HP iLO Component

Figure 3 shows the details of the single server deployment configuration of the TOE. The following previously undefined acronyms are used in Figure 3:

- LDAP – Lightweight Directory Access Protocol
- SNTP – Simple Network Time Protocol

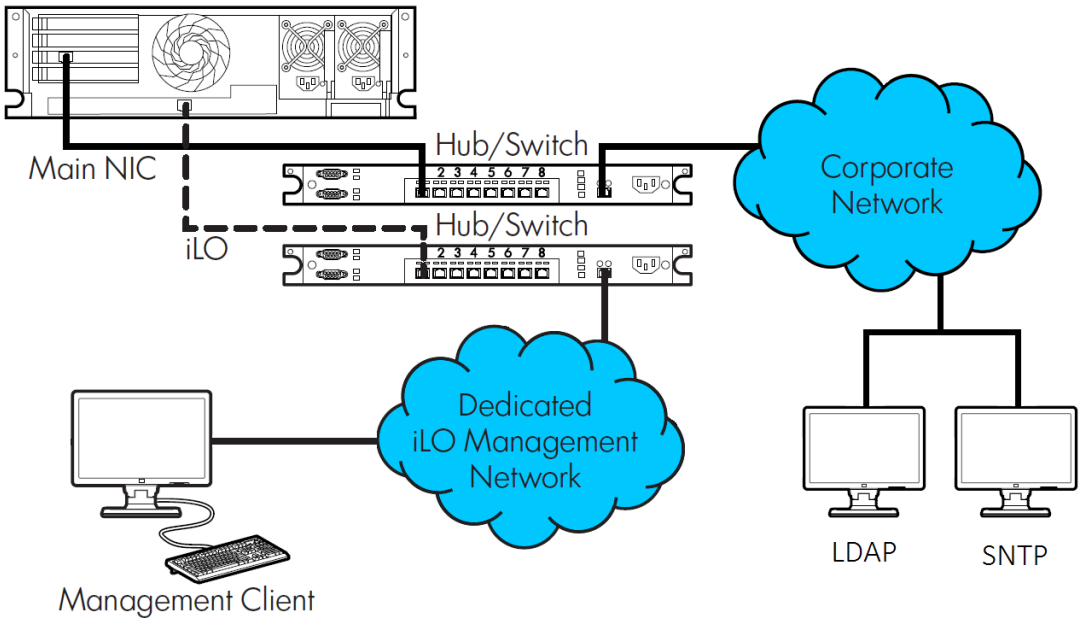

Figure 3 Single Server Deployment Configuration of the TOE

Figure 4 shows the details of the multiple server deployment configuration of the TOE.

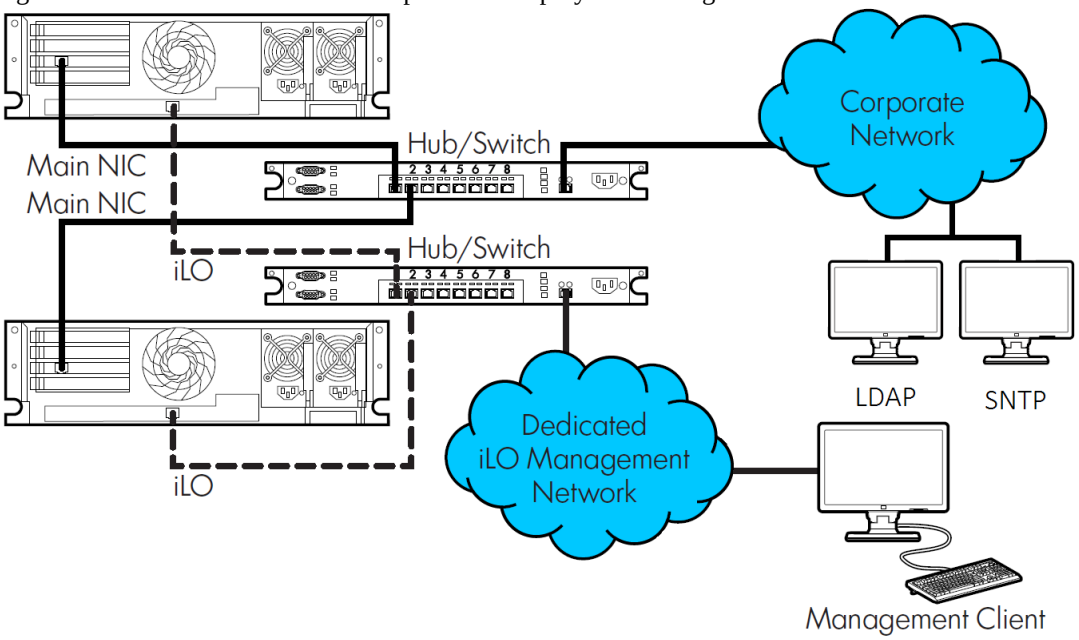

Figure 4 Multiple Server Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a secure Local Area Network (LAN) with external workstations and servers managed by system administrators operating under security policies consistent with those enforced by the system administrators of the TOE. The TOE is integrated into the motherboard of an HP ProLiant Gen8 or Gen9 DL, ML, SL, or XL server as listed in Table 3. The supported servers listed in Table 4 below are required to be part of the TOE environment.

Both local and remote management workstations will be used by system administrators when interfacing with the TOE. The following third party software is required when interfacing with the TOE:

- Java Runtime Environment – Minimum version of 1.4.2_13; Recommended to use the latest
- Microsoft .NET Framework – Minimum version of the 3.5; Recommended to use 4.5
- The following web browsers are supported:
  - Microsoft Internet Explorer 8.x and 11.x
  - Mozilla Firefox ESR[13] 24.x
  - Google Chrome (latest version)

Table 3 specifies the systems that host the TOE and the requirements for the proper operation of the TOE.

Table 3 TOE Evaluated Configuration[14]

Component	Requirements
HP iLO 4 Firmware	Version 2.11
HP iLO 4 Hardware	At least one of the following ASICs: • GLP-3 (Model number 531510-003) • GLP-4 (Model number 531510-004) • Sabine (Model number 610107-002)
HP iLO 4 License	HP iLO 4 Advanced License
HP iLO 4 Host[15]	The HP iLO 4 hardware is contained within the host server and cannot be chosen independently. At least one of the following hosts is required: • HP ProLiant Gen8 DL Rack Server (can contain a GLP-3 or Sabine ASIC) • HP ProLiant Gen9 DL Rack Server (contains a GLP-4 ASIC) • HP ProLiant Gen8 ML Tower Server (contains a Sabine ASIC) • HP ProLiant Gen9 ML Tower Server (contains a GLP-4 ASIC) • HP ProLiant Gen8 SL Scalable Server (contains a Sabine ASIC) • HP ProLiant Gen8 XL Scalable Server (contains a Sabine ASIC) • HP ProLiant Gen9 XL Scalable Server (contains a GLP-4 ASIC)

Table 4 specifies the minimum components for the TOE environment.

Table 4 TOE Environment

Device	Requirements
HP ProLiant Server (TOE host)	At least one of the following servers, two for the multiple server configuration: • HP ProLiant Gen8/Gen9 DL Rack Servers • HP ProLiant Gen8/Gen9 ML Tower Servers • HP ProLiant Gen8/Gen9 SL/XL Scalable Servers
SL Servers Only	HP ProLiant SL Scalable System
XL Servers Only	HP Apollo System

[13] ESR – Extended Support Release

[14] Note that testing was performed on the following HP ProLiant servers: DL160 Gen8 (Sabine), DL360p Gen8 (GLP3), DL380p Gen8 (GLP3), DL560 Gen9 (GLP4), ML310e Gen8 v2 (Sabine), ML350e Gen8 v2 (Sabine), ML150 Gen9 (GLP4), SL140s Gen8 (Sabine), SL210t Gen8 (Sabine), XL170r Gen9 (GLP4), XL190r Gen9 (GLP4), and XL220a Gen8 v2 (Sabine).

[15] For a complete list of the evaluated iLO 4 host server models, please see Appendix A of the HP iLO 4 Guidance Documentation Supplement.

Device	Requirements
LDAP Server	LDAPv3 (RFC[16] 4511)
SNTP Server	SNTPv4 (RFC 5905)

The LDAP server is used for authenticating and identifying TOE users to assign their required roles. Communications for the LDAP server are sent over TLS. An SNTP server will be used by the TOE to synchronize the internal clock with a reliable time source. Both the HP ProLiant SL Scalable System and HP Apollo System are used as midplanes for the servers that they host. They do not provide any management interfaces into the TOE.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.5.1 Physical Scope

Figure 5 depicts the single server configuration while Figure 6 depicts the multiple server configuration. Both diagrams illustrate the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a hardware-firmware solution that simplifies initial server setup, server health monitoring, power and thermal optimization, and remote server administration. The TOE runs on HP ProLiant servers listed in Table 3. The HP ProLiant server that the TOE is embedded on is installed in a corporate network as depicted in the figure below. The following previously undefined acronyms are used in Figure 5:

- UEFI – Unified Extensible Firmware Interface

[16] RFC – Request for Comments

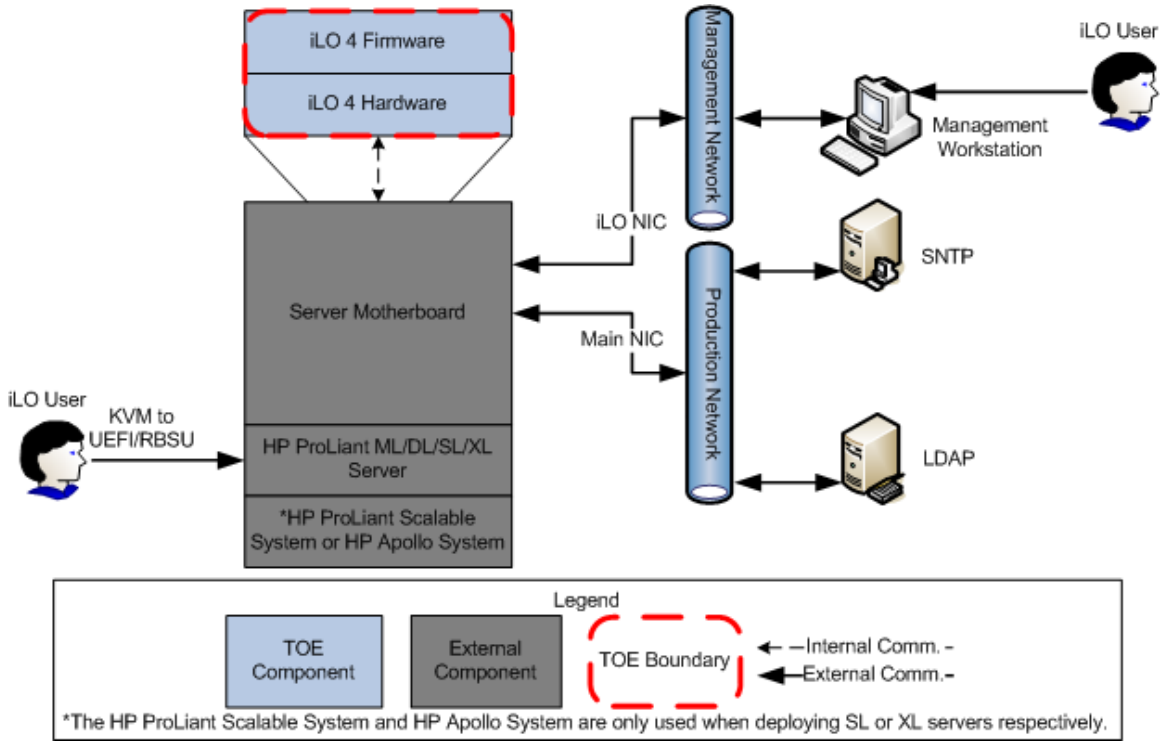

Figure 5 Physical TOE Boundary for Single Server Configuration

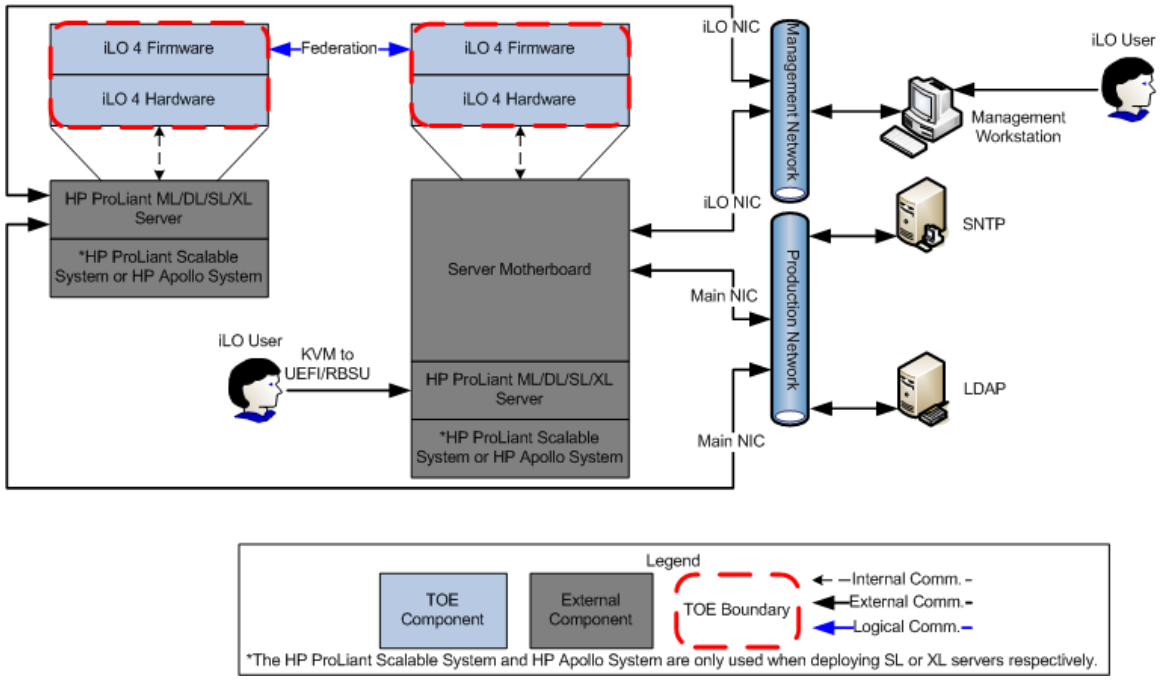

Figure 6 Physical TOE Boundary for Multiple Server Configuration

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- HP iLO 4 Scripting and Command Line Guide; HP Part Number 684919-009; Published: March 2015; Edition: 1
- HP iLO 4 User Guide; HP Part Number 684918-009; Published: March 2015; Edition: 1
- HP iLO 4 Release Notes 2.10; HP Part Number 684917-403; Published: March 2015; Edition: 1
- HP iLO Federation User Guide; HP Part Number 767159-003; Published: March 2015; Edition: 1
- HP Integrated Light-Out (iLO) Quick Specs (Overview); HP Part Number DA-14276; Published: March 2015; Edition: 12
- HP ProLiant Gen8 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 658801-003; Published: November 2013; Edition: 3
- HP ProLiant Gen9 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 795673-001; Published: September 2014; Edition: 1
- Managing HP Servers Using the HP RESTful[17] API[18] for iLO; HP Part Number 795538-002; Published: March 2015; Edition: 1
- Hewlett Packard Enterprise Development LP; Integrated Lights-Out 4 v2.11; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: 1.5

1.5.2 Logical Scope

The logical boundary of the TOE will be described in terms of the functional classes below (which are further described in sections 6 and 7 of this ST). The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the function classes described below.

1.5.2.1 Security Audit

The TOE generates audit records for the startup and shutdown of the audit function, all administrative events, and critical system events and status events. System administrators are associated to the audit events that are generated by their actions. System administrators are able to review all audit records, and the TOE prevents all unauthorized modification and deletion of audit records. While viewing the audit logs, the system administrator is able to apply ascending or descending ordering to the displayed columns. When the audit trail reaches capacity, the oldest records are overwritten with new records.

1.5.2.2 Cryptographic Support

The TOE is a FIPS 140-2-validated cryptographic module that implements the AES, 3DES[19], SHA[20], RSA[21], and DSA[22] algorithms. Any keys that are generated by the TOE will be destroyed using the FIPS 140-2-validated zeroization method provided by the cryptographic module. These cryptographic algorithms are used to secure management traffic between the system administrator and the TOE. Communications sent between the LDAP server and the TOE are also secured using the TOE's cryptographic module.

1.5.2.3 User Data Protection

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the TOE. When the TOE is reset to factory defaults, all authentication information and user-entered device settings are cleared from storage.

1.5.2.4 Identification and Authentication

The TOE will maintain the following list of security attributes belonging to local user accounts: User name, login name, password, and user permissions. The TOE has a minimum password length specified for system administrator authentication. The TOE provides access to the help links on the login page of the web

[17] REST – Representational State Transfer
[18] API – Application Programming Interface
[19] 3DES – Triple Data Encryption Standard
[20] SHA – Secure Hash Algorithm
[21] RSA – Rivest, Shamir, Adleman
[22] DSA – Digital Signature Algorithm

interface; system administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the LDAP server, the TOE is able to identify and authenticate users that use directory services. The TOE obscures the system administrator's password using either a bullet (•) in place of each character or a blank text area during authentication.

1.5.2.5 Security Management

The TOE will restrict access to the security functions based on the system administrator's privilege level. The privilege levels are: Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings.

The TOE will restrict a system administrator's ability to manage TSF[23] data on various objects within the TOE. Access to manage these objects is based on the assigned privilege levels. The TOE allows system administrators to perform the following actions:

- Manage iLO user accounts
- Manage user permissions
- Manage security settings
- Manage access settings
- Manage the system power
- Update the system firmware

A system administrator may have more than one privilege level assigned to them. The TOE is able to associate individual system administrators to these privilege levels. The roles that the TOE maintains (Administrator, Operator, and User) are a combination of the above privilege levels. The LDAP server would manage the groups associated to the privilege levels (or roles) of iLO.

1.5.2.6 Protection of the TSF

The TOE provides reliable timestamps by synchronizing time with an SNTP server. The TOE also implements numerous self-tests to ensure that the cryptographic functionality of the TOE is functioning correctly.

1.5.2.7 TOE Access

Inactive administrative sessions can be terminated by the TOE after a configurable time interval of system administrator inactivity. The TOE can be configured to display a configurable logon "banner" that causes a message to be displayed for every system administrator attempting to authenticate to the TOE's administrative interfaces. The TOE will enforce an incremented login delay between failed login attempts.

1.5.2.8 Trusted Path/Channel

The TOE provides a trusted channel between itself and the LDAP server by making secure connections over TLS. Only the TOE is allowed to initiate these secure channel communications. The TOE will use LDAPS[24] for communications with the LDAP server during user authentication.

A system administrator can initiate a secure connection to the TOE over an HTTPS[25] connection using TLS for use with the iLO Web GUI, iLO REST API, and iLO XML Scripting Interface, and also over an SSH connection for use with the iLO CLI. The HTTPS and SSH connections protect data communications from modification or disclosure, and ensures end point identification. A secure connection is required for initial authentication and all TSF management functions performed through these interfaces.

[23] TSF – TOE Security Functionality
[24] LDAPS – Lightweight Directory Access Protocol Secure
[25] HTTPS – Hypertext Transport Protocol Secure

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and/or functionality that are not part of the evaluated configuration of the TOE are:

- All SNMP functionality
- Remote CLI via Telnet session
- XML Reply
- iLO "System Maintenance Switch"
- HP ProLiant DL/ML/SL/XL server operating systems
- HP Online Configuration Utility (HPONCFG)
- HP Systems Management agent/driver
- Connecting to an HP IRS device using HP Insight Online
- iLO iOS[26] application
- iLO Android application

[26] iOS – iDevice Operating System

2 Conformance Claims

Table 5 identifies all CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 5 CC and PP Conformance

CC Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[27] as of 2015/07/28 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
EAL	EAL2+ with Flaw Remediation (ALC_FLR.2)

[27] CEM – Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains:

- All known and presumed threats countered by either the TOE or by the security environment
- All organizational security policies with which the TOE must comply
- All assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 6 below lists the applicable threats.

Table 6 Threats

Name	Description
T.ACCESS	A non-system administrator may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.
T.CONFIG	An unauthorized user or attacker, who is not a system administrator, could improperly gain access to TSF data if the product is misconfigured or does not enforce proper roles and permissions.
T.MASQUERADE	An unauthorized user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	An unauthorized user or attacker may gain access to security data stored on the TOE, even though the user is not authorized in accordance with the TOE security policy.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 7 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 7 Organizational Security Policies

Name	Description
P.MANAGE	The TOE may only be managed by authorized system administrators.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 8 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 8 Assumptions

Name	Description
A.LOCATE	The TOE is located within a controlled access facility.
A.NOEVIL	There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. The individuals are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE will be protected from unauthorized modification.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 9 below.

Table 9 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must provide protected communication channels for system administrators and authorized IT entities for access to and from the TOE.
O.ADMIN	The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that system administrators with the appropriate privileges (and only those system administrators) may exercise such control.
O.AUDIT	The TOE must securely record audit events that include the resulting actions of the security functional policies, the identified system administrator (if applicable), and provide the authorized system administrators with the ability to review the audit trail. When reviewing, the TOE must provide ordering of audit data to the system administrator. The TOE must also protect stored audit records while preserving a history of audit records that overwrites the oldest record once full.
O.AUTHENTICATE	The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 10 below lists the IT security objectives that are to be satisfied by the environment.

Table 10 IT Security Objectives

Name	Description
OE.OS	The operating systems running on the blade servers must be appropriately configured to prevent unauthorized administrative access to the TSF.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 11 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 11 Non-IT Security Objectives

Name	Description
NOE.NOEVIL	Sites deploying the TOE will ensure that system administrators are non-hostile, appropriately trained, and follow all administrator guidance to ensure the system is used securely.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Extended Components

There are no extended SFRs and extended SARs for this TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 12 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_RIP.1	Subset residual information protection	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.7	Protected authentication feedback		✓		

Name	Description	S	A	R	I
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_STM.1	Reliable time stamps				
FPT_TST.1	TSF testing	✓	✓		
FTA_SSL.3	TSF-initiated termination		✓		
FTA_TAB.1	Default TOE access banners				
FTA_TSE.1	TOE session establishment		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*all administrative actions taken on the iLO interfaces; critical system events and status*].
FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

FAU_GEN.2 User identity association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification
FAU_GEN.2.1
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_SAR.1.1
The TSF shall provide [*authorized system administrators*] with the capability to read [*all audit information*] from the audit records.
FAU_SAR.1.2
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review
FAU_SAR.3.1
The TSF shall provide the ability to apply [*ordering in ascending or descending*] of audit data based on [

- *ID*[28]
- *Severity*
- *Class*
- *Last Update*
- *Initial Update*
- *Count*
- *Description*].

FAU_STG.1 Protected audit trail storage

[28] ID – Identification

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1

The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*listed in the 'Algorithm' column of Table 13*] and specified cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 13*] that meet the following: [*FIPS 197, FIPS 46-3, FIPS 180-3, and FIPS 186-3*].

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*the operation in the 'Cryptographic Operation' column of Table 13*] in accordance with a specified cryptographic algorithm [*listed in the 'Algorithm' column of Table 13*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 13*] that meet the following: [*FIPS 140-2*].

Table 13 Cryptographic Algorithm and Key Sizes for iLO

Cryptographic Operation	Algorithm	Key Sizes (bits)	Certificate No.
Encryption/Decryption	AES – CBC[29] and ECB[30] mode	128, 192, 256	3400
Encryption/Decryption	AES – OFB[31] mode	128	3398, 3399, 3401
Encryption/ Decryption/ Generation/ Verification	AES – GCM[32] mode	128, 192, 256	3400
Encryption/Decryption	3DES – CBC and ECB mode	(3) 56	1924
Key Generation	RSA	2048, 3072	1740
Key Generation	DSA	2048, 3072	959
Signature Generation	RSA	2048, 3072	1740
Signature Generation	DSA	2048, 3072	959

[29] CBC – Cipher Block Chaining
[30] ECB – Electronic Codebook
[31] OFB – Output Feedback
[32] GCM – Galois/Counter Mode

Cryptographic Operation	Algorithm	Key Sizes (bits)	Certificate No.
Signature Verification	RSA	1024, 1536, 2048, 3072, 4096	1740
Signature Verification	DSA	2048, 3072	959
Public Key Generation/ Public Key Verification/ Signature Generation/ Signature Verification	ECDSA[33] for P-256 and P-384 curves	256, 384	676
Message Digest	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	2814
Message Authentication	HMAC[34]-SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	2169
Random Number Generation	CTR[35] DRBG[36] (with AES 128-bit)	N/A[37]	814

[33] ECDSA – Elliptical Curve Digital Signature Algorithm
[34] HMAC – Hash-based Message Authentication Code
[35] CTR – Counter Mode
[36] DRBG – Deterministic Random Bit Generator
[37] N/A – Not Applicable

6.2.3 Class FDP: User Data Protection

FDP_RIP.1 Subset residual information protection
Hierarchical to: No other components.
Dependencies: No dependencies
FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*Authentication information and settings*].

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [

- *User name*
- *Login name*
- *Password*
- *User permissions*].

Application Note: The User permissions attribute is a list of assigned privilege levels used it to control access to TOE features. The privilege levels include Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings.

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [*a configurable character length with a minimum of 8 characters and a maximum of 39 characters*].

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1
The TSF shall allow [*the use of the help link on the TOE's web interface login page (depicted as a question mark "?" in a box)*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1
The TSF shall provide only [*bullets (•), or a blank text area, for a password*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UID.1.1
The TSF shall allow [*the use of the help link on the TOE's web interface login page (depicted as a question mark "?" in a box)*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [*listed in the 'Security Functions' column of Table 14*] to [*the privilege levels listed under the 'Privilege Level' column of Table 14*].

Table 14 Management of Security Functions Behavior

Security Functions	Privilege Level	Permissions
User Accounts	Administer User Accounts	Determine the behavior of, disable, enable, or modify the behavior of
Server boot order	Virtual Media and Configure iLO Settings	Modify the behavior of
System Power Restore Settings	Configure iLO Settings	Modify the behavior of
IPv4/IPv6 Settings	Configure iLO Settings	Determine the behavior of, disable, enable, or modify the behavior of
Authentication methods	Configure iLO Settings	Determine the behavior of, disable, enable, or modify the behavior of
Directory Service Settings	Configure iLO Settings	Determine the behavior of, disable, enable, or modify the behavior of
Port Settings	Configure iLO Settings	Disable, enable, or modify the behavior of
Idle Timeout	Configure iLO Settings	Modify the behavior of
Require Login for iLO RBSU	Configure iLO Settings	Disable or enable
Serial CLI Settings	Configure iLO Settings	Disable, enable, or modify the behavior of
Security Login Banner	Configure iLO Settings	Disable, enable, or modify the behavior of
SNMP Settings	Configure iLO Settings	Determine the behavior of, disable, enable, or modify the behavior of

***Application Note**: The roles of Administrator, Operator, and User are made of a combination of the privilege levels listed in Table 14 above as stated below:*

- ***Administrator** – An Administrator has all listed privileges.*
- ***Operator** – An Operator has the following privilege levels: Remote Console Access, Virtual Power and Reset, and Virtual Media. Also, an Operator can have any combination of privilege levels greater than the previous statement but less than an Administrator's list of privileges.*
- ***User** – A User can have no privileges or any combination of privilege levels that are less than the Operator's list of privileges.*

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [[*the list of operations listed in the 'Operations' column of Table 15 to*]] the [*objects listed in the 'Objects' column of Table 15*] to [*the privilege levels listed under the 'Privilege Level' column of Table 15*].

Table 15 Management of TSF Data

Menu	Object	Privilege Level	Operations
Information	Overview	Everyone[38]	View
	System Information	Everyone	View
	iLO Event Log	Configure iLO Settings	Clear event logs
		Everyone	View
	Integrated Management Log	Configure iLO Settings	Mark as repaired, add maintenance notes, and clear event logs
		Everyone	View
	Active Health System Log	Configure iLO Settings	Enable/disable logging, and clear event logs
		Everyone	View
	Diagnostics	Configure iLO Settings	Reset iLO
		Virtual Power and Reset	Generate NMI[39] and swap the ROM
		Everyone	View
	Insight Agent	Everyone	View, and launch Insight Agent
iLO Federation	Multi-System View	Everyone	View, and Filter
	Multi-System Map	Everyone	View
	Group Virtual Media	Virtual Media	Manage media
		Everyone	View
	Group Power	Virtual Power and Reset	Use power buttons
		Everyone	View
	Group Power Settings	Configure iLO Settings	Manage
		Everyone	View
	Group Firmware Update	Configure iLO Settings	Update firmware
		Everyone	View
	Group Licensing	Configure iLO Settings	Update license
		Everyone	View

[38] Note that "Everyone" is not a role or privilege level. It refers to all roles and privilege levels managed by the TOE.
[39] NMI – Non-Maskable Interrupt

Menu	Object	Privilege Level	Operations
	Group Configuration	Configure iLO Settings	View, and Manage
Remote Console	Remote Console	Remote Console Access	Launch iLO Java Integrated Remote Console (JIRC) and iLO .NET Integrated Remote Console (NIRC)
		Configure iLO Settings	Reset and save hot key settings
		Everyone	View
Virtual Media	Virtual Media	Virtual Media	Use, eject, and insert media
		Virtual Power and Reset	Reset the server
		Configure iLO Settings	Manage
		Everyone	View
	Boot Order	Virtual Media and Configure iLO Settings	Manage (requires both privilege levels)
		Virtual Power and Reset	Reset the server
		Everyone	View
Power Management	Server Power	Configure iLO Settings	Manage
		Virtual Power and Reset	Use virtual power buttons
		Everyone	View
	Power Meter	Everyone	View
	Power Settings	Configure iLO Settings	Manage
		Everyone	View
Network	iLO Dedicated Network Port	Configure iLO Settings	Manage
		Everyone	View
Remote Support	Registration	Configure iLO Settings	Manage
		Everyone	View
	Service Events	Configure iLO Settings	Manage
		Everyone	View
	Data Collections	Configure iLO Settings	Manage
		Everyone	View
Administration	Firmware	Configure iLO Settings	Manage
		Everyone	View
	Licensing	Configure iLO Settings	Manage
		Everyone	View
	User Administration	Configure iLO Settings	Manage directory groups
		Administer User Accounts	Manage users
		Everyone	View, change personal password

Menu	Object	Privilege Level	Operations
	Access Settings	Configure iLO Settings	Manage
		Everyone	View
	Security	Administer User Accounts	Manage (only Secure Shell Keys)
		Configure iLO Settings	Manage (all except for Secure Shell Keys)
		Everyone	View
	Management	Configure iLO Settings	Manage
		Everyone	View
	Key Manager	Configure iLO Settings	Manage
		Everyone	View
	iLO Federation	Configure iLO Settings	Manage
		Everyone	View

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No Dependencies
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [

- *Management of iLO user accounts*
- *Management of user permissions*
- *Management of security settings*
- *Management of access settings*
- *Management of system power*
- *Update the system firmware*].

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1.1
The TSF shall maintain the ~~roles~~ **privilege levels** [*Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings*].
FMT_SMR.1.2
The TSF shall be able to associate users with ~~roles~~ **privilege levels**.

***Application Note**: The roles of Administrator, Operator, and User are made of a combination of the privilege levels listed above as stated below:*

- ***Administrator** – An Administrator has all listed privileges.*
- ***Operator** – An Operator has the following privilege levels: Remote Console Access, Virtual Power and Reset, and Virtual Media. Also, an Operator can have any combination of privilege levels greater than the previous statement but less than an Administrator's list of privileges.*
- ***User** – A User can have no privileges or any combination of privilege levels that are less than the Operator's list of privileges.*

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_TST.1.1
The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of [*the FIPS 140-2-validated cryptographic module's cryptographic functionality*].
FPT_TST.1.2
The TSF shall provide authorized users with the capability to verify the integrity of [*the FIPS 140-2-validated cryptographic module*].
FPT_TST.1.3
The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*configurable time interval of system administrator inactivity*].

Application Note: *FTA_SSL.3 is enforced by iLO's CLI, GUI, JIRC, and NIRC. All other external interfaces are excluded from the scope.*

FTA_TAB.1 Default TOE access banners
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application Note: *FTA_TAB.1 is enforced by iLO's GUI only. All other external interfaces are excluded from the scope.*

FTA_TSE.1 TOE session establishment
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [*TSF-enforced login delays between failed login attempts*].

Application Note: *FTA_TSE.1 is enforced by iLO's CLI, REST API, and GUI. All other external interfaces are excluded from the scope.*

6.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies
FTP_ITC.1.1
The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2
The TSF shall permit [the TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [*Authentication with an LDAP server over TLS*].

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies
FTP_TRP.1.1
The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure, [*and no other types of integrity or confidentiality violation*]].
FTP_TRP.1.2
The TSF shall permit [remote users] to initiate communication via the trusted path.
FTP_TRP.1.3
The TSF shall require the use of the trusted path for [initial user authentication, [*and all TSF management functions performed via the iLO Web GUI, CLI, REST API, and XML Scripting Interface*]].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 16 summarizes the requirements.

Table 16 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security function. Hence, each security function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 17 lists the security functions and their associated SFRs.

Table 17 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel

TOE Security Functionality	SFR ID	Description
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generate audit records for the startup and shutdown of their audit functions, all administrative events, critical system events, and status events that should be seen by system administrators. Audit records are stamped with the actual time at which the event occurred and associated to the system administrator that caused it (if applicable). After authenticating to the TOE's web GUI, CLI, or XML Scripting Interface, system administrators are able to review all audit records. The TOE also prevents unauthorized deletion or modification of the audit records. During the review of audit records through the TOE's web GUI, the system administrator may apply ordering to the Fields listed in Table 18 in ascending or descending order. When the audit trail reaches capacity, the oldest records are overwritten with new records.

The TOE audit records contain the following information listed in Table 18:

Table 18 Audit Record Contents

Field	Content
ID	The event ID number. Events are numbered in the order in which they are generated. By default, the Event Log is sorted by the ID, with the most recent event at the top.
Severity	The importance of the detected event. Possible values follow: • **Informational** – The event provides background information. • **Caution** – The event is significant but does not indicate performance degradation. • **Critical** – The event indicates a service loss or imminent service loss. Immediate attention is needed.
Class	The component or subsystem that identified the logged event.
Last Update	The date and time, as reported by the server clock, when the latest event of this type occurred. This value is based on the date and time stored by iLO.
Initial Update	The date and time, as reported by the server clock, when the first event of this type occurred. This value is based on the date and time stored by iLO.
Count	The number of times this event has occurred (if supported).
Description	The description identifies the component and detailed characteristics of the recorded event.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, and FAU_STG.4.

7.1.2 Cryptographic Support

The TOE implements a FIPS 140-2 validated cryptographic module that implement the algorithms listed in 6.2.2. These cryptographic algorithms are used to secure management traffic between the system administrators and the TOE. The iLO Web GUI and XML Scripting Interface are protected via the TLS protocol. The iLO CLI is protected via the SSH protocol. The TOE also uses TLS to protect communications when connecting to the LDAP server. The cryptographic module will generate and zeroize cryptographic keys in a FIPS 140-2 validated manner.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, and FCS_COP.1.

7.1.3 User Data Protection

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the TOE. Any previous authentication information and settings for each iLO managed server is deallocated and made unavailable when an authorized system administrator triggers an iLO reset to factory defaults.

TOE Security Functional Requirements Satisfied: FDP_RIP.1.

7.1.4 Identification and Authentication

The TOE will maintain the following security attributes for each local account that is created: user name, login name, password, and user permissions. The user permissions attribute is a list of assigned privilege levels used it to control access to TOE features. The privilege levels include Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings. System administrators can configure the TOE to require passwords of a minimum character length. The TOE provides access to the help link of the TOE's web interface. The web interface's login page provides a link to help about logging iLO into (depicted as a question mark "?" in a box). System administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the LDAP server, the TOE is able to identify and authenticate users that use directory services. Also, the TOE obscures the system administrator's password using either a bullet (•) in place of each character or displaying a blank text area during authentication.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, and FIA_UID.1.

7.1.5 Security Management

The TOE will restrict access to the security functions listed in Table 14. The system administrator's privilege level determines which security functions they have access to. The privilege levels include: Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings.

The TOE will restrict a system administrator's ability to manage TSF data on various objects within the TOE. Access to manage these objects is based on the assigned privilege levels. Please see Table 15 for the access control mapping. The TOE allows system administrators to manage the following:

- iLO user accounts
- User permissions
- Security settings
- Access settings
- System power
- System firmware

A system administrator may have more than one privilege level assigned to them. The TOE maintains several privilege levels: Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings. The TOE is able to associate individual system administrators to these privilege levels. The LDAP server would manage the groups associated to the privilege levels (or roles) of iLO. The roles of Administrator, Operator, and User are each a combination of the privilege levels as stated below:

- **Administrator** – An Administrator has all listed privileges.
- **Operator** – An Operator has the following privilege levels: Remote Console Access, Virtual Power and Reset, and Virtual Media. Also, an Operator can have any combination of privilege levels greater than the previous statement but less than an Administrator's list of privileges.

- **User** – A User can have no privileges or any combination of privilege levels that are less than the Operator's list of privileges.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE will provide reliable timestamps that are used for the audit trail. The TOE's time will be synchronized with an SNTP server in the TOE environment.

The TOE implements numerous self-tests (power-up self-tests, conditional self-tests, and critical self-test) to ensure that the cryptographic functionality of the TOE is functioning correctly. FIPS 140-2-required self-tests are performed during the initial start-up of the TOE on the cryptographic algorithms, and cryptographic module on the whole, to ensure their proper function. During the power-up, the TOE performs the following self-tests: firmware integrity test, Known Answer Tests (KATs) in hardware, and KATs in firmware. Conditional self-tests are performed by the module whenever a new random number is generated or when a new key pair is generated. The TOE performs the following conditional self-tests: continuous random number generator test, pairwise consistency tests, and a firmware load test. Critical self-tests are performed during power-up and conditionally. The TOE performs the following critical self-tests: SP[40] 800-90A CTR_DRBG Instantiate Health Test, SP 800-90A CTR_DRBG Generate Health Test, SP 800-90A CTR_DRBG Reseed Health Test, and SP 800-90A CTR_DRBG Uninstantiate Health Test. An authorized system administrator may verify the integrity of the FIPS 140-2 module and tested code by viewing the system logs within the TOE. If the self-tests pass, the module will start as intended and the TOE will operate correctly. If the self-tests fail, the module will error and not function properly until it is resolved.

TOE Security Functional Requirements Satisfied: FPT_STM.1 and FPT_TST.1.

7.1.7 TOE Access

The TOE will enforce an incremented login delay between failed login attempts on the CLI, REST API, and Web GUI. The TOE will also be configured to display a logon "banner" (a message that is displayed to every system administrator attempting to authenticate to the TOE; specifically on the Web GUI). Inactive sessions will be terminated by the TOE after a configurable time interval of system administrator inactivity for the CLI, Web GUI, JIRC, and NIRC.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_TAB.1, and FTA_TSE.1.

7.1.8 Trusted Path/Channels

The TOE provides a trusted channel between itself to the LDAP server. Only the TOE is allowed to initiate secure communications with the LDAP server. The TOE makes these secure connections over TLS to the LDAP server for use during authentication.

Using a supported browser, a remote system administrator initiates a secure connection to the TOE. The secure path is established using HTTPS for the iLO Web GUI, iLO REST API, and iLO XML Scripting Interface. Using an SSH client, a remote system administrator initiates a secure connection to the iLO CLI over SSH. The HTTPS and SSH connections are used to protect data communications from modification or disclosure, and ensures end point identification. A secure connection is required for authentication and all TSF management functions performed via the iLO Web GUI, CLI, REST API, and XML Scripting Interface.

TOE Security Functional Requirements Satisfied: FTP_ITC.1 and FTP_TRP.1.

[40] SP – Special Publication

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 19 below provides a mapping of the objectives to the threats they counter.

Table 19 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ACCESS A non-system administrator may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.	O.ACCESS The TOE must provide protected communication channels for system administrators and authorized IT entities for access to and from the TOE.	O.ACCESS counters this threat by ensuring that TSF data transmitted over the network is kept secure from modification and disclosure.
T.CONFIG An unauthorized user or attacker, who is not a system administrator, could improperly gain access to TSF data if the product is misconfigured or does not enforce proper roles and permissions.	O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that system administrators with the appropriate privileges (and only those system administrators) may exercise such control.	O.ADMIN ensures that the TOE provides efficient management of its functions and data, mitigating the threat of accidental misconfiguration. O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that the TOE has identified and authenticated a system administrator before they are allowed to access any data.

Threats	Objectives	Rationale
T.MASQUERADE An unauthorized user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that The TOE is able to identify and authenticate system administrators prior to allowing access to TOE administrative functions and data.
T.UNAUTH An unauthorized user or attacker may gain access to security data stored on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.AUDIT The TOE must securely record audit events that include the resulting actions of the security functional policies, the identified system administrator (if applicable), and provide the authorized system administrators with the ability to review the audit trail. When reviewing, the TOE must provide ordering of audit data to the system administrator. The TOE must also protect stored audit records while preserving a history of audit records that overwrites the oldest record once full.	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that system administrators with the appropriate privileges (and only those system administrators) may exercise such control.	O.ADMIN ensures that access to TOE security data is limited to those system administrators with access to the management functions of the TOE.

Threats	Objectives	Rationale
	O.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that system administrators are identified and authenticated prior to gaining access to TOE security data.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 20 below gives a mapping of policies and the objectives that support them.

Table 20 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.MANAGE The TOE may only be managed by authorized system administrators.	O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that system administrators with the appropriate privileges (and only those system administrators) may exercise such control.	O.ADMIN ensures that the TOE provides the necessary tools to support the P.MANAGE policy.
	O.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that only authorized system administrators are granted access to the tools required to manage the TOE.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 21 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 21 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE is located within a controlled access facility.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. NOE.PHYSICAL satisfies this assumption.
A.NOEVIL There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. The individuals are non-hostile, appropriately trained, and follow all guidance.	NOE.NOEVIL Sites deploying the TOE will ensure that system administrators are non-hostile, appropriately trained, and follow all administrator guidance to ensure the system is used securely.	NOE.NOEVIL upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all administrator guidance.
	OE.OS The operating systems running on the servers must be appropriately configured to prevent unauthorized administrative access to the TSF.	OE.OS ensures that the operating systems external to the TOE which may have direct access to TOE hardware are properly hardened to prevent unauthorized access.
A.PROTECT The TOE will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL ensures that the TOE's IT environment protects the TOE from interference and tampering by untrusted subjects.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended functional requirements defined for this TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 22 below shows a mapping of the objectives and the SFRs that support them.

Table 22 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must provide protected communication channels for system administrators and authorized IT entities for access to and from the TOE.	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by ensuring that the TOE will provide a secure communications channel with trusted IT products in the environment.
	FTP_TRP.1 Trusted path	The requirement meets the objective by ensuring that the TOE will provide a secure communications path when communicating with a system administrator.
O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that system administrators with the appropriate privileges (and only those system administrators) may exercise such control.	FCS_CKM.1 Cryptographic key generation	The requirement meets this objective by ensuring that the TOE uses secure cryptographic algorithms to protect management traffic.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets this objective by ensuring that the TOE zeroizes cryptographic keys to prevent their compromise.
	FCS_COP.1 Cryptographic operation	The requirement meets this objective by ensuring that the TOE performs cryptographic operations in accordance with the FIPS 140-2 standard.
	FDP_RIP.1 Subset residual information protection	The requirement meets this objective by ensuring that the TOE deallocates resources from cryptographic keys, authentication information, and settings when the TOE is reset to factory defaults.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only system administrators with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the system administrator's privileges.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates system administrators with privilege levels to provide access to TSF management functions and data.
	FPT_TST.1 TSF testing	The requirement meets the objective by ensuring that FIPS 140-2-validated self-tests will be performed by the cryptographic module.
O.AUDIT The TOE must securely record audit events that include the resulting actions of the security functional policies, the identified system administrator (if applicable), and provide the authorized system administrators with the ability to review the audit trail. When reviewing, the TOE must provide ordering of audit data to the system administrator. The TOE must also protect stored audit records while preserving a history of audit records that overwrites the oldest record once full.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the events, for the HP iLO interfaces.
	FAU_GEN.2 User Identity Association	The requirement meets this objective by ensuring that the TOE associates the user name to an audit event for any system administrator that causes the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.

Objective	Requirements Addressing the Objective	Rationale
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that the TOE provides the ability to order audit events in ascending or descending order for each column in the event log.
	FAU_STG.1 Protected audit trail storage	The requirement meets this objective by preventing arbitrary modification of the audit trail.
	FAU_STG.4 Prevention of audit data loss	The requirement meets this objective by overwriting the oldest stored audit records once the audit trail is full.
	FPT_STM.1 Reliable time stamps	The TOE provides reliable timestamps for its own use.
O.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must obscure passwords, display a logon banner to system administrators prior to their access of the system, handle idle sessions, and failed login attempts in a secure manner.	FIA_ATD.1 User attribute definition	The requirement meets this objective by ensuring that they TOE maintains user attributes used to authenticate the system administrator.
	FIA_SOS.1 Verification of secrets	The requirement meets this objective by ensuring that the system administrators' passwords are of sufficient length.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that system administrators are authenticated before access to TOE functions is allowed.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that passwords are obscured during the login process of the TOE.
	FIA_UID.1 Timing of identification	The requirement meets the objective by ensuring that system administrators are identified before access to TOE functions is allowed.
	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing access to administrative functions to ensure that only appropriately privileged system administrators may manage the security behavior of the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized system administrators are allowed access to manipulate security attributes and applications.
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that sessions are terminated after a configurable time interval of inactivity.
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that administrators can configure an advisory warning message which will be displayed on the management interfaces when a system administrator attempts to authenticate.
	FTA_TSE.1 TOE session establishment	The requirement meets the objective by ensuring that the TOE will increase a delay between each successive failed login attempt on the management interfaces.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor, assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 23 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 23 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_RIP.1	No dependencies	✓	
FIA_ATD.1	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	No dependencies	✓	
FPT_TST.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
FTA_TSE.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

9 Acronyms

This section and Table 24 define the acronyms used throughout this document.

Table 24 Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AHS	Active Health System
API	Application Programming Interface
ASIC	Application Specific Integrated Circuits
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CLI	Command Line Interface
CPU	Central Processing Unit
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
ECDSA	Elliptical Curve Digital Signature Algorithm
ERS	Embedded Remote Support
ESR	Extended Support Release
FIPS	Federal Information Processing Standard
GB	Gigabyte
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HPONCFG	HP Online Configuration Utility
HTTPS	Hypertext Transport Protocol Secure
ID	Identification
iLO	Integrated Lights-Out

Acronym	Definition
iOS	iDevice Operating System
IP	Internet Protocol
IRS	Insight Remote Support
IT	Information Technology
KAT	Known Answer Test
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
N/A	Not Applicable
NAND	Negated AND
NIC	Network Interface Card
NMI	Non-Maskable Interrupt
OFB	Output Feedback
ORCA	Option ROM Configuration for Arrays
OS	Operating System
OSP	Organizational Security Policy
POST	Power-on Self Test
PP	Protection Profile
RBSU	ROM-Based Setup Utility
RC4	Rivest Cipher 4
REST	Representational State Transfer
RFC	Request for Comments
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SD	Secure Digital
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Special Publication
SSH	Secure Shell

Acronym	Definition
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface
XML	eXtensible Markup Language

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com