Hewlett Packard Enterprise Development LP

Integrated Lights-Out 5 v1.11

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.9

Prepared for:

Hewlett Packard Enterprise

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

Phone: +1 281 370 0670
www.hpe.com

Prepared by:

Corsec

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

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Figures

List of Tables

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Hewlett Packard Enterprise Development LP (HPE) Integrated Lights-Out 5 v1.11 (iLO 5) with an iLO Advanced Premium Security Edition license, and it will hereafter be referred to as the TOE throughout this document. The TOE is a standard component of HPE ProLiant Gen10 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 Purpose

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 (PP), and Evaluation Assurance Level (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 to which the TOE adheres.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs 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 and terminology 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 5 v1.11 Security Target
ST Version	Version 0.9
ST Author	Corsec Security, Inc.
ST Publication Date	February 12, 2018

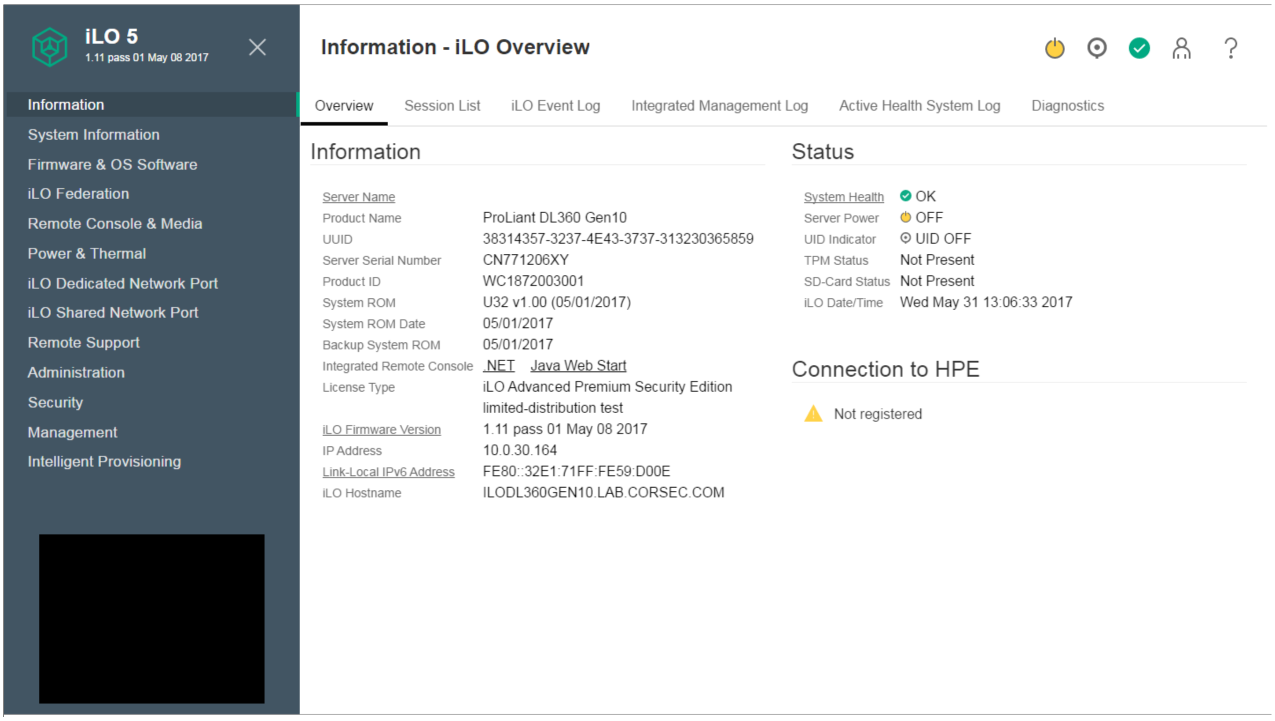
©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Reference	HPE Integrated Lights-Out 5 v1.11 on the GXP Application Specific Integrated Circuits (ASIC) with an iLO Advanced Premium Security Edition license
FIPS[1] 140-2 Status	Level 1, Validated crypto module, Certificate No. 3122

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The HPE Integrated Lights-Out 5 (HPE iLO 5) built into HPE ProLiant Gen10 servers is an autonomous secure management component embedded directly on the server motherboard. iLO helps simplify initial server setup, power optimization, thermal optimization, and remote server administration. It also provides server health monitoring with the HPE Active Health System (AHS) and 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 Gen10 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 HPE 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.



[redacted]

Information - iLO Overview

Information

Server Name	
Product Name	ProLiant DL360 Gen10
UUID	38314357-3237-4E43-3737-313230365859
Server Serial Number	CN771206XY
Product ID	WC1872003001
System ROM	U32 v1.00 (05/01/2017)
System ROM Date	05/01/2017
Backup System ROM	05/01/2017
Integrated Remote Console	.NET Java Web Start
License Type	iLO Advanced Premium Security Edition limited-distribution test
iLO Firmware Version	1.11 pass 01 May 08 2017
IP Address	10.0.30.164
Link-Local IPv6 Address	FE80::32E1:71FF:FE59:D00E
iLO Hostname	ILODL360GEN10.LAB.CORSEC.COM

Status

System Health	✓ OK
Server Power	OFF
UID Indicator	UID OFF
TPM Status	Not Present
SD-Card Status	Not Present
iLO Date/Time	Wed May 31 13:06:33 2017

Connection to HPE

⚠ Not registered

Figure 1 – HPE iLO (Example Management Screen)

[1] FIPS – Federal Information Processing Standard
[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

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

iLO 5 is supported on the following server platforms:

- HPE ProLiant Gen10 DL Rack Servers
- HPE ProLiant Gen10 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. 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 HPE 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 and works with the server to enable remote network booting through a variety of methods. It also allows control over the server's power and hardware reset functionality. 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 method for accessing iLO functionality is mediated by the iLO Web GUI. Using iLO Federation Management, a system administrator may manage multiple servers from one system running the iLO Web 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 HPE 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 HPE AHS does not collect information about operations, finances, customers, employees, partners, or the 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 HPE 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]. HPE ProLiant Gen10 servers with a 4GB[7] iLO NAND allow system administrators

[4] IT – Information Technology
[5] BIOS – Basic Input/Output System
[6] NAND – Negated AND
[7] GB – Gigabyte

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

to store a copy of the certified firmware image for disaster recovery purposes. If the active firmware image becomes corrupt, iLO will apply the stored recovery image over the corrupted image to restore functionality to the device. No settings are lost during this process, and it is performed automatically without intervention from the system administrator as long as the stored image is valid.

iLO provides a USB service port on the front panel of the Gen10 servers (excluding the XL230K). The intent of the USB service port is to allow support personnel to connect a USB to Ethernet device to it for accessing iLO's management interfaces from a local laptop. With physical access to the server, the support personnel can connect to iLO without having to connect to the corporate network while still having the same access to the management interfaces. While this does not require access to the network, it does require a valid username and password to login to iLO. While using the iLO USB service port with an Ethernet adaptor, the same security rules of the management network connect apply. The iLO USB service port has no access to the host server and cannot be accessed from the host server. If an unsupported device is plugged in, a message is logged to the iLO event log indicating the device is unsupported.

iLO Advanced Premium Security Edition features 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 – iLO Advanced Premium Security Edition Features

Feature	iLO Advanced Premium Security Edition
Virtual Keyboard, Video, Mouse (KVM[8])	Full text and graphic modes (pre-OS[9] & OS)
Global Team Collaboration (Virtual KVM)	Up to 6 Server Administrators
Console Record and Replay	✓
Virtual Power	✓
Virtual Media	✓
Virtual Folders	✓
Remote Serial Console	SSH[10] Only
Virtual Unit Indicator Display	✓
Email-based Alerting	✓
Drive Key Managers (i.e. ESKM[11])	✓
ROM[12]-Based Setup Utility (RBSU)	✓
Present Power Reading	✓
Power Usage Reporting	✓
Ambient Temperature Reporting	✓
Dynamic Power Capping	✓

[8] KVM – Keyboard, Video, Mouse
[9] OS – Operating System
[10] SSH – Secure Shell
[11] ESKM – Enterprise Secure Key Manager
[12] ROM – Read-Only Memory

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Feature	iLO Advanced Premium Security Edition
Power Supply High-Efficiency Mode	✓
Sea of Sensors	✓
Power-On Self-Test (POST) and Failure Sequence Replay	✓
iLO and Server Integrated Management Log	✓
Advanced Server Management	✓
Alert Administrator (SNMP Pass through)	✓
System Health & Configuration Display	✓
Directory Services Authentication	✓
Locally Stored Accounts	✓
Smartcard (CAC[13]/PIV[14]) Authentication	✓
Browser	✓
Command Line	✓
Extensible Markup Language (XML)/Perl Scripting	✓
Integrated Remote Console for Windows Clients	✓
Java Applet Client for Windows and Linux Clients	✓
RESTful[15] scripting	✓
Transport Layer Security (TLS)	✓
Secure Shell	✓
AES[16] (Virtual KVM)	✓
Dedicated Network Interface Controller (NIC)	✓
Shared Network Port	✓
iLO Federation Discovery	✓
iLO Federation Discovery Group License Activation	✓
iLO Federation Management	✓
Scan iLO and BIOS for malware	✓
High security modes (HIGH SECURITY, FIPS and CNSA[17])	✓

1.4 TOE Overview

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

[13] CAC – Common Access Card
[14] PIV – Personal Identification Verification
[15] REST – Representational State Transfer
[16] AES – Advanced Encryption Standard
[17] CNSA – Commercial National Security Algorithm

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

HPE Integrated Lights-Out 5 v1.11 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 server health monitoring, Active Health System log access, Federation management, virtual media control, server power control, and secure remote access to the server. iLO is integrated into HPE ProLiant Gen10 DL or XL server. The TOE functions independently of the server's state of operation by obtaining its power directly 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. The TOE provides the ability to store a recovery image on the internal NAND. This image will be used to recover from a fatal error in the active firmware, which happens automatically if an issue is detected by the TOE. Multiple forms of authentication are provided by the TOE and can be utilized by the system administrator as needed. The different forms of authentication include the use of LDAP[18], Kerberos, smartcards (including CACs and PIV cards), and local iLO accounts. HPE iLO 5 will be tested on the HPE ProLiant Gen10 DL and XL servers. Figure 2 below depicts the HPE iLO Component.

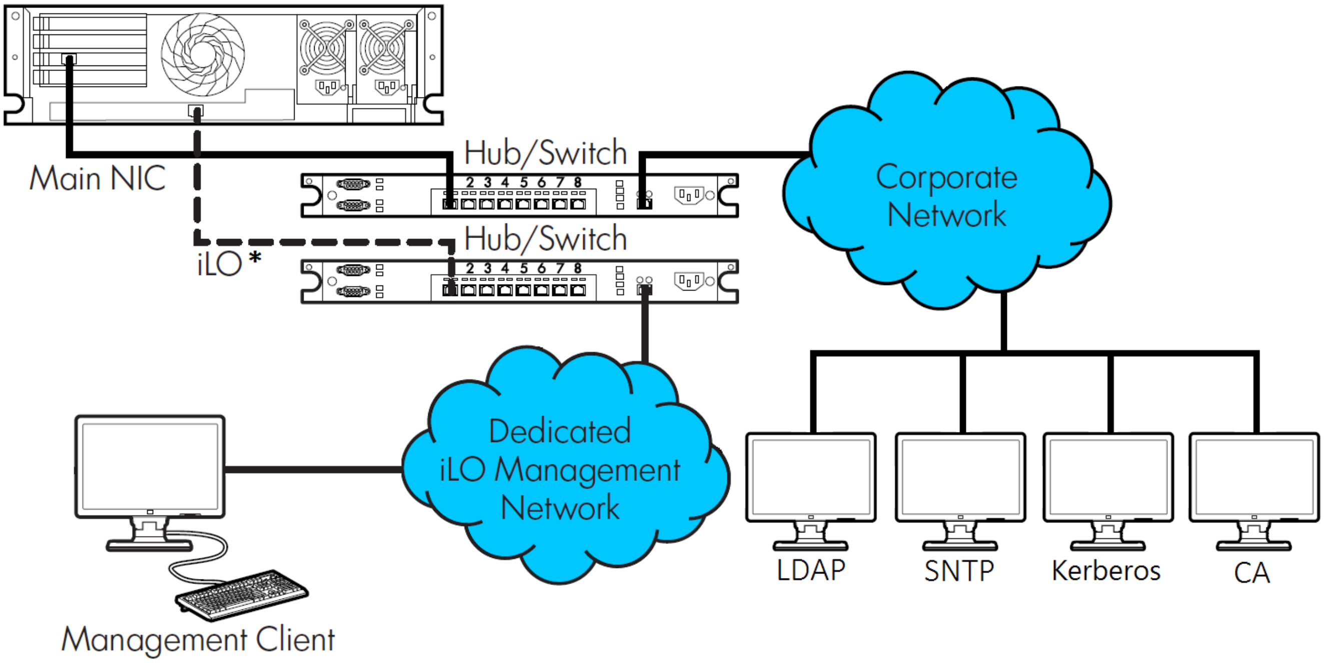
Figure 2 – HPE iLO Component

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

- CA – Certificate Authority
- SNTP – Simple Network Time Protocol

[18] LDAP – Lightweight Directory Access Protocol

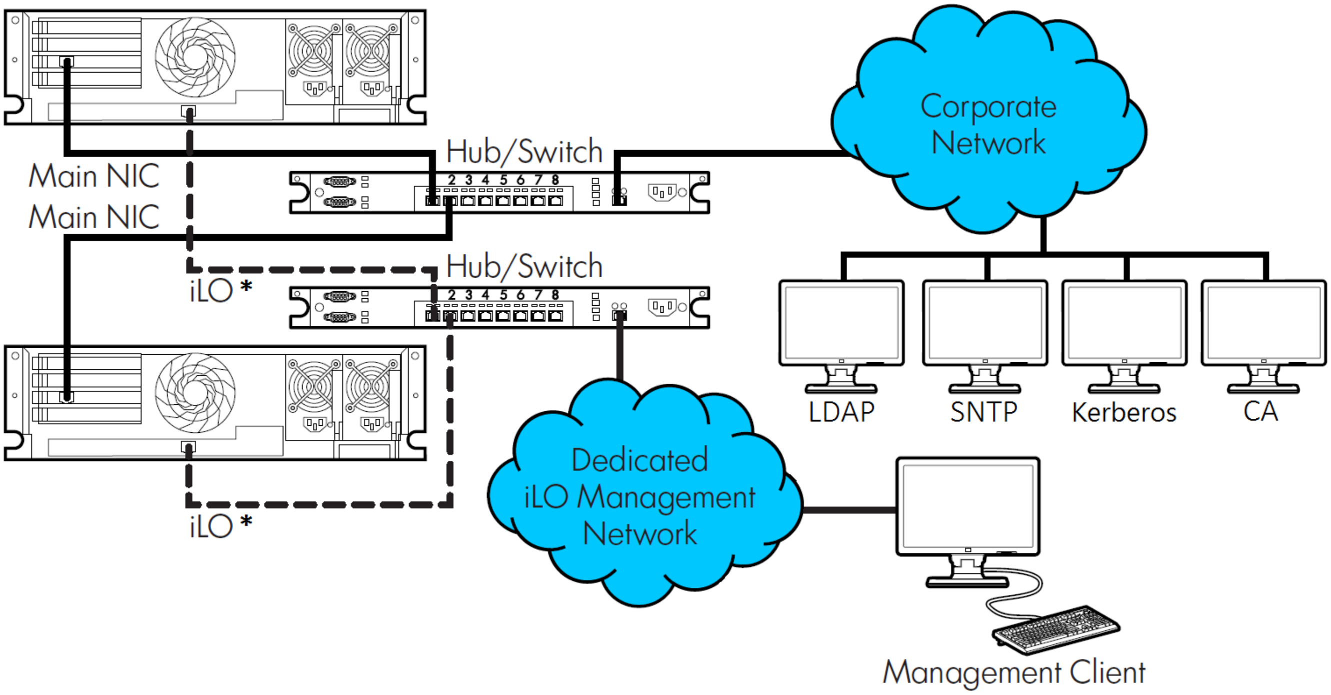
©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.



*A dotted line is used to represent the iLO connection as it crosses the Main NIC connection

Figure 3 – Single Server Deployment Configuration of the TOE

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



*A dotted line is used to represent the iLO connection as it crosses the Main NIC connection

Figure 4 – Multiple Server Deployment Configuration of the TOE

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 HPE ProLiant Gen10 DL 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. A card reader will be required on any workstation attempting to authenticate using smartcard authentication. A smartcard (generic smartcard, CAC, or PIV card) must also be provided to the system administrator if they choose to use the smartcard authentication method. The following third-party software is required when interfacing with the TOE:

- Java Runtime Environment – Minimum version of 8 Update 121; the latest version is recommended
- Microsoft .NET Framework – Minimum version of the 3.5; version 4.6 is recommended
- The following web browsers are supported:
  - Microsoft Internet Explorer 11.x
  - Microsoft Edge (latest version)
  - Mozilla Firefox (latest version)
  - 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

Component	Requirements
HPE iLO 5 Firmware	Version 1.11
HPE iLO 5 Hardware	GXP ASIC Model number 815393-001-B1
HPE iLO 5 License	iLO Advanced Premium Security Edition license
HPE iLO 5 Host	The HPE iLO 5 hardware is contained within the host server and cannot function independently. At least one of the following hosts is required: • HPE ProLiant Gen10 DL360 Rack Server • HPE ProLiant Gen10 DL380 Rack Server • HPE ProLiant Gen10 DL560 Rack Server • HPE ProLiant Gen10 XL230K Scalable Server

Table 4 specifies the minimum components for the TOE environment.

Table 4 – TOE Environment

Device	Requirements
HPE ProLiant Server (TOE host)	At least one of the following servers, two for the multiple server configuration: • HPE ProLiant Gen10 DL360 Rack Server • HPE ProLiant Gen10 DL380 Rack Server • HPE ProLiant Gen10 DL560 Rack Server • HPE ProLiant Gen10 XL230K Scalable Server

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Device	Requirements
XL230K Servers Only	HPE Apollo 6000 System
LDAP Server	LDAPv3 (RFC[19] 4511)
CA Server	X.509 Public Key Infrastructure with a CRL[20] (RFC 5280 and RFC 4158)
SNTP Server	SNTPv4 (RFC 5905)
Kerberos Server	Kerberos Network Authentication Service version 5 (RFC 4120)

The LDAP server is used for authenticating and identifying system administrators to assign their required roles. Communications for the LDAP server are sent over TLS. A CA server is used to maintain the CRL for certificate revocation used in smartcard authentication. An SNTP server is used by the TOE to synchronize the internal clock with a reliable time source. The Kerberos server is used for authenticating and identifying system administrators similarly to the LDAP server. Communications with the Kerberos server are sent using AES encryption for Kerberos version 5. The HPE Apollo System is used as a midplane for the XL230K servers that it hosts. It does 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 tie 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 HPE ProLiant servers listed in Table 3. The HPE ProLiant server that the TOE is embedded on is installed in a corporate network as depicted in the figures below. The following previously undefined acronyms are used in Figure 5:

- UEFI – Unified Extensible Firmware Interface
- USB – Universal Serial Bus

[19] RFC – Request for Comments

[20] CRL – Certificate Revocation List

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

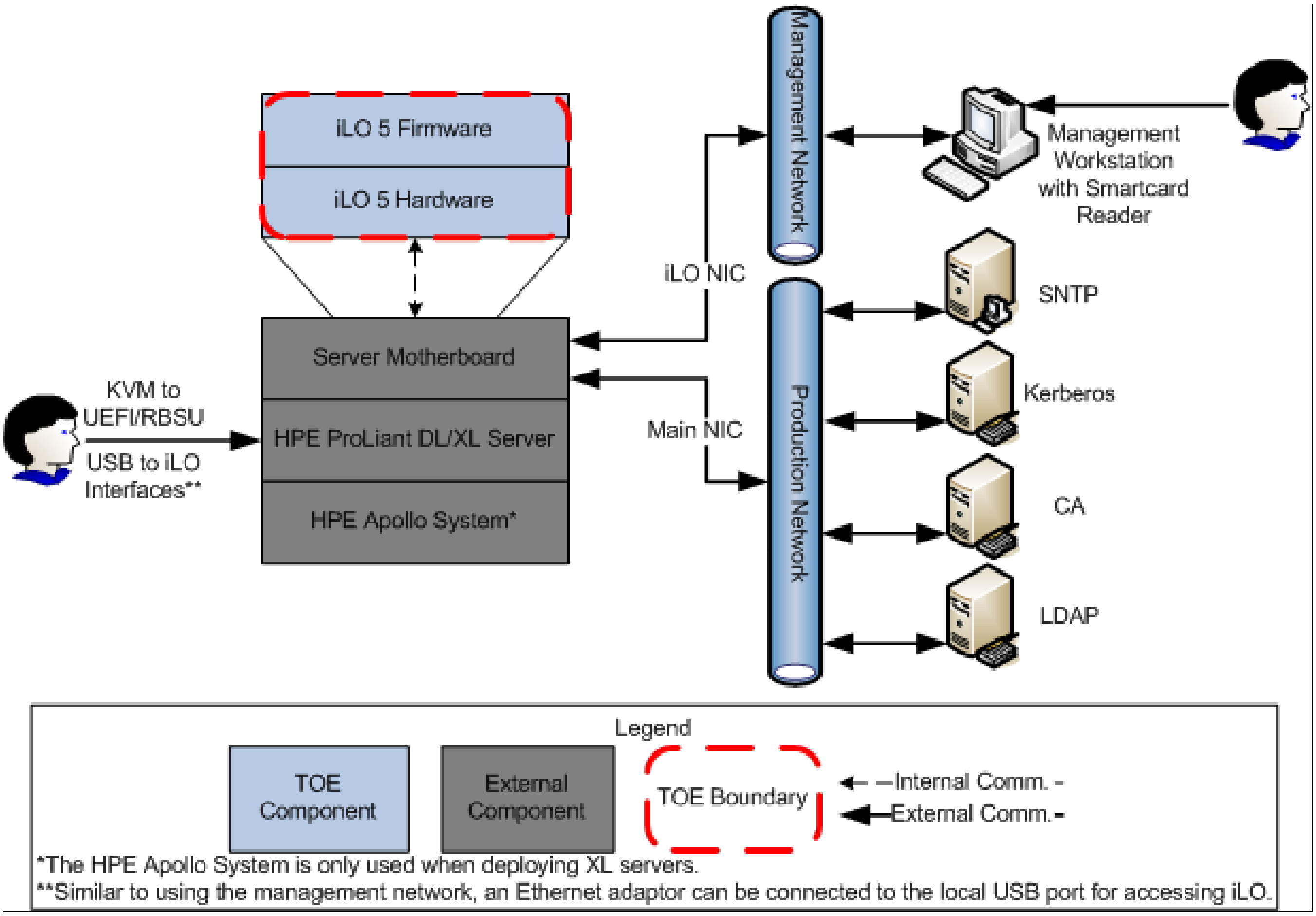
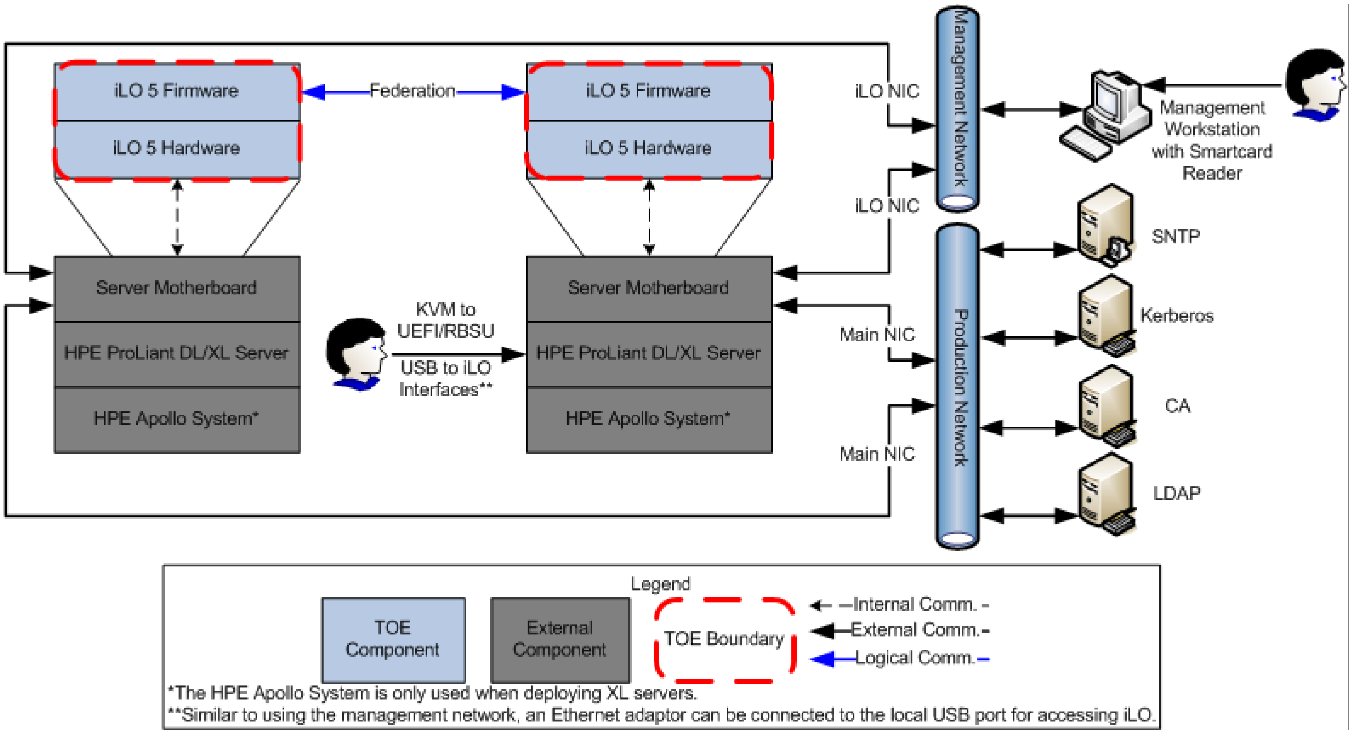

iLO 5 Firmware
iLO 5 Hardware
Server Motherboard
HPE ProLiant DL/XL Server
HPE Apollo System*
KVM to UEFI/RBSU
USB to iLO Interfaces**
iLO NIC
Main NIC
Management Network
Production Network
Management Workstation with Smartcard Reader
SNTP
Kerberos
CA
LDAP
Legend
TOE Component
External Component
TOE Boundary
Internal Comm.
External Comm.
*The HPE Apollo System is only used when deploying XL servers.
**Similar to using the management network, an Ethernet adaptor can be connected to the local USB port for accessing iLO.

Figure 5 – Physical TOE Boundary for Single Server Configuration

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.



*The HPE Apollo System is only used when deploying XL servers.

**Similar to using the management network, an Ethernet adaptor can be connected to the local USB port for accessing iLO.

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:

- *HPE iLO 5 Scripting and Command Line Guide*; Part Number 882043-001; Published: July 2017; Edition: 1
- *HPE iLO 5 User Guide*; Part Number 880740-001; Published: July 2017; Edition: 1
- *HPE iLO Federation User Guide for iLO 5*; Part Number 880724-001; Published: July 2017; Edition: 1
- *UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy*; Part Number 881334-001a; Published: July 2017; Edition: 2
- *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy*; Part Number: 873901-002; Published: July 2017; Edition: 1
- *iLO RESTful API*[21] *Document*; https://hewlettpackard.github.io/ilo-rest-api-docs/ilo5/
- *HPE iLO 5 Cryptographic Module; FIPS 140-2 Non-Proprietary Security Policy*; FIPS Security Level: 1; Document Version: 0.6
- *Hewlett Packard Enterprise Development LP; Integrated Lights-Out 5 v1.11; Guidance Documentation Supplement*; Evaluation Assurance Level (EAL): EAL2+; Document Version: 0.5

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, 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 SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

[21] API – Application Programming Interface

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[22]
- TOE Access
- Trusted Path/Channel

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[23], SHA[24], RSA[25], ECDSA[26], and DSA[27] 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 and Kerberos servers to the TOE are 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 iLO Web GUI and allows system administrators to use limited iLO CHIF commands before authenticating; system administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Multiple forms of authentication are provided by the TOE that include local account authentication, LDAP authentication, Kerberos authentication, and smartcard authentication (which includes CACs and PIV cards). Using the multiple forms of authentication, the TOE is able to identify and authenticate users that access the TOE before allowing them access to any TSF mediating functionality. The TOE also obscures the system administrator's

[22] TSF – TOE Security Functionality
[23] 3DES – Triple Data Encryption Standard
[24] SHA – Secure Hash Algorithm
[25] RSA – Rivest, Shamir, Adleman
[26] ECDSA – Elliptic Curve Digital Signature Algorithm
[27] DSA – Digital Signature Algorithm

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

password using either a bullet (•) in place of each character, an asterisk (*) in place of each character, or by displaying 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 Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, 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. 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
- Manage the recovery firmware image
- 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

When the TOE encounters a corrupt firmware image, it will automatically recover to a stored recovery image in the NAND without user intervention. If the TOE cannot recover functionality, it will enter a maintenance mode where the system administrator can apply a new image to recover the TOE. 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[28] for communications with the LDAP server during user authentication.

[28] LDAPS – Lightweight Directory Access Protocol Secure

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

A system administrator can initiate a secure connection to the TOE over an HTTPS[29] 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 ensure end point identification. A secure connection is required for initial authentication and all TSF management functions performed through these interfaces.

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:

- XML Reply
- iLO “System Maintenance Switch”
- HPE ProLiant DL/XL server operating systems
- HPE Online Configuration Utility (HPONCFG)
- Connecting to an HPE IRS device using HPE Insight Online
- iLO iOS[30] application
- iLO Android application
- Using the iLO service port for mass storage
- Use of SNMP functionality

[29] HTTPS – Hypertext Transport Protocol Secure

[30] iOS – iDevice Operating System

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2. Conformance Claims

This section and Table 5 provide the identification for any CC, 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

Common Criteria (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 Common Evaluation Methodology (CEM) as of 2017-06-30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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
- Organizational security policies to which the TOE must comply
- 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.CRITICAL_FAILURE	An unauthorized user or attacker could corrupt the TOE image to cause a critical failure of the TOE firmware that prevents system administrators from being able to access TOE functionality.
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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 the 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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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.RECOVERY	The TOE will provide mechanisms to automatically recover from a critical firmware failure.

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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 10 – IT Security Objectives

Name	Description
OE.OS	The operating systems running on the TOE hosts 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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5. Extended Components

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

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.

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		✓		

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
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_RCV.2	Automated recovery		✓		
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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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*[31]
- *Severity*
- *Description*
- *Last Update*
- *Count*
- *Category*].

FAU_STG.1 Protected audit trail storage

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

[31] ID – Identification

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 198, SP*[32] *800-67, SP 800-56A, SP 800-90A, FIPS 180-4, FIPS 186-2, and FIPS 186-4*].

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[33], OFB[34], and CTR[35] mode	128, 192, 256	4525
Encryption/ Decryption/ Generation/ Verification/Message Authentication	AES – GCM[36] mode	128, 192, 256	4525
Encryption/Decryption	3DES – CBC mode	(3) 56	2412
Key Generation/Signature Generation	RSA	2048, 3072	2462
Key Generation/Signature Generation/ Signature Verification	DSA	2048, 3072	1204
Signature Verification	RSA	1024, 1536, 2048, 3072, 4096	2462
Public Key Generation/ Public Key Verification/ Signature Generation/ Signature Verification	ECDSA for P-256 and P-384 curves	256, 384	1100

[32] SP – Special Publication
[33] CBC – Cipher Block Chaining
[34] OFB – Output Feedback
[35] CTR – Counter Mode
[36] GCM – Galois/Counter Mode

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Cryptographic Operation	Algorithm	Key Sizes (bits)	Certificate No.
ECC[37] CDH[38] Primitive	ECC CDH for P-256 and P-384 curves	256, 384	1201
Message Digest	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	3706
Message Authentication	HMAC [39] -SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	2985
Random Number Generation	CTR DRBG[40] (with 128-bit AES)	N/A[41]	1485

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 to control access to TOE features. The privilege levels include Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, 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*].

[37] ECC – Elliptic Curve Cryptography
[38] CDH – Cofactor Diffie Hellman
[39] HMAC – Hash-based Message Authentication Code
[40] DRBG – Deterministic Random Bit Generator
[41] N/A – Not Applicable

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 iLO Web GUI's login page (depicted as a question mark "?")*
- *The execution of the following iLO CHIF commands:*
    - *0x0002/0x8002 (Get iLO Status)*
    - *0x0067/0x8067 (Get miscellaneous configuration)*
    - *0x006b/0x806b (Get security jumper state)*
    - *0x0076/0x8076 (Option ROM milestone)*
    - *0x0140/0x8140 (Get iLO certificate)*
    - *0x0141/0x8141 (Set encryption key and iv)*
    - *0x0FFF/0x8FFF (Echo)*

] 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.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*the following authentication mechanisms:*

- *Local authentication mechanisms*
- *LDAP authentication mechanisms*
- *Kerberos authentication mechanisms*
- *Smartcard authentication mechanisms (including general smartcards, CACs, and PIV cards)*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*following rules:*

- *Local authentication – The system administrator navigates to the TOE and enters their local account's credentials. The TOE searches for the entered username in the local accounts database. If it is found, the entered password is compared to the stored password for that account. If the passwords match, the system administrator is assign the correct privileges and allowed access to the TOE.*
- *LDAP authentication – The system administrator navigates to the TOE and enters their domain account's credentials. The TOE forwards the credentials to the LDAP server. The LDAP server evaluates the credentials, and if the username corresponds to a valid domain user and the password matches the stored password, the LDAP server sends a successful message back to the TOE. The account's LDAP groups are queried to assign the correct privileges, and the system administrator is allowed access to the TOE.*

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *Kerberos authentication – There are two methods to authenticate using Kerberos: using a workstation that is part of the domain and using a workstation that is not part of the domain. If the workstation is already logged in to the domain, the ticket granting ticket (TGT) has already been requested during the initial login to the workstation. This means that the system administrator will not have to enter their Kerberos credentials to log in to the TOE. If the workstation is not logged in to the domain, the system administrator must provide their Kerberos credentials. The TOE then performs an Authentication Service Request (AS-REQ) to the Key Distribution Center (KDC) and obtains a TGT for the system administrator. For both methods, the TOE uses the TGT to do an Application Server Request (AP-REQ) to the server, which then does a Ticket Granting Server Request (TGS-REQ) to the KDC. The KDC returns a service ticket as part of an AP-REQ, which is then sent to the TOE. The TOE verifies that it was signed with its own key by the KDC. Contained within the AP-REQ is the Privileged Attribute Certificate (PAC) structure, which is used to determine privileges.*
- *Smartcard authentication – The system administrator inserts the card in to a card reader attached to the workstation. Then they navigate to the iLO Web GUI and click the "Login with SmartCard" button. The TOE will prompt the system administrator to choose their certificate, which is read from the card, from the displayed list. Once prompted, the system administrator types in their PIN[42]. The smartcard is accessed using the provided PIN, and the stored certificate is transferred to the TOE. The TOE checks the certificate's status against the stored CRL.*
    - *For LDAP accounts – If the status of the certificate is valid, the system administrator's username is read from the certificate. If the username is found in LDAP, their LDAP groups are queried to assign the correct privileges and the system administrator is allowed access to the TOE.*
    - *For local accounts – If the status of the certificate is valid, the system administrator's certificate on the smartcard is compared to their account's stored certificate in the TOE. If the certificate correctly maps to the system administrator's account, they are assigned the correct privileges and allowed access to the TOE.*].

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 (•), asterisks (*), 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 iLO Web GUI's login page (depicted as a question mark "?")*
- *The execution of the following iLO CHIF commands:*
    - *0x0002/0x8002 (Get iLO Status)*
    - *0x0067/0x8067 (Get miscellaneous configuration)*

[42] PIN – Personal Identification Number

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *0x006b/0x806b (Get security jumper state)*
- *0x0076/0x8076 (Option ROM milestone)*
- *0x0140/0x8140 (Get iLO certificate)*
- *0x0141/0x8141 (Set encryption key and iv)*
- *0x0FFF/0x8FFF (Echo)*

] 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

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

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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[43]	View
	Session List	Administer User Accounts	Disconnect active sessions
		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[44] and swap the ROM
		Everyone	View
System Information	Summary	Everyone	View
	Processors	Everyone	View
	Memory	Everyone	View
	Network	Everyone	View
	Device Inventory	Everyone	View
	Storage	Everyone	View
Firmware & OS Software	Firmware	Configure iLO Settings	Use Update Firmware button and Upload to iLO Repository button
		Virtual Power and Reset	Use Swap ROM button
		Everyone	View
	Software	Everyone	View
	iLO Repository	Configure System Recovery	Install or Delete firmware images
		Everyone	View
	Install Sets	Everyone	View
	Installation Queue	Everyone	View
iLO Federation	Setup	Configure iLO Settings	Manage
		Everyone	View

[43] Note that "Everyone" is not a role or privilege level. It refers to all roles and privilege levels managed by the TOE.

[44] NMI – Non-Maskable Interrupt

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Menu	Object	Privilege Level	Operations
	Multi-System View	Everyone	View and Filter
	Multi-System Map	Everyone	View and Filter
	Group Virtual Media	Virtual Media	Manage media
		Everyone	View and Filter
	Group Power	Virtual Power and Reset	Use power buttons
		Everyone	View and Filter
	Group Power Settings	Configure iLO Settings	Manage
		Everyone	View and Filter
	Group Firmware Update	Configure iLO Settings	Update firmware
		Everyone	View and Filter
	Group Licensing	Configure iLO Settings	Update license
		Everyone	View and Filter
	Group Configuration	Configure iLO Settings	View and Manage
Remote Console & Media	Launch	Remote Console	Launch iLO Java Integrated Remote Console (JIRC) and iLO .NET Integrated Remote Console (NIRC)
		Everyone	View
	Virtual Media	Virtual Media	Use, eject, and insert media
		Virtual Power and Reset	Reset the server
		Configure iLO Settings	Manage
		Everyone	View
	Hot Keys	Configure iLO Settings	Manage
		Everyone	View
	Security	Configure iLO Settings	Manage
		Everyone	View
Power & Thermal	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
	Power	Everyone	View
	Fans	Everyone	View
	Temperatures	Everyone	View
	Summary	Everyone	View
	General	Configure iLO Settings	Manage

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Menu	Object	Privilege Level	Operations
iLO Dedicated Network Port and iLO Shared Network Port		Everyone	View
	IPv4	Configure iLO Settings	Manage
		Everyone	View
	IPv6	Configure iLO Settings	Manage
		Everyone	View
	SNTP	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	User Administration	Administer User Accounts	Manage users
		Everyone	View, change personal password
	Directory Groups	Configure iLO Settings	Manage directory groups
		Everyone	View
	Licensing	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
	Key Manager	Configure iLO Settings	Manage
		Everyone	View
	Language	Configure iLO Settings	Manage
		Everyone	View
	Firmware Verification	Configure iLO Settings	Scan firmware
		Everyone	View
Security	Access Settings	Configure iLO Settings	Manage
		Everyone	View
	iLO Service Port	Configure iLO Settings	Manage
		Everyone	View
	Secure Shell Key	Administer User Accounts	Manage
		Everyone	View
	Certificate Map	Administer User Accounts	Manage

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Menu	Object	Privilege Level	Operations
		Everyone	View
	CAC/Smartcard	Configure iLO Settings	Manage
		Everyone	View
	SSL[45] Certificate	Configure iLO Settings	Manage
		Everyone	View
	Directory	Configure iLO Settings	Manage
		Everyone	View
	Encryption	Configure iLO Settings	Manage
		Everyone	View
	HPE SSO[46]	Configure iLO Settings	Manage
		Everyone	View
	Login Security Banner	Configure iLO Settings	Manage
		Everyone	View
Management	SNMP Settings	Configure iLO Settings	Manage
		Everyone	View
	AlertMail	Configure iLO Settings	Manage
		Everyone	View
	Remote Syslog	Configure iLO Settings	Manage
		Everyone	View
Intelligent Provisioning	Intelligent Provisioning	Host BIOS and Remote Console	View and manage

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*
- *Management of recovery firmware image*
- *Update the system firmware*].

[45] SSL – Secure Sockets Layer

[46] SSO – Single Sign-On

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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** [*Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, 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 except the System Recovery privilege.*
- ***Operator*** *– An Operator has the following privilege levels: Remote Console, Virtual Power and Reset, Virtual Media, and Host BIOS. 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_RCV.2 Automated recovery

Hierarchical to: FPT_RCV.1 Manual recovery

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.2.1

When automated recovery from [*a corrupt firmware image*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2

For [*a corrupt firmware image*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

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 [<u>*during initial start-up*</u>] to demonstrate the correct operation of [<u>*[the FIPS 140-2-validated cryptographic module's cryptographic functionality]*</u>].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [<u>*[the FIPS 140-2-validated cryptographic module]*</u>].

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 the iLO Web GUI, iLO CLI, iLO CHIF*[47]*, 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 the iLO Web 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 Web GUI, iLO CLI, iLO REST API, iLO UEFI/RBSU Interface, and iLO CHIF. 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

[47] CHIF – Host Channel Interface

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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, iLO CLI, iLO REST API, and iLO 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 these 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[48] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures

[48] CM – Configuration Management

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assurance Requirements	
	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.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 functionality. Hence, each security functionality 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 functionality 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.5	Multiple authentication mechanisms
	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 Functionality	FPT_RCV.2	Automated recovery
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.3	TSF-initiated termination

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Security Functionality	SFR ID	Description
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generates audit records for the startup and shutdown of its 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 iLO Web GUI, iLO CLI, iLO XML Scripting Interface, iLO REST API, or iLO CHIF, 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 iLO 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.
Description	The description identifies the component and detailed characteristics of the recorded 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.
Count	The number of times this event has occurred (if supported).
Category	Areas of iLO that are used to group events together. The categories include Administration, Configuration, Firmware Failure, Maintenance, Other, and Security.

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 implements the algorithms listed in Section 6.2.2. These cryptographic algorithms are used to secure management traffic between the system administrators and the TOE. The iLO Web GUI, iLO XML Scripting Interface, and iLO REST API are protected via the TLS protocol. The iLO CLI is protected via the SSH protocol. An encrypted data stream is used when accessing the JIRC and NIRC.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TOE also uses TLS to protect communications when connecting to the LDAP server. The TOE provides decryption of the Kerberos TGT encryption of the authenticator, and decryption of the client/server session key for Kerberos. 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 to control access to TOE features. The privilege levels include Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, and Configure iLO Settings.

System administrators can configure the TOE to require passwords of a minimum character length. The minimum character length is 8 characters. Also, the TOE obscures the system administrator's password using either a bullet (•) in place of each character, an asterisk (*) in place of each character, or displaying a blank text area during authentication.

The TOE provides unauthenticated access to the help link of the iLO Web GUI and various iLO CHIF commands. The iLO Web GUI's login page contains a question mark "?" link that links to information about logging in to iLO. The iLO CHIF provides the following unauthenticated commands:

- 0x0002/0x8002 (Get iLO Status) – This command returns the current iLO status.
- 0x0067/0x8067 (Get miscellaneous configuration) – This command is used to retrieve miscellaneous configuration items that the TOE is using.
- 0x006b/0x806b (Get security jumper state) – This command is used to retrieve the current state of the security jumper.
- 0x0076/0x8076 (Option ROM milestone) – This command is used to indicate an iLO Option ROM Milestone.
- 0x0140/0x8140 (Get iLO certificate) – This command provides a mechanism for the SMIF client to acquire the public iLO certificate.
- 0x0141/0x8141 (Set encryption key and iv) – This command provides a mechanism for the SMIF client to set iLO SMIF encryption key for current iLO CHIF connection.
- 0x0FFF/0x8FFF (Echo) – This command causes the iLO CHIF to echo back the data portion of this packet. This can be used for testing iLO responsiveness.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

System administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the authentication servers in the TOE environment, the TOE is able to identify and authenticate users that use directory services or smartcards.

The TOE utilizes local authentication, LDAP authentication, Kerberos authentication, and smartcard authentication mechanisms. Local authentication into the TOE is only available when a system administrator creates an account inside the TOE or uses the default Administrator account.

Local authentication works by sending the authenticating account's credentials to the TOE through one of its interfaces. The TOE compares the entered credentials with the stored credentials. The entered username and password must match the stored information or an error is returned. If the two sets of credentials match, the system administrator is authenticated, their privileges are assigned, and they are allowed access into the TOE.

The LDAP authentication uses an LDAP server to verify account information. LDAP groups must be defined within the TOE and associated to privilege levels before a system administrator can successfully access the TOE using this method. Using an interface of the TOE, the system administrator's credentials are passed through the interface to the TOE, which verifies them with the LDAP server. The LDAP server evaluates the credentials and returns a message. If the username corresponds to a valid domain user and the password matches the stored password, the server will return a successful message. Otherwise, an error is returned. If their credentials are valid, the TOE will query the account's LDAP groups and compare them with the group associations within the TOE's security settings. If the account does not have the appropriate LDAP groups to access the TOE, an error is returned. If the account has the same groups as defined in the security settings, then the system administrator is authenticated and allowed access to the TOE.

There are two methods to authenticate using Kerberos: using a workstation that is part of the domain and using a workstation that is not part of the domain. If the workstation is already logged in to the domain, the TGT has already been requested during the initial login to the workstation. This means that the system administrator will not have to enter their Kerberos credentials to log in to the TOE. If the workstation is not logged in to the domain, the system administrator must provide their Kerberos credentials. The TOE then performs an AS-REQ to the KDC and obtains a TGT for the system administrator. For both methods, the TOE uses the TGT to do an AP-REQ to the server, which then does a TGS-REQ to the KDC. The KDC returns a service ticket as part of an AP-REQ, which is then sent to the TOE. The TOE verifies that it was signed with its own key by the KDC. Contained within the AP-REQ is the PAC structure, which is used to determine privileges.

The final authentication method that the TOE offers is smartcard authentication that can be used with generic smartcards, CACs, and PIV cards. All three forms of cards work in the same manner; the cards are only physically different. A CRL can be present in the TOE for this method of authentication. The cards, certificates, and PINs will be managed by the environment. Local accounts that requires smartcard authentication need to have a copy of the certificate imported into the TOE before the TOE will correctly authenticate that account. For both local and directory accounts, the system administrator inserts the card into a card reader attached to the workstation. The system administrator then navigates to the iLO Web GUI and clicks the "Login with SmartCard" button. The TOE will prompt the system administrator to choose their certificate, which is read from the card, from the displayed list. Once prompted, the system administrator types in their PIN. The smartcard is accessed using the provided PIN, and the stored certificate is transferred to the TOE. The TOE checks the certificate's status against the stored CRL. When using a directory account and the status of the certificate is valid, the system administrator's username is read from the certificate. If the username is found in the LDAP server, their groups are queried to assign the correct privileges and the system administrator is allowed access to the TOE. When using a local account and the

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

status of the certificate is valid, the system administrator's certificate on the smartcard is compared to their account's stored certificate in the TOE. If the certificate correctly maps to the system administrator's account, they are assign the correct privileges and allowed access to the TOE.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, 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 Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, 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
- Recovery firmware image
- System firmware

A system administrator may have more than one privilege level assigned to them. The TOE maintains several privilege levels: Host BIOS, Remote Console, System Recovery, Administer User Accounts, Virtual Media, Virtual Power and Reset, 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 except the System Recovery privilege.
- **Operator** – An Operator has the following privilege levels: Remote Console, 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

A copy of the evaluated firmware is loaded into the iLO Repository for use in the automated recovery process. This recovery firmware is verified during the upload and stored in the iLO NAND. During boot up, the TOE verifies the firmware image before loading it for use. If the firmware image fails verification, a copy of the recovery image is taken from the NAND. The copied image is verified before replacing the failed image. No settings are lost during

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

the replacement of the firmware image, and the system is restored to a secure state. If the TOE cannot automatically recover from a corrupt firmware because the firmware fails validation when the recovery image was set, the TOE will enter a maintenance mode awaiting a new image from the system administrator that will not allow access to the TOE until the issue is resolved.

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 the cryptographic module overall, 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 during operation. The TOE performs the following critical self-tests: SP 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_RCV.2, 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 iLO Web GUI, iLO CLI, iLO REST API, iLO UEFI/RBSU Interface, and iLO CHIF. 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 iLO Web GUI). Inactive sessions will be terminated by the TOE after a configurable time interval of system administrator inactivity for the iLO Web GUI, iLO CLI, iLO CHIF, 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 and the LDAP server. Only the TOE is allowed to initiate secure communications with the LDAP server. During authentication, the TOE uses TLS1.2 to make a secure connection to the LDAP server.

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 ensure end point

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

identification. A secure connection is required for authentication and all TSF management functions performed via the iLO Web GUI, iLO CLI, iLO REST API, and iLO XML Scripting Interface.

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

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 the 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 a system 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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
T.CRITICAL_FAILURE An unauthorized user or attacker could corrupt the TOE image to cause a critical failure of the TOE firmware that prevents system administrators from being able to access TOE functionality	O.RECOVERY The TOE will provide mechanisms to automatically recover from a critical firmware failure.	O.RECOVERY counters this threat by ensuring that a corruption of the firmware image will be replaced by a recovery image to allow system administrators uninterrupted access to the TOE.
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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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 the 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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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 the 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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.	NOE.PHYSICAL satisfies this assumption by ensuring physical security is provided within the TOE environment to provide appropriate protection to the network resources.
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 system 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 that 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.	OE.PROTECT satisfies this assumption by ensuring the TOE environment provides protection from external interference or tampering.
	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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 the 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.
	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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
	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 HPE 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.
	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. Multiple methods to identify and authenticate system administrators must be provided by the TOE. 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.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that system administrators are provided multiple authentication methods when accessing the TOE.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that passwords are obscured during the TOE's login process.
	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.
	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 that will be displayed on the iLO Web GUI 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.
O.RECOVERY The TOE will provide mechanisms to automatically recover from a critical firmware failure.	FPT_RCV.2 Automated recovery	The requirement meets the objective by ensuring that the TOE automatically recovers from a corruption in the firmware image using the stored recovery images.

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.

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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	✓	
	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.5	No dependencies	✓	
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_RCV.2	AGD_OPE.1	✓	
FPT_STM.1	No dependencies	✓	
FPT_TST.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FTA_TAB.1	No dependencies	✓	
FTA_TSE.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9. Acronyms

Table 24 defines 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
AP-REQ	Application Server Request
ASIC	Application Specific Integrated Circuits
AS-REQ	Authentication Service Request
BIOS	Basic Input/Output System
CA	Certificate Authority
CAC	Common Access Card
CBC	Cipher Block Chaining
CC	Common Criteria
CDH	Cofactor Diffie Hellman
CEM	Common Evaluation Methodology
CHIF	Host Channel Interface
CLI	Command Line Interface
CM	Configuration Management
CNSA	Commercial National Security Algorithm
CRL	Certificate Revocation List
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDSA	Elliptical Curve Digital Signature Algorithm
ERS	Embedded Remote Support
ESR	Extended Support Release
ESKM	Enterprise Secure Key Manager

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
FIPS	Federal Information Processing Standard
GB	Gigabyte
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HPE	Hewlett Packard Enterprise Development LP
HPONCFG	HP Online Configuration Utility
HTTPS	Hypertext Transport Protocol Secure
ID	Identification
iLO	Integrated Lights-Out
iOS	iDevice Operating System
IP	Internet Protocol
IRS	Insight Remote Support
IT	Information Technology
JIRC	Java Integrated Remote Console
KAT	Known Answer Test
KDC	Key Distribution Center
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
NIRC	.NET Integrated Remote Console
NMI	Non-Maskable Interrupt
OFB	Output Feedback
OS	Operating System
OSP	Organizational Security Policy
PAC	Privilege Attribute Certificate
PIN	Personal Identification Number
PIV	Personal Identification Verification
POST	Power-on Self-Test
PP	Protection Profile

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
RBSU	ROM-Based Setup Utility
REST	Representational State Transfer
RFC	Request for Comments
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Security Target
TGS-REQ	Ticket Granting Server Request
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
XML	eXtensible Markup Language

©2018 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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