Hewlett Packard Enterprise

Integrated Lights-Out 6 v1.11

Security Target

Version 1.8

July 2025

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
0.1	26 June 2023	Initial draft.
0.2	13 September 2023	Initial draft for evaluation.
1.0	19 October 2023	Addressed evaluator ORs.
1.1	21 February 2024	Miscellaneous updates.
1.2	27 May 2024	Miscellaneous updates.
1.3	29 July 2024	Addressed CB ORs.
1.4	3 April 2025	Miscellaneous updates.
1.5	7 May 2025	Addressed evaluator ORs.
1.6	21 May 2025	Update X.509 claims.
1.7	17 June 2025	Updated LDAP cipher suites.
1.8	16 July 2025	Final updates.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Hewlett Packard Enterprise Integrated Lights-Out 6 v1.11 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 Hewlett Packard Enterprise (HPE) Integrated Lights-Out (iLO) is an integrated component of HPE ProLiant 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.

Figure 1: HPE iLO6

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Integrated Lights-Out 6 v1.11
Security Target	Integrated Lights-Out 6 v1.11 Security Target, v1.8

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) EAL4 augmented with ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
BMC	Baseboard Management Controller
CC	Common Criteria
EAL	Evaluation Assurance Level
HPE	Hewlett Packard Enterprise
iLO	Integrated Lights-Out
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

4 The TOE is a Baseboard Management Controller (BMC).

2.2 Usage

5 The TOE is used to simplify 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.

6 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.

7 System administrators will typically perform server administration by remotely connecting to iLO over HTTPS (Web GUI) or SSH (CLI). Using iLO Federation Management, a system administrator may manage multiple servers from one system running the iLO Web GUI.

8 The TOE also provides REST API and XML Scripting interfaces over HTTPS for secure integration with data centre automation tools.

9 The following figure depicts the TOE in the evaluated configuration:

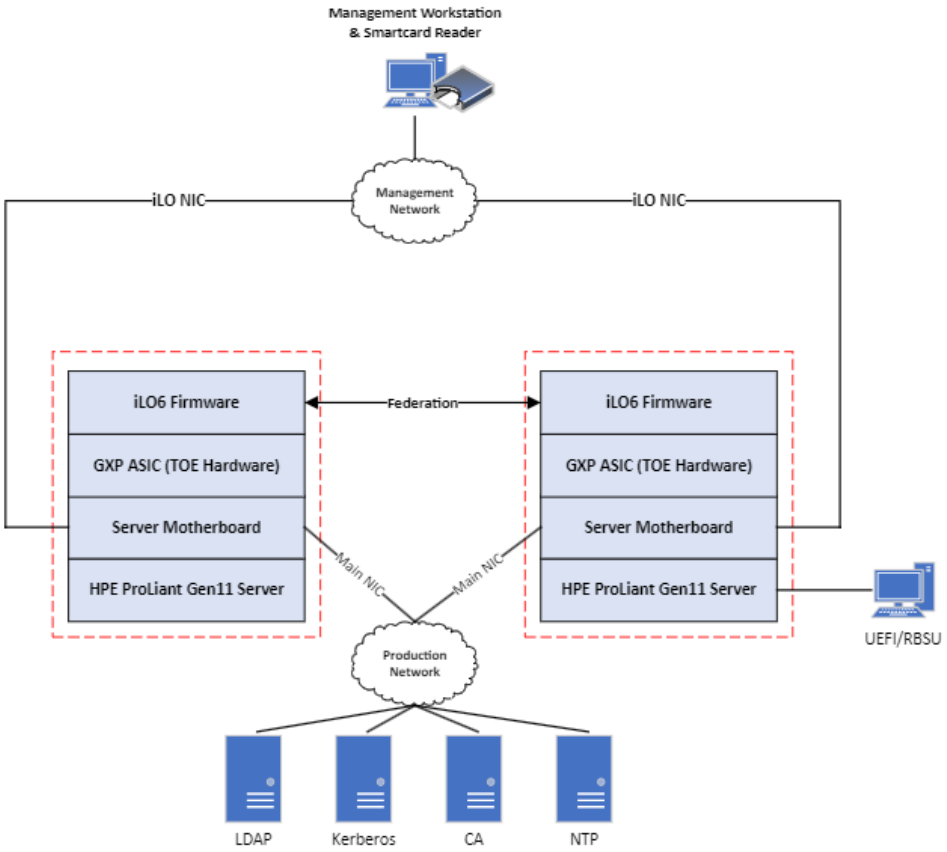

Figure 2: TOE Deployment

2.3 Security Functions / Logical Scope

10 The TOE provides the following security functions:

a) **Trusted Path/Channels.** The TOE provides protected communication with external entities:

i) HTTPS is used to protect remote administration via the iLO Web GUI, iLO REST API, and iLO XML Scripting Interface.

ii) SSH is used to protect remote system administration via the iLO CLI.

iii) TLS is used to protect communication with the LDAP server.

iv) Communications with the Kerberos server are protected using AES encryption for Kerberos version 5.

b) **Identification and Authentication.** The provides limited functionality prior to authentication. The TOE supports the following authentication mechanisms:

i) Username and password (local or LDAP)

ii) Kerberos authentication

iii) Smartcard authentication, including CAC/PIV cards (local or LDAP)

X.509 certificates are used for authentication of endpoints of trusted IT entities and remote administrators over HTTPS/TLS.

c) **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.

d) **Security Management.** The TOE enforces Role Based Access Control (RBAC). The TOE allows system administrators to perform the following actions:

i) Management of iLO user accounts

ii) Management of user permissions

iii) Management of security settings

iv) Management of host server access settings

v) Management of system power

vi) Management of recovery firmware image

vii) Update the system firmware.

e) **Self-Protection.** When the TOE detects 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 NTP server. The TOE also implements numerous self-tests to ensure that the cryptographic functionality of the TOE is functioning correctly.

f) **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.

g) **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.

h) **Cryptographic Operations.** The TOE incorporates FIPS-validated algorithms used for all protected communications (CAVP # A3417).

2.3.1 Exclusions

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

a) XML Reply – Requires configuration of external applications and is disabled by default.

b) iLO "System Maintenance Switch" - Disabled by default.

c) HPE Online Configuration Utility (HPONCFG) – Requires configuration of an external host application and is disabled by default.

d) Connecting to an HPE IRS device using HPE Insight Online – Requires configuration of external software and is disabled by default.

e) iLO iOS30 application – Disabled by default.

f) iLO Android application – Disabled by default.

g) Using the iLO service port for mass storage – Disabled by default.

h) Use of SNMP functionality – Disabled by default.

i) iLO ROM-Based Setup Utility (RBSU) – Disabled in the evaluated configuration.

2.4 Physical Scope

12 The physical boundary of the TOE encompasses:

a) Firmware: iLO6 v1.11

b) ASIC Hardware: GXP ASIC Part numbers P00197-265 and P00197-285.

c) The following HPE ProLiant Gen11 server hardware:

- HPE ProLiant DL365 Gen11
- HPE ProLiant DL385 Gen11
- HPE ProLiant DL325 Gen11
- HPE ProLiant DL345 Gen11
- HPE ProLiant DL360 Gen11
- HPE ProLiant DL320 Gen11
- HPE ProLiant DL380 Gen11
- HPE ProLiant DL380a Gen11
- HPE ProLiant DL110 Gen11
- HPE ProLiant DL560 Gen11

2.4.1 TOE Delivery

13 The TOE firmware comes pre-installed on the ASIC, integrated into the motherboard of the ProLiant server, and delivered to the customer by a commercial courier service with a package tracking system. Firmware updates may be downloaded by customers from the HPE Support Center at:
https://support.hpe.com/connect/s/softwaredetails?language=en_US&softwareId=MTX_af9a190233214ad493db9d1115

2.4.2 Guidance Documents

14 The following guidance documentation is provided to customers online in HTML format via the following links:

- HPE iLO 6 Scripting and Command Line Guide, Part Number: 30-6A3B1815-005
  https://support.hpe.com/hpesc/public/docDisplay?docId=sd00002199en_us&page=index.html
- HPE iLO 6 User Guide, Part Number: 30-7A345B12-025
  https://support.hpe.com/hpesc/public/docDisplay?docId=sd00002007en_us&page=index.html
- HPE iLO Federation User Guide for iLO 6, Part Number: 30-4176C04C-002
  https://support.hpe.com/hpesc/public/docDisplay?docId=sd00002291en_us&docLocale=en_US
- Integrated Management Log Messages for HPE ProLiant Gen10, Gen10 Plus, and Gen11 servers and HPE Synergy, Part Number: 30-EB5CD181-001
  https://support.hpe.com/hpesc/public/docDisplay?docId=a00046957en_us
- iLO RESTful API Guide
  https://servermanagementportal.ext.hpe.com/docs/redfishservices/ilos/ilo6/ilo6_111/
- UEFI System Utilities User Guide for HPE Compute Gen11 Servers, Part Number: 30-163527A4-001g
  https://support.hpe.com/hpesc/public/docDisplay?docId=sd00003788en_us&docLocale=en_US

15 The TOE also includes the following Common Criteria Guide, delivered via email as a PDF, and available to customers by raising a request to their HPE sales team:

- HPE Integrated Lights-Out 6 v1.11, Common Criteria Guide, v1.5

2.4.3 Non-TOE Components

16 The TOE operates with the following components in the environment:

a) **Management Workstation.** Workstation required to access and manage the TOE.

b) **Smartcard and reader.** FIPS 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcard and reader.

c) **LDAP Server.** LDAPv3 directory server.

d) **Kerberos Server.** Kerberos Network Authentication Service, version 5.

e) **CA Server.** X.509 Public Key Infrastructure with a CRL.

f) **NTP Server.** NTPv4 time server.

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
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.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.MASQUERADE	An unauthorized user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	An unauthorized user or attacker may gain access to security data stored on the TOE, even though the user is not authorized in accordance with the TOE security policy.

3.2 Assumptions

Table 4: Assumptions

Identifier	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

Table 5: Organizational Security Policies

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

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical and logical attack.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
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, and authenticate IT entities it's configured to communicate with. 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.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators, cluster transmissions, LDAP, and Kerberos connections.
O.RECOVERY	The TOE will provide mechanisms to automatically recover from a critical firmware failure.

5 Security Requirements

5.1 Conventions

17 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

18 Table 8 identifies the extended components which are incorporated into this ST.

Table 8: Extended Components

Component	Title	Rationale
FIA_X509.1	X509 Certificate Validation	No existing CC Part 2 classes or components address X.509 certificate requirements.
FIA_X509.2	X509 Certificate Authentication	

5.2.1 X509 Certificate Validation (FIA_X509)

5.2.1.1 Family Behavior

19 This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules.

5.2.1.2 Component Leveling

20 FIA_X509.1 - X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the rules specified in the component.

21 FIA_X509.2 - X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates.

5.2.1.3 Management: FIA_X509.1, FIA_X509.2

22 The following actions could be considered for the management functions in FMT:

a) None

5.2.1.4 Audit: FIA_X509.1, FIA_X509.2

23 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) None

FIA_X509.1 Certificate Validation

Hierarchical to: No other components.

Dependencies: FIA_X509.2 Certificate Authentication

FIA_X509.1.1 The TSF shall validate certificates in accordance with the following rules:

[selection:

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certificate path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP), a Certificate Revocation List (CRL), no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules: [assignment: rules that govern contents of the extendedKeyUsage field that needs to be verified].

].

FIA_X509.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509.2 Certificate Authentication

Hierarchical to: No other components.

Dependencies: FIA_X509.1 Certificate Validation

FIA_X509.2.1 The TSF shall use X.509v3 certificates to support authentication for [selection: DTLS, HTTPS, IPsec, TLS, SSH, [assignment: other protocols], no protocols], and [selection: code signing for system software updates [assignment: other uses], no additional uses].

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title	Source
FAU_GEN.1	Audit Data Generation	CC Part 2
FAU_GEN.2	User Identity Association	CC Part 2
FAU_SAR.1	Security Audit Review	CC Part 2
FAU_SAR.3	Selectable Audit Review	CC Part 2
FAU_STG.1	Protected Audit Trail Storage	CC Part 2
FAU_STG.4	Prevention of Audit Data Loss	CC Part 2
FCS_COP.1	Cryptographic Operation	CC Part 2
FDP_RIP.1	Subset Residual Information Protection	CC Part 2
FIA_ATD.1	User Attribute Definition	CC Part 2
FIA_SOS.1	Verification of Secrets	CC Part 2
FIA_UAU.1	Timing of Authentication	CC Part 2
FIA_UAU.5	Multiple Authentication Mechanism	CC Part 2
FIA_UAU.7	Protected Authentication Feedback	CC Part 2
FIA_UID.1	Timing of Identification	CC Part 2
FIA_X509.1(1)	X509 Certificate Validation/Smartcard	CC Part 2 - Extended
FIA_X509.1(2)	X509 Certificate Validation/LDAP	CC Part 2 - Extended
FIA_X509.2(1)	X509 Certificate Authentication/Smartcard	CC Part 2 - Extended
FIA_X509.2(2)	X509 Certificate Authentication/LDAP	CC Part 2 - Extended
FMT_MTD.1	Management of TSF Data	CC Part 2
FMT_SMF.1	Specification of Management Functions	CC Part 2
FMT_SMR.1	Security Roles	CC Part 2
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	CC Part 2
FPT_RCV.2	Automated Recovery	CC Part 2

Requirement	Title	Source
FPT_STM.1	Reliable Time Stamps	CC Part 2
FTA_SSL.3	TSF-Initiated Termination	CC Part 2
FTA_TAB.1	Default TOE Access Banners	CC Part 2
FTA_TSE.1	TOE Session Establishment	CC Part 2
FTP_ITC.1	Inter-TSF Trusted Channel	CC Part 2
FTP_TRP.1	Trusted Path	CC Part 2

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*All administrative actions taken on the iLO interfaces; critical system events and status*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorized system administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.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*
- *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.

5.3.2 Cryptographic Support (FCS)

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 10, Table 11, Table 12, and Table 13*] in accordance with a specified cryptographic algorithm [*listed in the 'Algorithm' column of Table 10, Table 11, Table 12, and Table 13*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 10, Table 11, Table 12, and Table 13*] that meet the following: [*the standard in the 'Standard' column of Table 10, Table 11, Table 12, and Table 13*].

Application Note: Table 10 identifies the cryptographic operations for the TLS implementation. Table 11 defines the cryptographic operations for the SSH implementation. Table 12 identifies the cryptographic operations for the Kerberos implementation. Table 13 identifies the cryptographic operations for the iLO Federation implementation.

Table 10: Cryptographic Algorithms and Keys (TLS)

Cryptographic Operation	Algorithm	Key/Digest/Curve Size	Standard	CAVP
Encryption/Decryption	AES-CBC, AES-GCM	128, 256	NIST SP 800-38A	A3417
Key Agreement	Diffie-Hellman (KAS FFC)	2048, 3072	NIST SP 800-56A	
	KAS ECC	NIST P-256 and P-384 curves		
Key Generation	RSA, DSA, ECDSA	Keys: 2048, 3072 Curves: NIST P-256 and P-384	FIPS PUB 186-4	
Message Digest	SHA-256, SHA-384	256, 384	FIPS PUB 180-4	
Message Authentication	HMAC-SHA-256, HMAC-SHA-384	256, 384	FIPS PUB 198-1 and 180-4	
Random Number Generation	CTR DRBG (128-bit and 256-bit AES)	N/A	NIST SP 800-90A	

Table 11: Cryptographic Algorithms and Keys (SSH)

Cryptographic Operation	Algorithm	Key/Digest/Curve Size	Standard	CAVP
Encryption/Decryption	AES-GCM, AES-CTR	256	NIST SP 800-38A	A3417
Key Generation	RSA, ECDSA	Keys: 2048, 4096 Curves: NIST P-384	FIPS PUB 186-4	
Key Agreement	KSA FFC (FFC Safe Primes)	2048	NIST SP 800-56A	
Message Digest	SHA-1, SHA-256	160, 256	FIPS PUB 180-4	
Message Authentication	HMAC-SHA-256	256	FIPS PUB 198-1 and 180-4	
Random Number Generation	CTR DRBG (128-bit and 256-bit AES)	N/A	NIST SP 800-90A	

Table 12: Cryptographic Algorithms and Keys (Kerberos)

Cryptographic Operation	Algorithm	Key / Digest	Standard	CAVP
Encryption/Decryption	AES-CBC	256	NIST SP 800-38A	A3417
Message Digest	SHA-1	160	FIPS PUB 180-4	
Message Authentication	HMAC-SHA1-96	96	FIPS PUB 198-1 and 180-4	
Random Number Generation	CTR DRBG (256-bit AES)	N/A	NIST SP 800-90A	

Table 13: Cryptographic Algorithms and Keys (iLO Federation)

Cryptographic Operation	Algorithm	Key / Digest	Standard	CAVP
Encryption/Decryption	AES-CBC	128	NIST SP 800-38A	A3417
Random Number Generation	CTR DRBG (128-bit AES)	N/A	NIST SP 800-90A	

5.3.3 User Data Protection (FDP)

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*].

5.3.4 Identification and Authentication (FIA)

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*].

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 0 characters and a maximum of 39 characters*].

FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

- *The use of the help link on the iLO Web GUI's login page (depicted as a question mark "?")*

] 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 assigned 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.*
- *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 . 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 (•) 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 "?")*

] 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.

FIA_X509.1(1) Certificate Validation/Smartcard

Hierarchical to: No other components.

Dependencies: FIA_X509.2(1) Certificate Authentication/Smartcard

FIA_X509.1.1(1) The TSF shall validate certificates in accordance with the following rules:

[

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certificate path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL)].

].

FIA_X509.1.2(1) The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509.2(1) Certificate Authentication/Smartcard

Hierarchical to: No other components.

Dependencies: FIA_X509.1 Certificate Validation

FIA_X509.2.1(1) The TSF shall use X.509v3 certificates to support authentication for [no protocols] and [[*smartcard user authentication*]].

FIA_X509.1(2) Certificate Validation/LDAP

Hierarchical to: No other components.

Dependencies: FIA_X509.2(2) Certificate Authentication/LDAP

FIA_X509.1.1(2) The TSF shall validate certificates in accordance with the following rules:

[

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certificate path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method].

- The TSF shall validate the extendedKeyUsage field according to the following rules: [*Server certificates presented for HTTPS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field].*].

].

FIA_X509.1.2(2) The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509.2(2) Certificate Authentication/Smartcard

Hierarchical to: No other components.

Dependencies: FIA_X509.1(2) Certificate Validation/LDAP

FIA_X509.2.1(2) The TSF shall use X.509v3 certificates to support authentication for [TLS] and [no additional uses].

5.3.5 Security Management (FMT)

FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [[*perform the operations listed in the "Operations" column of Table 14 to*]] the [*objects listed in the "Objects" column of Table 14*] to [*the privilege levels listed under the "Privilege Level" column of Table 14*].

Application Note: "Everyone" is not a role or privilege level. It refers to all roles and privilege levels supported by the TOE. Where specified, a privilege may be restricted to only having access to the function/feature.

Table 14: Management of TSF Data

Function/Feature	Object	Privilege Level	Operations
Information	Overview	Everyone	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

Function/Feature	Object	Privilege Level	Operations
	Active Health System Log	Configure iLO Settings	Enable/disable logging and clear event logs.
		Everyone	View
	Diagnostics	Configure iLO Setting	Reset iLO
		Virtual Power and Reset	Generate Non-Maskable Interrupt and swap the ROM.
		Everyone	View
System Information	Summary	Everyone	View
	Processors	Everyone	View
	Memory	Everyone	View
	Network	Everyone Host NIC	View
	Device Inventory	Everyone	View
	Storage	Everyone Host Storage	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	Recovery Set	Install or Delete firmware images
		Everyone	View
	Install Sets	Everyone	View
	Installation Queue	Everyone	View

Function/Feature	Object	Privilege Level	Operations
iLO Federation	Setup	Configure iLO Settings	Manage
		Everyone	View
	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 and Media	Launch	Remote Console	Launch 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

Function/Feature	Object	Privilege Level	Operations
Power and 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
		Everyone	View
iLO Dedicated Network Port and iLO Shared Network Port	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.

Function/Feature	Object	Privilege Level	Operations
	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
		Everyone	View
	CAC/Smartcard	Configure iLO Settings	Manage
		Everyone	View
	SSL Certificate	Configure iLO Settings	Manage
		Everyone	View
	Directory	Configure iLO Settings	Manage

Function/Feature	Object	Privilege Level	Operations
		Everyone	View
	Encryption	Configure iLO Settings	Manage
		Everyone	View
	HPE SSO	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	Manage and View

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

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

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the ~~roles~~ **privilege levels** [*Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS, Configure iLO Settings, Administer User Accounts, Host NIC, Host Storage, Recovery Set*].

FMT_SMR.1.2 The TSF shall be able to associate users with ~~roles~~ **privilege levels**.

Application Note: The TOE is shipped with a default Administrator account that is assigned all privileges. This account is used to setup the TOE and assign the primary Administrator role. The roles of Administrator, Operator, ReadOnly, and Custom are pre-defined roles made of a combination of the privilege levels listed above, as follows:

- Administrator – Enables all privileges except for Recovery Set.
- Operator – Enables all privileges except Configure iLO Settings, Administer User Accounts, and Recovery Set.
- ReadOnly – Enables only the Login privilege.
- Custom – Allows the user to define a custom set of privileges.

5.3.6 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

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.

5.3.7 TOE Access (FTA)

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 and iLO CLI. All other external interfaces are excluded from the scope.

FTA_TAB.1 TOA 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, and iLO REST API. All other external interfaces are excluded from the scope.

5.3.8 Truster Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*authentication with an LDAP and/or a Kerberos server*].

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].

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 [[*TOE administration performed via the iLO Web GUI, iLO CLI, iLO REST API, and iLO XML Scripting Interface*]].

5.4 Assurance Requirements

24 The TOE security assurance requirements are summarized in Table 15 commensurate with EAL4+ (ALC_FLR.2).

Table 15: Assurance Requirements

Assurance Class	Components	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
ALC: Life-cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
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

Assurance Class	Components	Description
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

6 TOE Summary Specification

6.1 Security Audit

Related SFRs: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4

25 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, or iLO REST API, system administrators are able to review all audit records.

26 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 16 in ascending or descending order. When the audit trail reaches capacity, the oldest records are overwritten with new records.

Table 16: Audit Record Content

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.

6.2 Cryptographic Support

Related SFRs: FCS_COP.1

27 The TOE implements FIPS-validated cryptographic algorithms (CAVP # A3417) used to implement the cryptographic operations listed in FCS_COP.1.1. 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. The TOE also uses TLS to protect communications when connecting to the LDAP server.

28 The TOE provides decryption of the Kerberos TGT encryption of the authenticator, and decryption of the client/server session key for Kerberos using AES256-CTS-HMAC-SHA1-96. Communications between iLO instances in a cluster (iLO Federation) are encrypted using AES_128_CBC.

6.3 User Data Protection

Related SFRs: FDP_RIP.1

29 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.

6.4 Identification and Authentication

Related SFRs: FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FIA_X509.1(1), and FIA_X509.2(1)

30 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 Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS, Configure iLO Settings, Administer User Accounts, Host NIC, Host Storage, Recovery Set.

31 System administrators can configure the TOE to require passwords of a minimum character length. The minimum default length is 8 characters. The minimum configurable length is 0 characters to a maximum of 39. During authentication, the TOE obscures the system administrator’s password using either a bullet (•) in place of each character for the Web GUI, or blank text for the CLI.

32 The TOE provides unauthenticated access to the help link of the iLO Web GUI. The iLO Web GUI’s login page contains a question mark “?” link that links to information about logging in to iLO.

33 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.

34 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.

35 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.

36 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.

37 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.

38 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 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.

6.5 Security Management

Related SFRs: FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

39 The TOE will restrict access to the following security functions:

- Management of iLO user accounts
- Management of user permissions
- Management of security settings
- Management of host server access settings
- Management of system power
- Management of recovery firmware image
- Update the system firmware.

40 The TOE will restrict a system administrator's ability to manage TSF data on various objects on the host server. Access to manage these objects is based on the assigned privileges defined in Table 14.

41 The following table provides a high-level description of the privilege levels and associated permissions:

Table 17: iLO User Privileges

Privilege	Description
Login	Enables a user to login to iLO. This minimum privilege must be assigned to a user before any TOE feature can be accessed.
Remote Console	Enables a user to access the host system remote console, including video, keyboard, and mouse control. Users with this privilege can access the BIOS, and therefore may be able to perform host-based BIOS, iLO, storage, and network tasks.
Virtual Power and Rest	Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the Generate NMI to System button.
Virtual Media	Enables a user to use the virtual media feature on the host system.
Host BIOS	Allows configuration of the host BIOS settings by using the UEFI System Utilities. This privilege is required for replacing the active system ROM with the redundant system ROM. This privilege does not affect configuration through host-based utilities.
Configure iLO Settings	Enables a user to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.
Administer User Accounts	Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you are not assigned this privilege, you can view your own settings and change your own password.
Host NIC	Enables a user to configure the host NIC settings.

Privilege	Description
HOST Storage	Enables a user to configure the host storage settings.
Recovery Set	Enables a user to manage the Recovery Set. By default, the Recovery Set privilege is assigned to the default Administrator account. This privilege can be added to a user account only by creating or editing the account with an account that already has this privilege.

42 A system administrator may have more than one privilege level assigned to them. The LDAP server would manage the groups associated to the privilege levels (or roles) of iLO. The TOE supports user roles of Administrator, Operator, ReadOnly, and Custom, and are made of a combination of the privilege levels listed above, as follows:

Administrator – Enables all privileges except for Recovery Set.

Operator – Enables all privileges except Configure iLO Settings, Administer User Accounts, and Recovery Set.

ReadOnly – Enables only the Login privilege.

Custom – Allows the user to define a custom set of privileges.

43 Additional detail about iLO user account privileges can be found in the iLO User Guide: https://support.hpe.com/hpesc/public/docDisplay?docId=sd00002007en_us&page=GUID-99266123-6796-4FAB-9F9C-24E0B3A756EF.html

6.6 Protection of the TSF

Related SFRs: FPT_RCV.2, FPT_STM.1

44 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 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.

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

6.7 TOE Access

Related SFRs: FTA_SSL.3, FTA_TAB.1, FTA_TSE.1

46 The TOE will enforce an incremented login delay between failed login attempts on the iLO Web GUI, iLO CLI, and iLO REST API. 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 and iLO CLI.

6.8 Trusted Path/Channels

Related SFRs: FTP_ITC.1, FTP_TRP.1, FIA_X509.1(2), FIA_X509.2(2), FPT_ITT.1

6.8.1 Web GUI, REST API, and XML Scripting Communications

47 All communications with remote administrators via the Web GUI, REST API, and XML Scripting interfaces are protected using TLSv1.2. The following default cipher suites are supported in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

6.8.1.1 X.509 Certificates

48 X.509 server certificates are verified and signed by a trusted CA before being loaded onto the TOE. When the X.509 certificate is loaded onto the TOE, the TOE compares the public key from the CSR and validates that the extendedKeyUsage authentication purpose is set to Server Authentication.

49 If any of the validations fail the TOE reverts back to its self-signed certificate.

6.8.2 CLI Communications

50 When the CLI is used, the connection between the TOE and the remote administrator is protected from modification and disclosure using SSHv2. The TOE supports both username/password and publickey-based authentication. The following algorithms are supported in the evaluated configuration:

Publickey Algorithms: ssh-rsa.

Encryption Algorithms: aes256-ctr, AEAD_AES_256_GCM, aes256gcm@openssh.com.

MAC Algorithms: hmac-sha2-256, AEAD_AES_256_GCM.

Key Exchange Algorithms: diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1.

6.8.3 LDAP Communications

51 Communications with an external LDAP server are protected using TLSv1.2. The following default cipher suites are supported in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

6.8.3.1 X.509 Certificates

52 The TOE performs TLS client validation of the LDAP server certificate during the TLS handshake, checking for the following characteristics:

a) The certification path terminates with a trusted CA certificate;

b) All CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE

c) The extendedKeyUsage field contains the Server Authentication Purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1).

53 If any of the above validations fail the TOE does not accept the connection.

Note: In the evaluated configuration, the LDAP CA certificate is manually imported onto the TOE and is not automatically validated. Administrators must manually verify the certificate CA flag and the key usage prior to import.

6.8.4 Kerberos Communications

54 Communications with the Kerberos server are protected using AES encryption for Kerberos version 5. The TOE provides decryption of the Kerberos TGT encryption of the authenticator, and decryption of the client/server session key for Kerberos.

6.8.5 Cluster Communications (iLO Federation)

55 Message exchange between iLO instances in a cluster is performed over HTTP. The exchanged payload is encrypted using AES_128_CBC.

7 Rationale

7.1 Security Objectives Rationale

56 Table 18 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 18: Security Objectives Mapping

	T.CONFIG	T.CRITICAL_FAILURE	T.EAVES	T.MASQUERADE	T.UNAUTH	A.LOCATE	A.MANAGE	P.MANAGE
O.ADMIN	X				X			X
O.AUDIT					X			
O.AUTHENTICATE	X			X	X			X
O.PROTCOMMS			X					
O.RECOVERY		X						
OE.ADMIN							X	
OE.PHYSICAL						X		

57 Table 19 provides the justification to show that the security objectives are suitable to address the security problem.

Table 19: Suitability of Security Objectives

Element	Justification
T.CONFIG	**O.ADMIN** ensures that the TOE provides efficient management of its functions and data, mitigating the threat of accidental misconfiguration. It counters this threat by allowing a system administrator to properly configure the mechanisms of the TOE. **O.AUTHENTICATE** ensures that the TOE has identified and authenticated a system administrator before they are allowed to access any data.
T.CRITICAL_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.

Element	Justification
T.EAVES	**O.PROTCOMMS** mitigates this threat as it requires the TOE to encrypt communications with remote administrators, cluster communications, and communications with external LDAP and Kerberos providers.
T.MASQUERADE	**O.AUTHENTICATE** ensures that The TOE is able to identify and authenticate system administrators prior to allowing access to TOE administrative functions and data, and authenticate IT entities it's configured to communicate with.
T.UNAUTH	**O.AUDIT** ensures that unauthorized attempts to access the TOE are recorded. **O.ADMIN** ensures that access to TOE security data is limited to those system administrators with access to the management functions of the TOE. **O.AUTHENTICATE** ensures that system administrators are identified and authenticated prior to gaining access to TOE security data.
A.LOCATE	**OE.PHYSICAL** supports this assumption by ensuring that the operational environment provides physical and logical protection of the TOE.
A.MANAGE	**OE.ADMIN** supports this assumption by ensuring the availability of trained, competent administrators who are trustworthy and not malicious.
P.MANAGE	**O.ADMIN** ensures that the TOE provides the necessary tools to support the P.MANAGE policy. **O.AUTHENTICATE** ensures that only authorized system administrators are granted access to the tools required to manage the TOE.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

58 The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2). EAL4 was chosen to provide a level of assurance that is consistent with robust commercial security practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 20: Security Requirements Mapping

	O.ADMIN	O.AUDIT	O.AUTHENTICATE	O.PROTCOMMS	O.RECOVERY
FAU_GEN.1		X			
FAU_GEN.2		X			
FAU_SAR.1		X			
FAU_SAR.3		X			
FAU_STG.1		X			
FAU_STG.4		X			
FCS_COP.1				X	
FDP_RIP.1	X				
FIA_ATD.1			X		
FIA_SOS.1			X		
FIA_UAU.1			X		
FIA_UAU.5			X		
FIA_UAU.7			X		
FIA_UID.1			X		
FIA_X509.1(1)			X		
FIA_X509.1(2)			X	X	
FIA_X509.2(1)			X		
FIA_X509.2(2)			X	X	

	O.ADMIN	O.AUDIT	O.AUTHENTICATE	O.PROTCOMMS	O.RECOVERY
FMT_MTD.1	X				
FMT_SMF.1	X				
FMT_SMR.1	X				
FPT_ITT.1				X	
FPT_RCV.1					X
FPT_STM.1		X			
FTA_SSL.3			X		
FTA_TAB.1			X		
FTA_TSE.1			X		
FTP_ITC.1				X	
FTP_TRP.1				X	

Table 21: Suitability of SFRs

Objectives	SFRs
O.ADMIN	**FDP_RIP.1** 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_MTD.1 and FMT_SMF.1** meet the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF. **FMT_SMR.1** meets the objective by ensuring that the TOE associates system administrators with privilege levels to provide access to TSF management functions and data.

Objectives	SFRs
O.AUDIT	**FAU_GEN.1** 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** 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** meets the objective by ensuring that the TOE provides the ability to review logs. **FAU_SAR.3** 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** meets this objective by preventing arbitrary modification of the audit trail. **FAU_STG.4** meets this objective by overwriting the oldest stored audit records once the audit trail is full. **FPT_STM.1** satisfies this objective by providing reliable time stamps for use in all audit logs.
O.AUTHENTICATE	**FIA_ATD.1** meets this objective by ensuring that they TOE maintains user attributes used to authenticate the system administrator. **FIA_SOS.1** meets this objective by ensuring that the system administrators' passwords are of sufficient length. **FIA_UAU.1** meets the objective by ensuring that system administrators are authenticated before access to TOE functions is allowed. **FIA_UAU.5** meets the objective by ensuring that system administrators are provided multiple authentication methods when accessing the TOE. **FIA_UAU.7** meets the objective by ensuring that passwords are obscured during the TOE's login process. **FIA_UID.1** meets the objective by ensuring that system administrators are identified before access to TOE functions is allowed. **FIA_X509.1(1/2) and FIA_X509.2(1/2)** meet this objective by ensuring that both users and IT entities configured to communicate with the TOE are authenticated. **FTA_SSL.3** meets the objective by ensuring that sessions are terminated after a configurable time interval of inactivity. **FTA_TAB.1** 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** meets the objective by ensuring that the TOE will increase a delay between each successive failed login attempt on the management interfaces.

Objectives	SFRs
O.PROTCOMMS	**FCS_COP.1** meets this objective by ensuring that the TOE performs cryptographic operations in accordance with the FIPS 140-2 standard. **FIA_X509.1(2)** meets this objective by ensuring that the TOE uses X.509 certificates for TLS communications. **FIA_X509.2(2)** meets this objective by ensuring that the TOE uses X.509 for TLS authentication. **FPT_ITT.1** meets this objective by ensuring that the TOE encrypts communications between components in a federated (cluster) deployment. **FTP_ITC.1** meets this objective by ensuring that the TOE encrypts communications with an external LDAP server. **FTP_TRP.1** meets this objective by ensuring that the TOE encrypts communications with remote administrators.
O.RECOVERY	**FPT_RCV.1** meets the objective by ensuring that the TOE automatically recovers from a corruption in the firmware image using the stored recovery images.

Table 22: Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met
FAU_GEN.2	FAU_GEN.1	Met
	FIA_UID.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FAU_SAR.3	FAU_SAR.1	Met
FAU_STG.1	FAU_GEN.1	Met
FAU_STG.4	FAU_STG.1	Met
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Not met, as per scheme policy.
	FCS_CKM.4	Not met, as per scheme policy.
FDP_RIP.1	None	-
FIA_ATD.1	None	-
FIA_SOS.1	None	-

SFR	Dependency	Rationale
FIA_UAU.1	FIA_UID.1	Met
FIA_UAU.5	None	-
FIA_UAU.7	FIA_UAU.1	Met
FIA_UID.1	None	-
FIA_X509.1(1)	FIA_X509.2(1)	Met
FIA_X509.1(2)	FIA_X509.2(2)	Met
FIA_X509.2(1)	FIA_X509.1(1)	Met
FIA_X509.2(2)	FIA_X509.1(2)	Met
FMT_MTD.1	FMT_SMF.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met
FPT_ITT.1	None	-
FPT_RCV.1	AGD_OPE.1	Met
FPT_STM.1	None	-
FTA_SSL.3	None	-
FTA_TAB.1	None	-
FTA_TSE.1	None	-
FTP_ITC.1	None	-
FTP_TRP.1	None	-