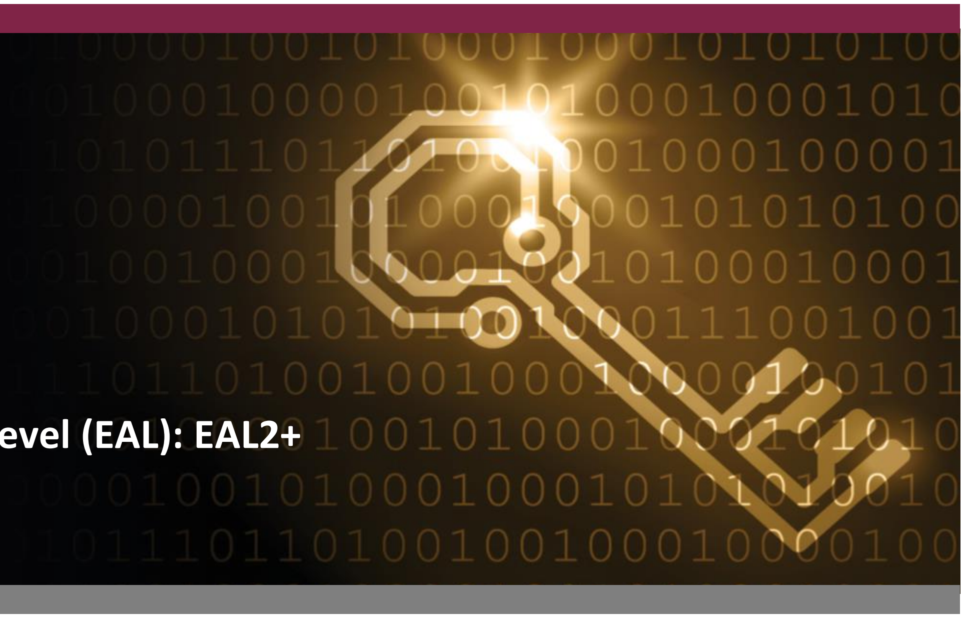
Hewlett Packard Enterprise Development LP

BladeSystem c-Class Enclosure Architecture

Including BladeSystem c7000 Enclosure, Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66

Security Target



Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.6

Prepared for:

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 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

List of Figures

List of Tables

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) BladeSystem c-Class Enclosure Architecture (BladeSystem) including BladeSystem c7000 enclosure, Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66, and will hereafter be referred to as the TOE throughout this document. The TOE is a rack-mountable system comprised of a BladeSystem enclosure, c-Class blade servers with iLO modules, OA management modules, VC interconnect modules, and all the power, cooling, and I/O[1] infrastructure needed to support them.

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 BladeSystem c-Class Enclosure Architecture including BladeSystem c7000 Enclosure, Integrated Lights-Out (iLO) 5 v1.11, Onboard Administrator (OA) v4.71, and Virtual Connect (VC) v4.66 Security Target

[1] I/O – Input/Output

ST Version	Version 0.6
ST Author	Corsec Security, Inc.
ST Publication Date	August 31, 2018
TOE Reference	HPE BladeSystem c-Class Enclosure Architecture including BladeSystem c7000 enclosure, iLO 5 v1.11, OA v4.71, and VC v4.66 with an iLO Advanced Premium Security Edition license
FIPS[2] 140-2 Status	iLO Level 1 FIPS-validated crypto module: Certificate No. 3122 OA Level 1 FIPS-validated crypto module: Certificate No. 3174 VC Level 1 FIPS-validated crypto module: Certificate No. N/A[3]

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.

1.3.1 BladeSystem c-Class Enclosure Architecture

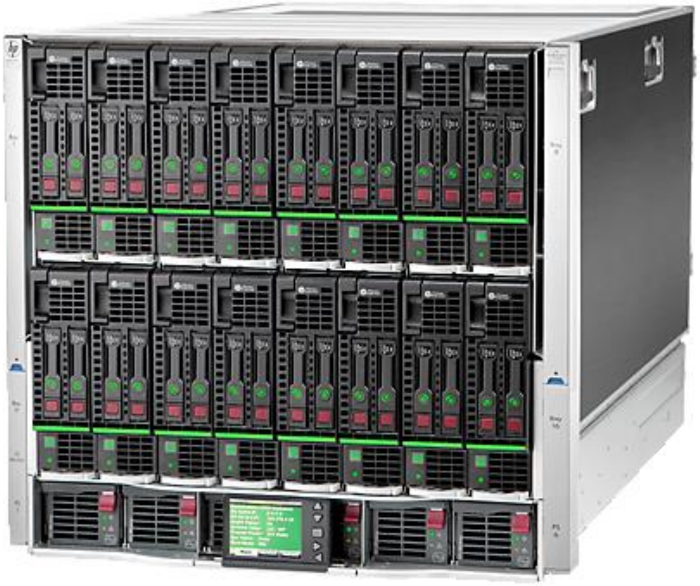


Figure 1 – HPE BladeSystem c7000 Enclosure (Example)

The BladeSystem c-Class Enclosure Architecture is implemented by the HPE BladeSystem c7000 enclosure, which is optimized for enterprise datacenter applications. Figure 1 above shows an example of a fully populated c7000 enclosure. The enclosures fit into standard 19-inch racks and it accommodates the BladeSystem c-Class blade servers with iLO modules, OA management modules, and VC interconnect modules. The enclosure also provides

[2] FIPS – Federal Information Processing Standard

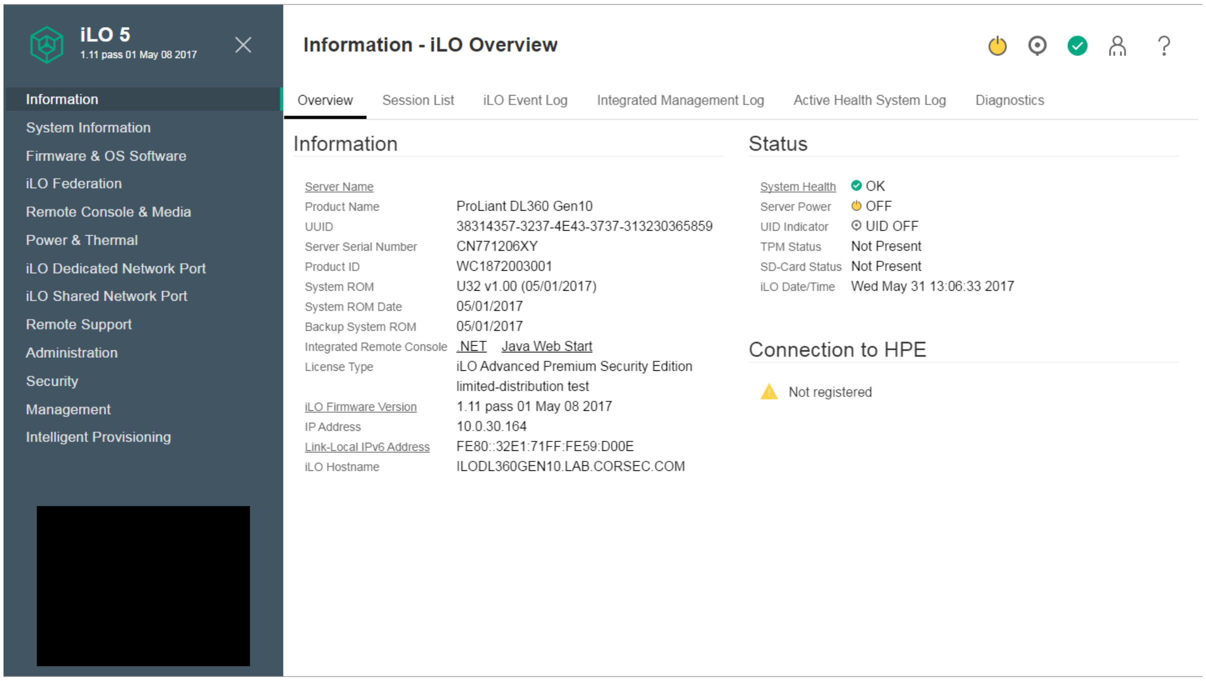
[3] Note that the VC Level 1 FIPS-validated crypto module v4.65 achieved certificate number 3173. VC firmware v4.66 was created to address a CVE making the CMVP validation inapplicable to this evaluation. VC still implements CAVP-validated algorithms for purposes of protecting TSF data.

all the power, cooling, and I/O infrastructure needed to support the modules. The c7000 enclosure can be populated with the following physical hardware components:

- Up to 8 full-height or 16 half-height blade servers per enclosure.
    - Each independent blade server provides support for running its own, unique instance of a general-purpose operating system (OS).
    - Blade servers can leverage their own local storage or they can be logically attached to a storage network to provide bootable storage media.
    - Blade servers include iLO technology (discussed below).
- Up to 2 OA management modules.
    - A second OA management module can be used for redundancy.
- Up to 8 VC interconnect modules.
    - The VC interconnect modules are used to simultaneously supporting a variety of network interconnect fabrics such as Ethernet, Fibre Channel (FC), InfiniBand, Internet Small Computer System Interface (iSCSI), or Serial-attached SCSI[4].
- Up to 10 Active Cool 200 fan kits.
- Up to 6 power supplies.

The c7000 enclosure include a shared 5-terabit-per-second, high-speed midplane for connection of blade servers to network and shared storage. A pooled-power backplane delivers power and ensures that the full capacity of the power supplies is available to all modules.

1.3.2 Integrated Lights-Out (iLO)



[redacted]

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 2 – iLO Management Screen (Example)

[4] SCSI – Small Computer Systems Interface

The HPE Integrated Lights-Out 5 (HPE iLO) 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[5] with true Agentless Management using SNMP[6] 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 also the foundation of BladeSystem High Availability (HA) embedded server and fault management. 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 2 above shows an example screenshot of the iLO management interface.

iLO 5 is supported on the HPE ProLiant Gen10 BL Blade Servers used within the BladeSystem c-Class Enclosure Architecture. Blade servers are small form factor servers that can be housed inside a BladeSystem enclosure, which is designed for modularity and high-density footprints allowing more servers in a smaller space. 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. Blade servers are designed so that administrative functions that are performed locally can also be performed remotely. 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[7] 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, usernames, 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

[5] Note that a system administrator is not a role or privilege level but can refer to any TOE user.
[6] SNMP – Simple Network Management Protocol
[7] IT – Information Technology

- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS[8] 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[9]. HPE ProLiant Gen10 servers with a 4GB[10] iLO NAND allow system administrators 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 firmware 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[11] service port on the front panel of the Gen10 servers. 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 the same iLO management interfaces without having to connect to the corporate network. While this does not require access to the network, it does require a valid username and password to log in 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 datacenters and remote locations.

1.3.3 Onboard Administrator (OA)

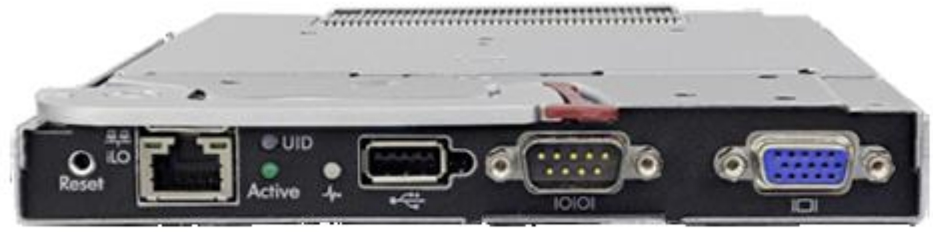


Figure 3 – HPE BladeSystem OA Module (Example)

The heart of the BladeSystem c-Class Enclosure Architecture is the OA module (shown in Figure 3 above). The OA module is located in the enclosure and is used to manage the enclosure. OA is a Linux-based appliance that performs four management functions for the entire enclosure:

- Detecting component insertion and removal

[8] BIOS – Basic Input/Output System
[9] NAND – Negated AND
[10] GB – Gigabyte
[11] USB – Universal Serial Bus

- Identifying components and required connectivity
- Managing power and cooling
- Controlling components

An optional second OA in the c7000 enclosure provides complete redundancy for these functions. The HPE BLc7000 OA with KVM[12] option is used within the BladeSystem c-Class Enclosure Architecture.

System administrators can access OA in the different ways: remotely through the OA Web GUI; remotely through the scriptable OA CLI; remotely through the OA SOAP[13] Interface; or through the built-in diagnostic LCD[14] panel included in the front of the c7000 enclosure.

The ERS options are available through OA when using IRS in the environment. When configured, information about the c-Class enclosure is sent to HPE either directly or through an IRS centralized hosting device in the local IT environment.

OA also allows IPv6[15] addresses to be assigned when associated features are enabled and multiple addresses are supported.

1.3.3.1 Managing power and cooling

The most important OA tasks are power control and thermal management. OA can remotely control the power state of all components in BladeSystem c-Class Enclosure Architecture. For servers in the front device bays of an enclosure, OA communicates with the each server's iLO module to control the server and its communications.

Once components are granted power, OA begins its thermal management process with Thermal Logic. The Thermal Logic feature in the BladeSystem c-Class Enclosure Architecture minimizes fan's power consumption by reading numerous sensors located throughout the enclosure. Thermal Logic also adjusts fan speeds of the 4 different cooling zones within the enclosure to minimize power consumption and maximize cooling efficiency.

1.3.3.2 Controlling components

OA uses embedded management interfaces to provide the health status of and detailed information about all bays in the enclosure. OA also reports the firmware versions of various components in the enclosure and updates those components if a system administrator desires to change the component's firmware.

1.3.3.3 Internal management interfaces

OA monitors and communicates with each bay in the enclosure via several hardware interfaces. The management hardware interfaces include unique presence pins[16]as well as Inter-Integrated Circuit (I2C), serial, and Ethernet connections. These management interface connections are completely isolated from the blade server connections and are only accessible within the enclosure's private management network through logically separated management channels.

[12] KVM – Keyboard-Video-Mouse
[13] SOAP – Simple Object Access Protocol
[14] LCD – Liquid Crystal Display
[15] IPv6 – Internet Protocol Version 6
[16] Unique presence pins – Used to detect whether a component is installed within a particular bay

1.3.3.4 External management interfaces

Each enclosure has several external management interfaces connected to OA. The primary external management interface is the management port for each OA, which is an RJ-45 [17] jack. This port provides Ethernet communications not only to each OA, but also to every device bay with a management processor. This includes iLO communication for the blade servers and any VC interconnect module using the c-Class embedded Ethernet management network. For redundant OAs, both OA management ports are connected to the management network, providing redundant management network connections to each enclosure.

A serial port on each OA module provides full out-of-band CLI access to OA and is used for OA firmware flash recovery. USB ports on the OA module are used for recovering or writing enclosure configuration to or from a USB flash drive or for supplying firmware images. The USB ports are also used to connect DVD[18] drives to the enclosure as an alternative to using the enclosure's built-in DVD drive.

1.3.3.5 Redundant enclosure management

Redundant enclosure management is an optional feature of the c7000 enclosure. It requires installation of a second OA module to act as a completely redundant controller in an active-standby mode. Using redundant OA modules provides complete fault tolerance. The redundancy logic is based on a continuous heartbeat between the two modules over a dedicated serial connection. If the period between heartbeats exceeds a timeout, the standby module automatically takes control of the enclosure and becomes the active OA.

1.3.3.6 Insight Remote Support

When a c-Class enclosure is registered with an IRS server using the ERS options, the OA module sends information about the shared infrastructure components within the enclosure to the IRS server that is located at HPE or inside the IT environment. The following information is sent over an HTTPS[19] connection:

- Registration – Data that uniquely identifies the enclosure hardware. Examples of data that is collected include:
  - Enclosure name
  - Enclosure product name
  - Enclosure part number
  - Enclosure serial number
  - Enclosure manufacturer name
  - Onboard Administrator firmware version
  - Onboard Administrator IP and MAC[20] addresses
- Service events – Data to uniquely identify the relevant hardware component. Examples of data that is collected include:
  - Enclosure model
  - Enclosure serial number
  - Part number of the relevant hardware component
  - Description, location, and other identifying characteristics of the relevant hardware component
- Data collections – Data used to enable proactive advice and consulting. Information about the enclosure hardware as well as populated system components including the LCD module, OA modules, enclosure fan

[17] RJ – Registered Jack
[18] DVD – Digital Versatile Disc
[19] HTTPS – Hypertext Transport Protocol Secure
[20] MAC – Media Access Control

modules, enclosure power supply modules, VC interconnect modules, and blade servers is sent. Examples of data that is collected for these system components include:

- Hardware module descriptors such as manufacturer, product name, serial number, UUID[21], part number, and location within the enclosure
- Firmware revision
- Diagnostic and status information
- Power and thermal configuration and status information
- Network and port mapping information

1.3.3.7 IPv6

OA supports the use of IPv6 when choosing a protocol for the enclosure. When enabled, the IPv6 settings support multiple addresses. OA can have both automatically-assigned IP addresses and user-specified static IP addresses. The IPv6 Settings screen gives you additional choices, some of which are unique to IPv6.

1.3.4 Virtual Connect (VC)

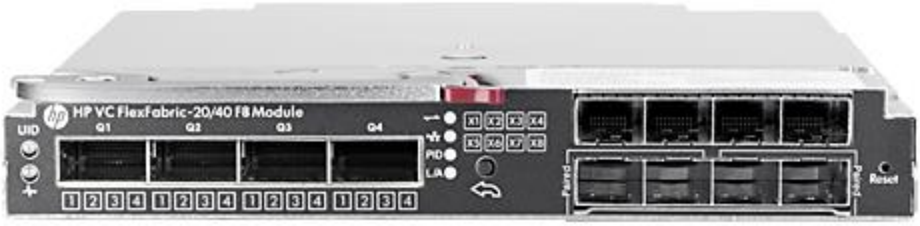


Figure 4 – HPE BladeSystem VC Module (Example)

VC technology is a set of interconnect modules and embedded software for the BladeSystem c-Class Enclosure Architecture. VC simplifies the setup and administration of server connections. Figure 4 above shows an example of a VC module. The HPE VC FlexFabric-20/40 F8 for c-Class BladeSystem with TAA[22] module is used within the BladeSystem c-Class Enclosure Architecture.

VC-Enet[23] modules enable connectivity to datacenter Ethernet switches. VC-Enet modules can also be directly connected to other types of devices, such as printers, laptops, rack servers, and network storage devices. VC Manager (VCM) is embedded on VC-Enet modules and is accessed through a VC Web GUI, VC CLI, or VC SOAP Interface. These interfaces are also accessible from OA. FlexFabric modules enable connectivity of the enclosure to datacenter FC switches. Every FC fabric is limited in the number of switches it can support, but the FlexFabric modules do not appear as switches to the FC fabric and do not count against FC fabric limits.

VC offers a unique approach to connecting and adapting server, LAN[24], and SAN[25] domains across the datacenter. When the LAN and SAN connections are made available to the pool of servers within the enclosure, the system administrator uses VCM to define a server connection profile for each server. The server connection profile is an

[21] UUID – Universally Unique Identifier
[22] TAA – Trade Agreement Act
[23] Enet – Ethernet
[24] LAN – Local Area Network
[25] SAN – Storage Area Network

interconnect option for the BladeSystem that is designed to simplify the connection of blade servers to datacenter networks. System administrators can automatically manage resources independent of server connections to network and storage resources in a BladeSystem, saving administrative time and effort.

VC enables a system administrator to connect and pre-assign all the LAN and SAN connections that the server pool might need. Using VC FlexFabric modules, system administrators can choose how many NICs[26] or HBAs[27] are on each server and dynamically set the bandwidth of each connection in increments of 100 Mb[28] between 100 Mb and 20 Gb[29].

Like other Ethernet and FC switches, VC modules slide into the interconnect bays of BladeSystem c-Class Enclosure Architecture. The VCM software runs on a processor that resides on the VC module. Together, VC modules and the VCM allow a system administrator to create a change-ready infrastructure to add, move, and recover servers across the datacenter without impacting production LANs and SANs.

VC modules can be administered in two ways: directly, via the VC Web GUI, VC CLI, or VC SOAP Interface; and indirectly, via an OA module installed in the BladeSystem enclosure.

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.

The hardware/firmware TOE is the HPE BladeSystem c-Class Enclosure Architecture. In the evaluated configuration, the TOE is comprised of a BladeSystem c7000 rack-mountable enclosure, one or more OA modules, one or more VC modules, one or more blade servers that include iLO functionality, one or more power supplies, and one or more fan units.

Table 2 below lists the hardware components' versions and the corresponding firmware included in the evaluated configuration of the TOE.

Table 2 – Evaluated Hardware Versions

Component	Version
BladeSystem Enclosure	HPE BladeSystem c7000 Enclosure with up to 10 Active Cool 200 fan kits and up to 6 power supplies
iLO/Blade Server	HPE iLO 5 GXP ASIC[30] model number 815393-001-B1 with an Advanced Premium Security Edition license running firmware version 1.11 on the HPE ProLiant Gen10 BL460c blade server
OA	HPE BLc7000 OA with KVM option running firmware version 4.71
VC	HPE VC FlexFabric-20/40 F8 for c-Class BladeSystem with TAA module running firmware version 4.66

[26] NIC – Network Interface Card
[27] HBA – Host Bus Adapter
[28] Mb – Megabit
[29] Gb – Gigabit
[30] ASIC – Application Specific Integrated Circuit

The TOE is managed by appropriately privileged system administrators through the interfaces provided by iLO, OA, and VC. To remotely access the functions available via these interfaces, a system administrator must use a web browser, a SSH[31] client, or external software to enter the IP address or hostname of iLO, OA, or VC. A system administrator may also manage the TOE locally over a serial connection.

Figure 5 below shows the details of the deployment configuration of the TOE. The following previously undefined acronyms are used in Figure 5:

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

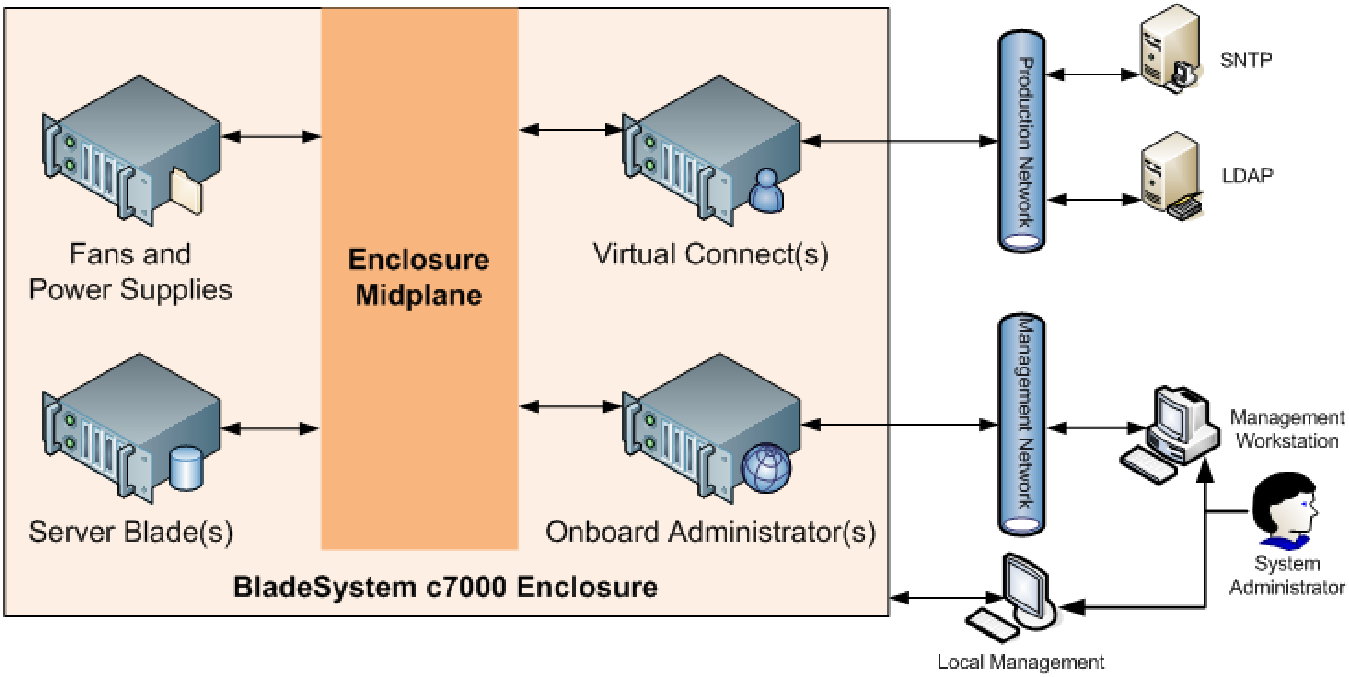


Figure 5 – Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE is intended to be deployed in a secure datacenter that protects physical access to the TOE. The TOE is intended to be connected to a secure 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. Table 3 lists the server requirements to setup the TOE Environment:

Table 3 – TOE Environment

Device	Requirement
LDAP Server	LDAPv3 (RFC[32] 4511)

[31] SSH – Secure Shell

[32] RFC – Request for Comments

Device	Requirement
SNTP Server	SNTPv4 (RFC 5905)

The LDAP server is used by iLO, OA, and VC for authenticating and identifying system administrators to assign their required roles. Communications for the LDAP server are sent over TLS[33]. An SNTP server will be used by iLO to synchronize the internal clock with a reliable time source.

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

- Java Runtime Environment – Minimum version of 8 Update 121; Recommended to use the latest version
- Adobe Flash Player – Minimum version of 11.2; Recommended to use the latest version
- Microsoft .NET Framework – Minimum version of the 3.5; Recommended to use version 4.6
- At least one of the following supported web browsers:
    - For OA interfaces:
        - Microsoft Internet Explorer 11.0.96
        - Mozilla Firefox 50.1.0
        - Google Chrome (latest version)
    - For iLO interfaces:
        - Microsoft Internet Explorer 11.x
        - Microsoft Edge (latest version)
        - Mozilla Firefox (latest version)
        - Google Chrome (latest version)
    - For VC interfaces:
        - Microsoft Internet Explorer 11.0.35
        - Mozilla Firefox ESR[34] 45.7
        - Mozilla Firefox 51.0.1

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 6 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- BladeSystem c7000 enclosure and support hardware (such as fans and power supplies)
- OA hardware and firmware v4.71 in *.BIN format
- VC hardware and firmware v4.66 in *.BIN format

[33] TLS – Transport Layer Security

[34] ESR – Extended Support Release

- Blade Server hardware
    - To host the iLO 5 hardware and firmware v1.11 in *.BIN format after extracting it from the *.EXE
- TOE Environment servers listed in Section 1.4.1
- External network(s) (not included in the TOE boundary)

After ordering TOE hardware through the HPE website or by contacting a sales representative directly, HPE will use a secured third-party shipping company to deliver the product. The primary shippers are DHL and FedEx. Firmware will already be installed on the delivered hardware but if needed, the evaluated version of firmware for each component is available on the HPE website.

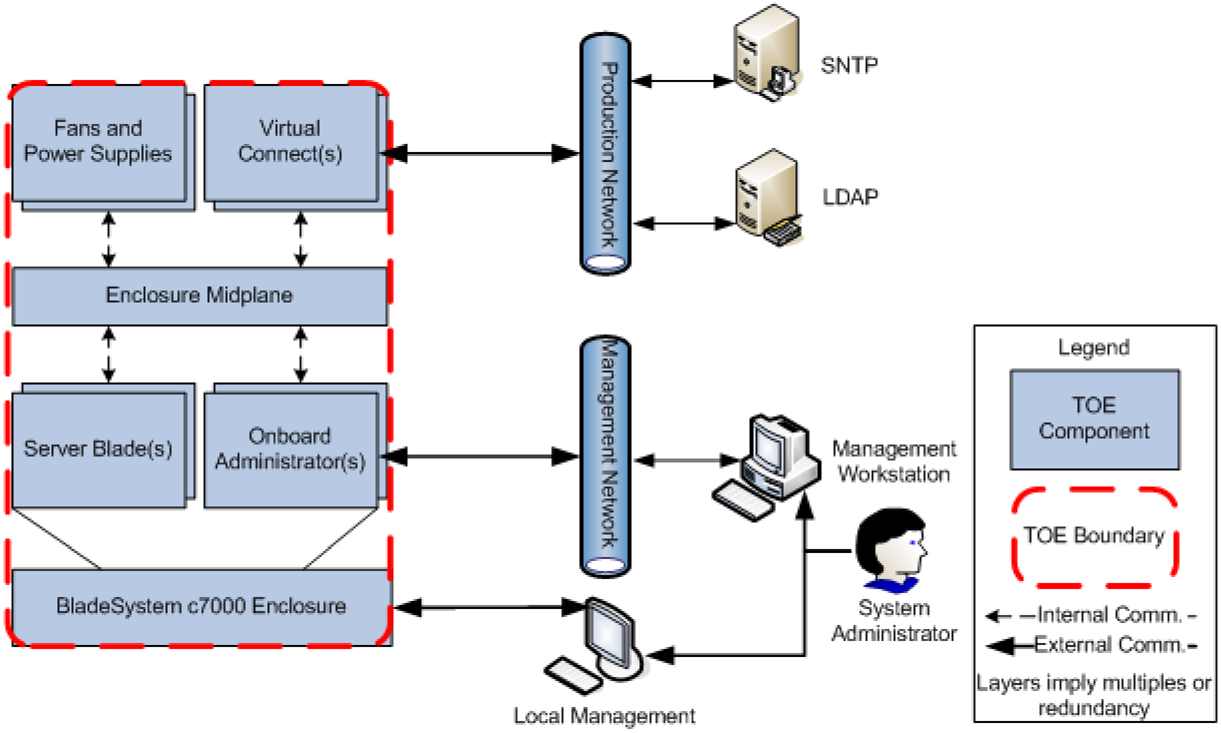


Figure 6 – Physical TOE Boundary

1.5.1.1 Guidance Documentation

The following PDF formatted guides, that are available for download through the HPE website, are required reading and part of the TOE:

- *Architecture and Technologies in the HPE BladeSystem c7000 Enclosure*; HPE Part Number: 4AA4-8125ENW; Published: July 2017, Rev. 3
- *HPE BladeSystem c7000 Enclosure Quick Setup Instructions*; HPE Part Number: 411762-404; Published: February 2015; Edition: 13
- *HPE BladeSystem c7000 Enclosure Setup and Installation Guide*; HPE Part Number: 411272-401R; Published: November 2015; Edition: 11
- *HPE BladeSystem c-Class Solution Overview*; HPE Part Number: 413339-006; Published: March 2012; Edition: 6
- *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy*; Part Number: 873901-002; Published: July 2017; Edition: 1

- *HPE ProLiant BL460c Gen10 Server Blade User Guide*; Part Number: 876833-001; Published: July 2017; Edition: 1
- *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 881334-001; Published: July 2017; Edition: 1
- *HPE BladeSystem Onboard Administrator Command Line Interface User Guide*; Part Number: 695523-401; Published: July 2017; Edition: 29
- *HPE BladeSystem Onboard Administrator User Guide*; Part Number: 695522-402; Published: June 2017; Edition: 28
- *HPE BladeSystem c-Class Virtual Connect Support Utility Version 1.13.5 User Guide*; Part Number: 859819-004; Published: September 2018; Edition: 1
- *HPE Virtual Connect for c-Class BladeSystem Setup and Installation Guide Version 4.65/4.66*; Part Number: P01610-002; Published: September 2018; Edition: 1
- *HPE Virtual Connect for c-Class BladeSystem User Guide Version 4.65/4.66*; Part Number: P01611-002; Published: September 2018; Edition: 1
- *HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide Version 4.65/4.66*; Part Number: P01609-002; Published: September 2018; Edition: 1
- *HPE ProLiant Gen9 Troubleshooting Guide Volume II: Error Messages*; Part Number: 795673-004; Published: July 2016; Edition: 5
- *Hewlett Packard Enterprise Development LP; BladeSystem c-Class Enclosure Architecture; Guidance Documentation Supplement*; Evaluation Assurance Level (EAL): EAL2+; Document Version: 0.4

The following PDF formatted guides, that are available for download through the NIST[35] CMVP[36] website, are required reading and part of the TOE:

- *Hewlett Packard Enterprise Development LP; iLO 5 Cryptographic Module; FIPS 140-2 Non-Proprietary Security Policy*; FIPS Security Level: 1; Document Version: 1.0
- *Hewlett Packard Enterprise Development LP; HPE BladeSystem c-Class Onboard Administrator Firmware; FIPS 140-2 Non-Proprietary Security Policy*; FIPS Security Level: 1; Document Version: 1.2
- *Hewlett Packard Enterprise Development LP; HPE BladeSystem c-Class Virtual Connect Firmware; FIPS 140-2 Non-Proprietary Security Policy*; FIPS Security Level: 1; Document Version: 0.7

The following web-based guides, that are available through the GitHub website, are required reading and part of the TOE:

- *iLO RESTful[37] API[38] Document*; https://hewlettpackard.github.io/ilo-rest-api-docs/ilo5/

[35] NIST – National Institute of Standards and Technology
[36] CMVP – Cryptographic Module Validation Program
[37] REST – Representational State Transfer
[38] API – Application Programming Interface

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes that 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:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[39]
- Resource Utilization
- TOE Access

1.5.2.1 Security Audit

The TOE generates audit records for the start-up and shutdown of the audit function, all administrative events, critical system events, and status events. System administrators are able to review all audit records, and the TOE prevents all unauthorized modification and deletion of audit records. When the audit trail reaches capacity, the oldest records are overwritten with new records.

1.5.2.2 Cryptographic Support

The TOE contains two FIPS 140-2 validated cryptographic modules that implement the AES[40], 3DES[41], SHA[42], RSA[43], and DSA[44] algorithms for iLO and OA. In addition, VC uses algorithms that are Cryptographic Algorithm Validation Program (CAVP) validated against FIPS 140-2 requirements. These cryptographic algorithms are used to secure management traffic between the system administrators and the TOE. Communications sent to the LDAP server are also secured using the TOE's cryptographic modules.

1.5.2.3 User Data Protection

When iLO, OA, or VC are reset to factory defaults, or when a FIPS mode of operation is instantiated, all authentication information and device settings are cleared from storage except for the OA's default Administrator account's password. The Lost Password/Flash Disaster Recovery (LP/FDR) mode must be used to clear the OA's default Administrator account's password

The TOE enforces three Security Functional Policies (SFPs):

- Management Access Control SFP
- VC Information Flow Control SFP
- iLO Information Flow Control SFP

[39] TSF – TOE Security Functionality
[40] AES – Advanced Encryption Standard
[41] 3DES – Triple Data Encryption Standard
[42] SHA – Secure Hash Algorithm
[43] RSA – Rivest, Shamir, Adleman
[44] DSA – Digital Signature Algorithm

The Management Access Control SFP ensures that only authorized and appropriately privileged system administrators can access or configure the TOE. The VC Information Flow SFP ensures that blade servers within the enclosure communicate only with other internal blade servers or entities on the external network(s) for which they have been configured by a system administrator to communicate with. The iLO Information Flow Control SFP ensures that only appropriately privileged system administrators are allowed to use the iLO functionality of installed blade servers.

1.5.2.4 Identification and Authentication

The OA and VC components have a minimum password complexity and length specified for authentication. The iLO component has a minimum password length specified for authentication. The TOE provides CHIF[45] commands, enclosure information, and access to the help links before a system administrator is authenticated by the TOE. All system administrators must successfully identify and authenticate before they are allowed to take any other administrative actions on the TOE. Using the LDAP server, the TOE is able to identify and authenticate system administrators that use directory services.

1.5.2.5 Security Management

The TOE allows only authenticated system administrators to access the TOE management interfaces, and access to specific functionality via those interfaces is only granted to appropriately privileged system administrators.

System administrators of the TOE can be authenticated directly by the TOE using a username and password. System administrators of the TOE can also be authenticated by a separate LDAP server. The LDAP server would manage the groups associated to the “privilege levels” (or roles) of OA and iLO, which control access to TSF functionality. System administrators are assigned a privilege level and are also bound to an arbitrary number of BladeSystem components and features over which they can exercise their assigned privilege level. This functionality is mediated by the OA or VC component through the enforcement of the Management Access Control SFP (detailed in section 1.5.2.3 above). To access iLO’s management functions, OA provides a login bypass feature for authenticated system administrators; however, iLO also provides its own set of local accounts and privilege levels to authenticate system administrators directly interfacing with it, and it can also be configured to leverage existing LDAP repositories.

1.5.2.6 Protection of the TSF

The TOE implements numerous self-tests to ensure that both the cryptographic functionality of the TOE and the BladeSystem components composing the TOE are functioning correctly. The TOE can also detect when a BladeSystem component is tampered with, when a component fails, and when a new BladeSystem component is added to the enclosure. It can alert the system administrators when these events occur. If a BladeSystem component fails, and if a comparable failover-ready component is installed, the TOE automatically fails-over to use the other component, thus providing uninterrupted service.

The iLO, OA, and VC components each provide reliable time stamps. iLO will be synchronized to an SNTP server for a reliable time stamp.

1.5.2.7 Resource Utilization

If a BladeSystem component fails, and if a comparable failover-ready component is installed, the TOE automatically fails-over to use the other component, thus ensuring the TOE’s operations during the failure.

[45] CHIF – Host Channel Interface

1.5.2.8 TOE Access

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

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:

- Use of any SNMP functionality
- XML[46] Reply
- iLO and VC System Maintenance Switches
- ProLiant Blade Server operating systems
- Utility Ready Blades (URB)
- Insight Display and KVM (locked in FIPS mode)
- HPE Online Configuration Utility (HPONCFG)
- HPE Insight Online connecting to an IRS device
- iLO iOS[47] application
- iLO Android application
- Using the iLO service port for mass storage
- OA running with IPv6 enabled

[46] XML – eXtensible Markup Language
[47] iOS – iDevice Operating System

2. Conformance Claims

This section and Table 4 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 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[48] as of February 21, 2018 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)

[48] CEM – Common Evaluation Methodology

3. Security Problem

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

- Known and presumed threats countered by either the TOE or by the security environment
- 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 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.CONFIG	An unauthorized user or attacker, who is not a system administrator, could improperly gain access to user data if the product is misconfigured or does not enforce proper roles and permissions.
T.FAILURE_OR_TAMPER	Physical failure or tampering of a TOE component, by an unauthorized user or attacker, could go undetected or could cause a breach of the TSF.
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 could access data stored by the TOE by bypassing the protection mechanisms of the TOE.

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 6 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 6 – 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 7 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 7 – Assumptions

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

4. Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 8 below.

Table 8 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must ensure that only authorized system administrators may access and configure the product.
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 and the identified system administrator (if applicable). The TOE must also provide the authorized system administrators with the ability to review the audit trail and 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 system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must handle idle sessions and failed login attempts in a secure manner.
O.FAILURE_OR_TAMPER	The TOE must ensure that TSF services continue to be offered in case of physical component failure. The TOE must also ensure that physical tampering with (removal of) physical components is detected and system administrators are informed.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 9 below lists the IT security objectives that are to be satisfied by the environment.

Table 9 – IT Security Objectives

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

4.2.2 Non-IT Security Objectives

Table 10 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 10 – Non-IT Security Objectives

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

5. Extended Components

There are no extended SFRs or extended SARs for this evaluation of the TOE.

6. Security Requirements

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

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the 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 [<u>underlined text within brackets</u>].
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	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_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_IFC.1(a)	Subset information flow control (VC to Blade Server)		✓		✓
FDP_IFC.1(b)	Subset information flow control (OA to iLO)		✓		✓
FDP_IFF.1(a)	Simple security attributes (VC to Blade Server)		✓		✓
FDP_IFF.1(b)	Simple security attributes (OA to iLO)		✓		✓

Name	Description	S	A	R	I
FDP_RIP.1	Subset residual information protection	✓	✓		
FIA_SOS.1(a)	Verification of secrets (iLO)		✓		✓
FIA_SOS.1(b)	Verification of secrets (OA and VC)		✓		✓
FIA_UAU.1	Timing of authentication		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_PHP.2	Notification of physical attack		✓		
FPT_RCV.2	Automated recovery		✓		
FPT_STM.1	Reliable time stamps				
FPT_TST.1(a)	TSF testing (Cryptographic module)	✓	✓		✓
FPT_TST.1(b)	TSF testing (BladeSystem components)	✓	✓		✓
FRU_FLT.2	Limited fault tolerance		✓		
FTA_SSL.3	TSF-initiated termination		✓		
FTA_TAB.1	Default TOE access banners				
FTA_TSE.1	TOE session establishment		✓		

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, OA, and VC 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_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_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

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 12*] and specified cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 12*] that meet the following: [*FIPS 197, FIPS 198, SP*[49] *800-67, SP 800-56A, SP 800-90A, FIPS 180-4, and FIPS 186-4*].

***Application Note**: iLO and OA both implement CMVP validated modules. The VC firmware changed from v4.65 to v4.66 to address a CVE, making the CMVP validation inapplicable to this evaluation. VC still implements CAVP-validated algorithms for purposes of protecting TSF data. Therefore, FCS_CKM.1 is not applicable to VC following the guidance of CCS Instruction #4.*

[49] SP – Special Publication

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*].

Application Note*: iLO and OA both implement CMVP validated modules. The VC firmware changed from v4.65 to v4.66 to address a CVE, making the CMVP validation inapplicable to this evaluation. VC still implements CAVP-validated algorithms for purposes of protecting TSF data. Therefore, FCS_CKM.4 is not applicable to VC following the guidance of CCS Instruction #4.*

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 12*] in accordance with a specified cryptographic algorithm [*listed in the 'Algorithm' column of Table 12*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 12*] that meet the following: [*FIPS 140-2*].

Table 12 – Cryptographic Algorithm and Key Sizes for iLO, OA, and VC

Module	Algorithm	Key Sizes (bits)	Cryptographic Operation	Certificate No.
iLO	AES – CBC[50], OFB[51], and CTR[52] mode	128, 192, 256	Encryption/Decryption	4525
	AES – GCM[53] mode	128, 192, 256	Encryption/ Decryption/ Generation/ Verification/ Message Authentication	4525
	3DES – CBC mode	(3) 56	Encryption/Decryption	2412
	RSA	2048, 3072	Key Generation/ Signature Generation	2462
	RSA	1024, 1536, 2048, 3072, 4096	Signature Verification	2462
	DSA	2048, 3072	Key Generation/ Signature Generation/ Signature Verification	1204
	ECDSA[54] for P-256 and P-384 curves	256, 384	Public Key Generation/ Public Key Verification/ Signature Generation/ Signature Verification	1100

[50] CBC – Cipher Block Chaining
[51] OFB – Output Feedback
[52] CTR – Counter Mode
[53] GCM – Galois/Counter Mode
[54] ECDSA – Elliptic Curve Digital Signature Algorithm

Module	Algorithm	Key Sizes (bits)	Cryptographic Operation	Certificate No.
	ECC[55] CDH[56] for P-224 and P-384 curves	256, 384	ECC CDH Primitive	1201
	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	Message Digest	3706
	HMAC[57]-SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	Message Authentication	2985
	CTR DRBG[58] (AES)	N/A[59]	Random Number Generation	1485
OA	AES – CBC, CTR, ECB[60] mode	128, 192, 256	Encryption/Decryption	4776
	AES – CFB[61]128 mode	128	Encryption/Decryption	4776
	AES – GCM mode	128, 256	Encryption/Decryption/ Authentication	4776
	3DES – CBC, ECB mode	(3) 56	Encryption/Decryption	2538
	RSA FIPS PUB 186-4	2048	Key Generation/ Signature Generation/ Signature Verification	2617
	RSA FIPS PUB 186-2	2048	Signature Verification	2617
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160, 224, 256, 384, 512	Message Digest	3920
	SHA-1	160	Message Digest	3921
	SHA-256	256	Message Digest	3922
	HMAC SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	160, 224, 256, 384, 512	Message Authentication	3186
	CTR DRBG (AES)	N/A	Random Number Generation	1654
VC	AES – CBC, CTR mode	128, 192, 256	Encryption/Decryption	4777
	AES – CFB128 mode	128	Encryption/Decryption	4777
	AES – GCM mode	128, 256	Encryption/Decryption/ Authentication	4777
	AES – KW[62]	128, 192, 256	Key Wrapping/Unwrapping	4777
	3DES – CBC mode	(3) 56	Encryption/Decryption	2539
	RSA FIPS PUB 186-4	2048	Key Generation/ Signature Generation/ Signature Verification	2618
	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	Message Digest	3923
	HMAC SHA-256, SHA-384, SHA-512	256, 384, 512	Message Authentication	3187
	CTR DRBG (AES)	N/A	Random Number Generation	1655

[55] ECC – Elliptic Curve Cryptography
[56] CDH – Cofactor Diffie-Hellman
[57] HMAC – Hash-based Message Authentication Code
[58] DRBG – Deterministic Random Bit Generator
[59] N/A – Not Applicable
[60] ECB – Electronic Codebook
[61] CFB – Cipher Feedback
[62] KW – Key Wrap

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Management Access Control SFP*] on [

- *Subjects: System administrators*
- *Objects: iLO components, OA components, and VC components*
- *Operations: Access and configure*].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

The TSF shall enforce the [*Management Access Control SFP*] to objects based on the following: [

- *Subjects attributes:*
  - *Username*
  - *Privilege level*
  - *Component assignments*
- *Object attributes:*
  - *Component identifier*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a valid subject of the TOE is allowed to access or configure an object if the subject has a privilege level that allows the operation and a component assignment that binds the subject to the object*].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*None*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*None*].

FDP_IFC.1(a) Subset information flow control (VC to Blade Server)

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(a).1

The TSF shall enforce the [*VC Information Flow Control SFP*] on [

- *Subjects: BladeSystem blade servers, external servers, and workstations*
- *Information: Network data*
- *Operations: Transmit*].

FDP_IFC.1(b) Subset information flow control (OA to iLO)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(b).1

The TSF shall enforce the [*iLO Information Flow Control SFP*] on [

- *Subjects: OA system administrators*
- *Information: BladeSystem blade server iLO data*
- *Operations: Transmit*].

FDP_IFF.1(a) Simple security attributes (VC to Blade Server)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1(a).1

The TSF shall enforce the [*VC Information Flow Control SFP*] based on the following types of subject and information security attributes: [

- *Subject attributes:*
  - *Unique subject identifier*
- *Information attributes:*
  - *Unique source identifier*
  - *Unique destination identifier*].

FDP_IFF.1(a).2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*a unique subject is allowed to transmit data to another unique subject via the VC component only if the system administrator configurable rule for that unique source identifier or unique destination identifier permits communication*].

FDP_IFF.1(a).3(a)

The TSF shall enforce the [*information flow so that data tagged with a unique destination identifier will be forwarded to only the interfaces configured with the same destination identifier*].

FDP_IFF.1(a).3(b)

The TSF shall enforce the [*distinct separation of data traffic so that it is not interfered with by any other data traffic when it is within the TOE's scope of control*].

FDP_IFF.1(a).4

The TSF shall explicitly authorize an information flow based on the following rules: [*None*].

FDP_IFF.1(a).5

The TSF shall explicitly deny an information flow based on the following rules: [*None*].

FDP_IFF.1(b) Simple security attributes (OA to iLO)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1(b).1

The TSF shall enforce the [*iLO Information Flow Control SFP*] based on the following types of subject and information security attributes: [

- *Subject attributes:*
    - *OA system administrator unique identifier*
    - *OA system administrator component assignment*
- *Information attributes:*
    - *BladeSystem blade server unique identifier*].

FDP_IFF.1(b).2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*an OA system administrator is allowed to transmit iLO data to a BladeSystem blade server via the OA component based on the OA system administrator unique identifier, OA system administrator component assignment, the BladeSystem blade server unique identifier, and if the OA configuration allows the system administrator and blade server to communicate*].

FDP_IFF.1(b).3

The TSF shall enforce the [*None*].

FDP_IFF.1(b).4

The TSF shall explicitly authorize an information flow based on the following rules: [*None*].

FDP_IFF.1(b).5

The TSF shall explicitly deny an information flow based on the following rules: [*None*].

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 [<u>deallocation of the resource from</u>] the following objects: [*authentication information and settings for each iLO, OA, and VC module*].

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1(a) Verification of secrets (iLO)

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.1(a).1

The TSF shall provide a mechanism to verify that secrets meet [*a configurable minimum character length for the iLO interfaces.*].

FIA_SOS.1(b) Verification of secrets (OA and VC)

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.1(b).1

The TSF shall provide a mechanism to verify that secrets meet [*a configurable minimum character length for the OA and VC interfaces. Additionally, the OA and VC mechanisms shall verify that secrets contain at least one character from three of the four following categories: Uppercase, Lowercase, Numeric, Non-alphanumeric*].

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[63] milestone)*
  - *0x0140/0x8140 (Get iLO certificate)*
  - *0x0141/0x8141 (Set encryption key and iv[64])*
  - *0x0FFF/0x8FFF (Echo)*
- *The use of the help link on the OA Web GUI's login page (depicted as a question mark "?" in a box)*
- *The use of the enclosure information table displayed on the OA Web GUI login page*
- *The use of the "Sign-in help" link on the VC Web GUI's login page*

] 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_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)*
  - *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)*
- *The use of the help link on the OA Web GUI's login page (depicted as a question mark "?" in a box)*
- *The use of the enclosure information table displayed on the OA Web GUI login page*
- *The use of the "Sign-in help" link on the VC Web GUI's login page*

] on behalf of the user to be performed before the user is identified.

[63] ROM – Read Only Memory

[64] IV – Initialization Vector

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 Behavior Permissions' column of Table 13*] to [*the authorized identified roles listed under the 'Role/Privilege Level' column of Table 13*].

Table 13 – Management of Security Functions Behavior by Role

Module	Role/Privilege Level	Security Functions Behavior Permissions
iLO	Administer User Accounts	Determine the behavior of, disable, enable, or modify the behavior of the local accounts.
	Virtual Media and Configure iLO Settings	Modify the behavior of the server boot order.
	Configure iLO Settings	Modify the behavior of the power restore settings and idle timeouts
	Configure iLO Settings	Determine the behavior of, disable, enable, or modify the behavior of the IPv4[65]/IPv6, directory service, SNMP, and authentication settings.
	Configure iLO Settings	Disable, enable, or modify the behavior of the port, serial CLI, and login banner settings.
	Configure iLO Settings	Disable or enable the option to require login for the iLO UEFI[66]/RBSU[67] Interface.
OA	Administrator	Determine the behavior of, disable, enable, or modify the behavior of all configuration and TOE functions. This includes configuration, firmware updates, account management, and restoring factory default settings.
	Operator	Determine the behavior of, disable, enable, or modify the behavior of the configuration settings and viewing of all information.
VC	Domain	Determine the behavior of, disable, enable, or modify the behavior of the local accounts, roles, enclosures, VC domains, domain IP address, SSL[68] certificates, and SNMP settings.
	Network	Determine the behavior of, disable, enable, or modify the behavior of the network settings and network configurations.
	Storage	Determine the behavior of or modify the behavior of the World Wide Name (WWN) to be used by the domain.
	Storage	Determine the behavior of, disable, enable, or modify the behavior of the connections to external fabrics

[65] IPv4 – Internet Protocol Version 4
[66] UEFI – Unified Extensible Firmware Interface
[67] RBSU –ROM-Based Setup Utility
[68] SSL – Secure Sockets Layer

Module	Role/Privilege Level	Security Functions Behavior Permissions
	Server	Determine the behavior of, disable, enable, or modify the behavior of the server VC profiles, profiles assignments, server power settings.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Management Access Control SFP, iLO Information Flow Control SFP, and VC Information Flow Control SFP*] to restrict the ability to [change_default, query, modify, delete, [create]] the security attributes [*listed in the 'Security Attributes Access' column of Table 14*] to [*the authorized identified roles listed under the 'Role/Privilege Level' column of Table 14*].

Table 14 – Management of Security Attributes

Module	Role/Privilege Level	Security Attribute Access	Access Type
iLO	Administrator	OA system administrator unique identifier	Change default Query Modify Delete Create
		Privilege level	Change default Query Modify Delete Create
		OA system administrator component assignment	Change default Query Modify Delete Create
	Operator	OA system administrator unique identifier	Query
		Privilege level	Query
		OA system administrator component assignment	Query
	User	OA system administrator unique identifier	Query
		Privilege level	Query
		OA system administrator component assignment	Query

Module	Role/Privilege Level	Security Attribute Access	Access Type
OA	Administrator	OA system administrator unique identifier	Change default Query Modify Delete Create
		Privilege level	Change default Query Modify Delete Create
		OA system administrator component assignment	Change default Query Modify Delete Create
	Operator	OA system administrator unique identifier	Query
		Privilege level	Query
		OA system administrator component assignment	Query
	User	OA system administrator unique identifier	Query
		Privilege level	Query
		OA system administrator component assignment	Query
VC	Administrator	Unique subject identifier	Change default Query Modify Delete Create
		Privilege level	Change default Query Modify Delete Create
	User	Unique subject identifier	Query
		Privilege level	Query

***Application Note**: System administrators granted an OA role as defined in the table above are automatically mapped to the same role within iLO. This is only applicable for system administrators accessing iLO through the OA interfaces. iLO maintains its own account database in which system administrators are granted a set of iLO-specific privilege levels. The User role contains no iLO privilege levels. The Operator role is mapped to the "Remote Console Access", "Virtual Power and Reset", "Virtual Media", and "Host BIOS" iLO privilege levels. The Administrator includes all Operator privileges and in addition, grants the "Administer User Accounts", and "Configure iLO Settings" privilege levels. The VC Administrator role identified in the table above is a generic term that is assumed by system administrators of the VC modules that have been explicitly assigned one of the four VC* *privilege levels, e.g. "Domain", "Server", "Storage", and "Network". The User role is not assigned any privilege levels.*

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*Management Access Control SFP, iLO Information Flow Control SFP, and VC Information Flow Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*appropriately privileged system administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

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

FMT_MTD.1.1

The TSF shall restrict the ability to [*[the 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 'Role/Privilege Level' column of Table 15*].

Table 15 – Management of TSF Data

Module	Object	Role/Privilege Level	Operations
iLO	Information: Overview	Everyone[69]	View
	Information: Session List	Administer User Accounts	Disconnect active sessions
		Everyone	View
	Information: iLO Event Log	Configure iLO Settings	Clear event logs
		Everyone	View
	Information: Integrated Management Log	Configure iLO Settings	Mark as repaired, add maintenance notes, and clear event logs
		Everyone	View
	Information: Active Health System Log	Configure iLO Settings	Enable/disable logging and clear event logs
		Everyone	View
	Information: Diagnostics	Configure iLO Settings	Reset iLO
		Virtual Power and Reset	Generate NMI[70] and swap the ROM
		Everyone	View
	System Information: Summary	Everyone	View

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

Module	Object	Role/Privilege Level	Operations
	System Information: Processors	Everyone	View
	System Information: Memory	Everyone	View
	System Information: Network	Everyone	View
	System Information: Device Inventory	Everyone	View
	System Information: 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
	Firmware & OS Software: Software	Everyone	View
	Firmware & OS Software: iLO Repository	Configure System Recovery	Install or delete firmware images
		Everyone	View
	Firmware & OS Software: Install Sets	Everyone	View
	Firmware & OS Software: Installation Queue	Everyone	View
	iLO Federation: Setup	Configure iLO Settings	Manage
		Everyone	View
	iLO Federation: Multi-System View	Everyone	View and filter
	iLO Federation: Multi-System Map	Everyone	View and filter
	iLO Federation: Group Virtual Media	Virtual Media	Manage media
		Everyone	View and filter
	iLO Federation: Group Power	Virtual Power and Reset	Use power buttons
		Everyone	View and filter
	iLO Federation: Group Power Settings	Configure iLO Settings	Manage
		Everyone	View and filter
	iLO Federation: Group Firmware Update	Configure iLO Settings	Update firmware
		Everyone	View and filter
	iLO Federation: Group Licensing	Configure iLO Settings	Update license
		Everyone	View and filter
	iLO Federation: Group Configuration	Configure iLO Settings	View and manage
	Remote Console & Media: Launch	Remote Console	Launch iLO Java Integrated Remote Console (iLO JIRC) and iLO .NET Integrated Remote Console (iLO NIRC)
		Everyone	View
	Remote Console & Media: Virtual Media	Virtual Media	Use, eject, and insert media
		Virtual Power and Reset	Reset the server
		Configure iLO Settings	Manage

Module	Object	Role/Privilege Level	Operations
		Everyone	View
	Remote Console & Media: Hot Keys	Configure iLO Settings	Manage
		Everyone	View
	Remote Console & Media: 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 & Thermal: Power Meter	Everyone	View
	Power & Thermal: Power Settings	Configure iLO Settings	Manage
		Everyone	View
	Power & Thermal: Power	Everyone	View
	Power & Thermal: Fans	Everyone	View
	Power & Thermal: Temperatures	Everyone	View
	iLO Network Port: Summary	Everyone	View
	iLO Network Port: General	Configure iLO Settings	Manage
		Everyone	View
	iLO Network Port: IPv4	Configure iLO Settings	Manage
		Everyone	View
	iLO Network Port: IPv6	Configure iLO Settings	Manage
		Everyone	View
	iLO Network Port: SNTP	Configure iLO Settings	Manage
		Everyone	View
	Remote Support: Registration	Configure iLO Settings	Manage
		Everyone	View
	Remote Support: Service Events	Configure iLO Settings	Manage
		Everyone	View
	Remote Support: Data Collections	Configure iLO Settings	Manage
		Everyone	View
	Administration: Boot Order	Virtual Media and Configure iLO Settings	Manage (requires both privilege levels)
		Virtual Power and Reset	Reset the server
		Everyone	View
	Administration: Licensing	Configure iLO Settings	Manage
		Everyone	View
	Administration: User Administration	Configure iLO Settings	Manage directory groups

ystem c-Class Enclosure Architecture

Module	Object	Role/Privilege Level	Operations
		Administer User Accounts	Manage users
		Everyone	View, change personal password
	Administration: Key Manager	Configure iLO Settings	Manage
		Everyone	View
	Administration: Language	Configure iLO Settings	Manage
		Everyone	View
	Security: Access Settings	Configure iLO Settings	Manage
		Everyone	View
	Security: iLO Service Port	Configure iLO Settings	Manage
		Everyone	View
	Security: Secure Shell Key	Administer User Accounts	Manage
		Everyone	View
	Security: Certificate Map	Administer User Accounts	Manage
		Everyone	View
	Security: CAC Authentication	Configure iLO Settings	Manage
		Everyone	View
	Security: SSL Certificate	Configure iLO Settings	Manage
		Everyone	View
	Security: Directory	Configure iLO Settings	Manage
		Everyone	View
	Security: Encryption	Configure iLO Settings	Manage
		Everyone	View
	Security: HPE SSO[71]	Configure iLO Settings	Manage
		Everyone	View
	Security: Login Security Banner	Configure iLO Settings	Manage
		Everyone	View
	Management: SNMP Settings	Configure iLO Settings	Manage
		Everyone	View
	Management: AlertMail	Configure iLO Settings	Manage
		Everyone	View
	Management: Remote Syslog	Configure iLO Settings	Manage
		Everyone	View
OA[72]	Rack Overview	Everyone	View

[71] SSO – Single Sign-On

[72] The OA operations of the Administrator, Operator, and User privilege levels are observed while access to all bays is enabled.

Module	Object	Role/Privilege Level	Operations
	Rack Firmware	Administrator	View
		Operator and User	Limited view
	Enclosure Information	Administrator	View and manage
		Operator	Limited view and manage
		User	Limited view
	AlertMail	Administrator and Operator	View and manage
		User	View
	Device Power Sequence	Administrator	View and manage
		Operator and User	View
	Date and Time	Administrator and Operator	View and manage
		User	View
	Enclosure TCP[73]/IP Settings	Everyone	View and manage
	Network Access	Administrator	View and manage
		Operator	Limited view and limited management
	Link Loss Failover	Administrator and Operator	View and manage
		User	View
	SNMP Settings	Administrator and Operator	View and manage
		User	View
	IPv4	Administrator and Operator	View and manage
		User	View
	IPv6	Administrator and Operator	View and manage
		User	View
	Configuration Scripts	Administrator	View and manage
	Reset Factory Defaults	Administrator	View and manage
	Device Summary	Everyone	View
	DVD Drive	Administrator and Operator	View, manage, and launch
		User	View and launch
	VLAN[74] Configuration	Administrator and Operator	View and manage
		User	View
	Enclosure Firmware Management	Administrator	View and manage
	Active Health System	Administrator	View and manage
	Remote Support	Administrator	View and manage
	Certificate Administration	Administrator	View and manage

[73] TCP – Transmission Control Protocol

[74] VLAN – Virtual Local Area Network

Module	Object	Role/Privilege Level	Operations
	Active Onboard Administrator	Everyone	View and manage
	TCP/IP Settings	Everyone	View
	Certificate Administration	Administrator	View and manage
		Operator and User	View
	Firmware Update	Administrator and Operator	View and manage
	System Log	Administrator and Operator	View and manage
		User	Limited view
	Device Bays	Everyone	View and refresh
	Device #	Administrator and Operator	View and manage
		User	Limited view and limited management
	iLO	Everyone	View
	Port Mapping	Everyone	View
	Firmware	Administrator	View and manage
	Interconnect Bays	Everyone	View and refresh
	Interconnect Module #	Administrator and Operator	View and manage
		User	Limited view and limited management
	Port Mapping	Everyone	View
	Management Console	Everyone	Launch
	Power and Thermal	Everyone	View and refresh
	Power Management	Administrator and Operator	View and manage
		User	View
	Enclosure Power Allocation	Everyone	View and refresh
	Enclosure Power Summary	Administrator	View and refresh
	Power Meter	Everyone	View and refresh
	Power Subsystem	Everyone	View and refresh
	Power Supply #	Everyone	View and refresh
	Thermal Subsystem	Everyone	View and refresh
	Fan #	Everyone	View and refresh
	Local Users	Administrator	View, manage, create, and delete
	Username	Administrator	View all users and manage
		Operator and User	View current user and limited management
	Password Settings	Administrator	View and manage
	Directory Settings	Administrator	View and manage
	Directory Groups	Administrator	View and manage
	Directory Group Name	Administrator	View and manage

Module	Object	Role/Privilege Level	Operations
	SSO Integration	Administrator	View and manage
	Two-Factor Authentication	Administrator	View and manage
	CAC Authentication	Administrator	View and manage
	Signed in Users	Administrator	View and manage
	Insight Display	Administrator and Operator	View, manage, and use
		User	View and use
	Virtual Connect Manager	Everyone	Launch
VC	Home Screen	Everyone	View
	Configure	Domain	View and manage
		Network, Server, Storage, and User[75]	View
	IP Address	Domain	View and manage
		Network, Server, Storage, and User	View
	Enclosures	Everyone	View
	Backup/Restore	Domain	View and manage
		Network, Server, Storage, and User	View
	Storage Mgmt Credentials	Domain, Network, Server, and User	View
		Storage	View and manage
	SNMP Configuration	Domain, Network, and Storage	View and limited management
		Server and User	View
	System Log	Domain	View, refresh, and manage
		Network, Server, Storage, and User	View and refresh
	Stacking Links	Domain	View and manage
		Network, Server, Storage, and User	View
	Local Users	Domain	View, create, delete, and manage
		Network, Server, Storage, and User	View current user and limited management
	CAC Authentication	Domain	View and manage
		Network, Server, Storage, and User	View
	LDAP Settings	Domain	View and manage
		Network, Server, Storage, and User	View
	Radius Settings	Domain, Network, Server, Storage, and User	View
	TACACS+[76] Settings	Domain, Network, Server, Storage, and User	View

[75] In VC, the User role is assumed when no privileges are assigned to a user's account.

[76] TACACS+ – Terminal Access Controller Access Control System Plus

Module	Object	Role/Privilege Level	Operations
	Role Management	Domain	View and manage
		Network, Server, Storage, and User	View
	SSL Certificate	Domain	View and manage
		Network, Server, Storage, and User	View
	SSH Administration	Everyone	View and manage
	Web SSL Configuration	Domain	View and manage
		Network, Server, Storage, and User	View
	MAC Addresses	Everyone	View
	Port Monitoring	Domain, Storage, and User	View
		Network and Server	View and manage
	Advanced Settings	Domain, Server, Storage, and User	View
		Network	View and manage
	sFlow Settings	Domain and Server	View, refresh, and limited management
		Network	View, refresh, and manage
		Storage and User	View and refresh
	Quality of Service (QoS)	Domain, Server, Storage, and User	View
		Network	View and manage
	IGMP[77] Settings	Domain, Storage, and User	View
		Network and Server	View and manage
	WWN Settings	Domain, Network, Server, and User	View
		Storage	View and manage
	Server Serial Numbers	Domain, Network, Storage, and User	View
		Server	View and manage
	Server Profiles	Domain, Network, Storage, and User	View
		Server	View and manage
	Ethernet Networks	Domain, Server, Storage, and User	View
		Network	View, create, and manage
	Shared Uplink Sets	Domain, Server, Storage, and User	View
		Network	View and manage
	SAN Fabrics	Domain, Network, Server, and User	View
		Storage	View and manage
	Network Access Groups	Domain, Server, Storage, and User	View
		Network	View and manage
	Overview	Everyone	View

[77] IGMP – Internet Group Management Protocol

Module	Object	Role/Privilege Level	Operations
	OA Module Name	Everyone	View
	Interconnect Bays	Everyone	View
	Device Bays	Everyone	View

F.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 security functions behavior*
- *Management of TSF data*
- *Management of security attributes*].

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 [

- *For iLO accounts:*
  - *Host BIOS*
  - *Remote Console*
  - *System Recovery*
  - *Administer User Accounts*
  - *Virtual Media*
  - *Virtual Power and Reset*
  - *Configure iLO Settings*
- *For OA accounts:*
  - *Administrator*
  - *Operator*
  - *User*
- *For VC accounts:*
  - *Domain*
  - *Network*
  - *Storage*
  - *Server*
  - *User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note*: The “roles” listed here are called “privilege levels” in BladeSystem vernacular. The “User” role in VC is assigned by default to provide read-only access to VC.*

6.2.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*failure of BladeSystem hardware components*].

Application Note*: FPT_FLS.1 is enforced by the iLO, OA, and VC components. FPT_FLS.1 functionality can be manually exercised through the iLO Web GUI and iLO XML Scripting Interface. All other external interfaces are excluded from the scope.*

FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1 Passive detection of physical attack
Dependencies: FMT_MOF.1 Management of security functions behavior

FPT_PHP.2.1

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3

For [*BladeSystem hardware components*], the TSF shall monitor the devices and elements and notify [*the authorized system administrator*] when physical tampering with the TSF's devices or TSF's elements has occurred.

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 [*BladeSystem hardware component failure or tampering*] 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 [*BladeSystem hardware component failure when a functional failover component is available*], 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(a) TSF testing (Cryptographic module)

Hierarchical to: No other components.
Dependencies: No dependencies

FPT_TST.1(a).1

The TSF shall run a suite of self tests [*during initial start-up and periodically during normal operation*] to demonstrate the correct operation of [*[the FIPS 140-2-validated cryptographic modules used by iLO and OA]*].

FPT_TST.1(a).2

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

FPT_TST.1(a).3

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

FPT_TST.1(b) TSF testing (BladeSystem components)

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1(b).1

The TSF shall run a suite of self tests [*during initial start-up, periodically during normal operation, at the request of the authorized user, and at the conditions [that a BladeSystem hardware component is inserted or removed]*] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1(b).2

The TSF shall provide authorized users with the capability to verify the integrity of [*[BladeSystem hardware component]*].

FPT_TST.1(b).3

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

6.2.7 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.2.1

The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*BladeSystem hardware component failure when a functional failover component is present*].

6.2.8 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1

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

Application Note*: FTA_SSL.3 is enforced by iLO Web GUI, iLO CLI, iLO CHIF, iLO JIRC, iLO NIRC, OA Web GUI, OA CLI, OA SOAP Interface, VC Web GUI, and VC CLI. All other external interfaces are excluded from the scope.*

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.
Dependencies: No dependencies

FTA_TAB.1.1

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

Application Note*: FTA_TAB.1 is enforced by iLO Web GUI, OA Web GUI, OA CLI, VC Web GUI, and VC CLI. 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 CHIF, iLO UEFI/RBSU Interface, iLO REST API, OA Web GUI, and OA SOAP Interface. All other external interfaces, including VC interfaces, are excluded from the scope.*

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 system
	ALC_CMS.2 Parts of the TOE CM[78] coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification

[78] CM – Configuration Management

Assurance Requirements	
	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

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 each security functionality and its associated SFRs.

Table 17 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID[79]	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	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_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1(a)	Subset information flow control (VC to Blade Server)
	FDP_IFC.1(b)	Subset information flow control (OA to iLO)
	FDP_IFF.1(a)	Simple security attributes (VC to Blade Server)
	FDP_IFF.1(b)	Simple security attributes (OA to iLO)
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions

[79] ID – Identification

TOE Security Functionality	SFR ID[79]	Description
	FMT_SMR.1	Security roles
Protection of TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.2	Notification of physical attack
	FPT_RCV.2	Automated recovery
	FPT_STM.1	Reliable time stamps
	FPT_TST.1(a)	TSF testing (Cryptographic module)
	FPT_TST.1(b)	TSF testing (BladeSystem components)
Resource Utilization	FRU_FLT.2	Limited fault tolerance
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment

7.1.1 Security Audit

The iLO, OA, and VC TOE components generate audit records for the start-up and shutdown of their audit functions, all administrative events, critical system events, and status events that should be seen by system administrators. Audit records are stamped with the actual time at which the event occurred. After authenticating to a TOE component, system administrators are able to review all audit records, and the TOE prevents unauthorized deletion or modification of the audit records. When the audit trail reaches capacity, the oldest records are overwritten with new records.

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

7.1.2 Cryptographic Support

The TOE implements two FIPS 140-2 validated cryptographic modules (iLO and OA) that implement the AES, 3DES, SHA, RSA, and DSA algorithms. VC uses algorithms that are CAVP-validated against FIPS 140-2 requirements. These cryptographic algorithms are used to secure management traffic between the system administrators and the TOE. The iLO Web GUI, OA Web GUI, and VC Web GUI are protected via the TLS protocol. The iLO CLI, OA CLI, and VC CLI are protected via the SSH protocol. Communications sent to the LDAP server are also secured using the TOE's cryptographic modules. The iLO, OA, and VC devices will connect to the LDAP server using LDAP over TLS to form LDAPS[80] when identifying and authenticating system administrators. The iLO and OA cryptographic modules 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.

[80] LDAPS – Lightweight Directory Access Protocol Secure

7.1.3 User Data Protection

By triggering an iLO reset to factory defaults, an authorized system administrator can ensure that any previous authentication information and settings for each iLO managed blade server are deallocated and made unavailable. All authentication data supplied to OA is released from the contents of memory upon de-allocation of its resources. When OA is reset to factory defaults, all passwords and TSF data, except for the default Administrator account's password, are cleared from storage. To deallocate the default Administrator account's password the LP/FDR mode must be used. Once a FIPS transition is initiated in OA, the system administrator is asked for a new (strong) password. The password is hashed, and the hash is stored within OA. All VC authentication data is stored securely within protected memory registers, and the contents of these registers are erased upon de-allocation of the memory from the authentication data. When VC is reset to factory defaults, or when a FIPS mode of operation is instantiated, all authentication information and device settings are cleared from storage.

The TOE implements three SFPs:

- The Management Access Control SFP that is detailed in Section 7.1.3.1 below
- The VC Information Flow Control SFP that is detailed in Section 7.1.3.2 below
- The iLO Information Flow Control SFP that is detailed in Section 7.1.3.3 below

7.1.3.1 Management Access Control SFP

The Management Access Control SFP ensures that only authorized and appropriately privileged system administrators can access or configure the TOE via the iLO, OA, and VC components. The Management Access Control SFP governs the use of the Management TSF as described in Section 6 above. The TOE determines which system administrators are allowed to access which iLO, OA, and VC components via a system administrator's username, privilege level, and component assignments. A username is a system administrator's unique identifier within the TOE. Once access to a component is determined, the TOE will determine which operations a system administrator can perform on that component.

An OA system administrator can have one of following privilege levels:

- Administrator: Allows full configuration and access of all aspects of the TOE, including configuration, firmware updates, account management, and resetting default settings.
- Operator: Allows access to all information, but only certain configuration settings can be changed.
- User: Allows access to all information, but no changes can be made.

An iLO system administrator can have one of the following privilege levels:

- Administer User Accounts: Allows access to configure local iLO accounts. This privilege level is mapped to OA Administrators.
- Remote Console Access: Allows access to virtual server consoles. This is mapped to the OA Administrator and Operator roles.
- Virtual Power and Reset: Allows control of the server power functions. The power functions are used to power-cycle or reset the host platform. This is mapped to the OA Administrator and Operator roles.
- Virtual Media: Allows access to mount removable storage devices to the remote server. This is mapped to the OA Administrator and Operator roles.

- Configure iLO Settings: Allows control of iLO configuration aspects, including security-relevant settings. This is mapped to the OA Administrator role.
- Host BIOS: Allows access to configure the host BIOS settings by using the iLO UEFI/RBSU Interface. This privilege level is mapped to OA Administrators.
- System Recovery: Allows access to manage the critical recovery install set. By default, this privilege is assigned to the default iLO Administrator account. To assign this privilege to another account, the system administrator must log in with an account that already has this privilege.

System administrators have one or more component assignments, which are associations or bindings of the system administrator to specific BladeSystem components (such as enclosure bays, VC modules, blade servers, etc.) on which they have permission to execute the privileges granted to them by their privilege level. BladeSystem components can be uniquely identified by a variety of variables, called component identifiers in this SFP, such as the component serial number or the enclosure bay in which a component is installed.

7.1.3.2 VC Information Flow Control SFP

The VC Information Flow SFP ensures that the blade servers within the enclosure only communicate with other internal blade servers or entities on the external network(s) for which they have been configured by a system administrator to communicate. The TOE determines which BladeSystem blade servers, external servers, and workstations are allowed to communicate with each other based on the source and destination identities of the data and the rules configured within the VC module by an appropriately privileged system administrator.[81]

The TOE controls information flow to ensure that the blade servers are permitted to transmit data to external networks only when explicitly assigned a profile[82] associated with an external network. To further isolate the flow of information, data tagged with a unique identifier is forwarded to only the interfaces that are configured with matching unique identifiers. For example, packets tagged with a particular VLAN ID in their header will only be forwarded to interfaces configured with that same VLAN ID. Examples of unique identifiers used by the TOE are LAN ID, VLAN ID, IP address, MAC address, and WWN.

The TOE enforces a distinct separation of the information flow to ensure that no traffic is interfered with by any other traffic when it is within the TOE's scope of control. For example, data traveling over one VLAN will never be seen by any other VLAN even though all of the VLANs move through the same TOE.

Access to VC management functions is provided through the following role assignments:

- Domain: Allows configuration of local accounts, firmware management, IP address configuration, and other VC domain settings.
- Network: Allows configuration of the enclosure network.
- Server: Allows configuration of server connectivity profiles and server power functions.
- Storage: Allows configuration of server storage fabrics.

[81] For example, a rule might specify that a blade server in bay #1 is allowed to communicate via an installed VC with a blade server in bay #3 but that the blade server cannot communicate with another blade server in bay #2. Rules can be based on many types of source and destination identifiers including IP address, MAC address, etc. For detailed information about VC configuration and rules, please refer to the VC administrative manuals.

[82] Profile – A collection of device-independent network and storage connection settings.

7.1.3.3 iLO Information Flow Control SFP

The iLO Information Flow Control SFP ensures that only appropriately privileged system administrators are allowed to use the iLO functionality of installed blade servers. The TOE determines which iLO-enabled BladeSystem blade servers a system administrator is allowed to communicate with based on the system administrator's username, role, component assignment(s), the BladeSystem blade server's unique identifier, and the rules configured within the OA module by an appropriately privileged system administrator.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1(a), FDP_IFC.1(b), FDP_IFF.1(a), FDP_IFF.1(b), and FDP_RIP.1.

7.1.4 Identification and Authentication

System administrators can configure the TOE to require passwords for OA and VC to be of a specific minimum character complexity and length. System administrators can also configure password length requirements for the iLO interfaces.

The TOE provides unauthenticated access to basic enclosure information on the OA Web GUI's login page, various iLO CHIF commands, and the help link of the iLO Web GUI, OA Web GUI, and VC Web GUI login pages. The OA Web GUI's login page provides a help link depicted as a question mark "?" in a box that provides information about logging into OA as well as information about the enclosure that OA is connected to. The VC Web GUI's login page provides the "Sign-in help" link that displays helpful information about logging into VC. The iLO Web GUI's login page contains a question mark "?" icon 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 iLO 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[83] 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 the iLO SMIF encryption key for the 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.

System administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the LDAP server, iLO, OA, and VC modules are able to identify and authenticate system administrators that use directory services.

TOE Security Functional Requirements Satisfied: FIA_SOS.1(a), FIA_SOS.1(b), FIA_UAU.1, and FIA_UID.1.

[83] SMIF – Systems Management Interface

7.1.5 Security Management

The TOE allows only authenticated system administrators to access the TOE management interfaces. Additionally, access to specific functionality via those interfaces only to appropriately privileged system administrators by enforcing the Management Access Control SFP, the VC Information Flow Control SFP, and the iLO Information Flow Control SFP. The TOE allows management of TSF data, security attributes, and the behavior of its security functions.

System administrators of the TOE can be authenticated directly by the TOE using a local username and password or by an external LDAP authentication server using their external LDAP credentials. iLO and OA support LDAP directories such as Microsoft Active Directory for authentication and authorization. VC supports LDAP for authentication only; authorization is handled internally by VC.

System administrators are assigned a “privilege level” (sometimes called a “role”) and are bound to an arbitrary number of BladeSystem components and features over which they are allowed to exercise their assigned privilege level. This functionality is mediated by the iLO, OA, and VC components through their enforcement of the Management Access Control Security Functional Policy and VC Information Flow Control Policy.

Each of the iLO, OA, and VC management interfaces may be directly accessed by authorized system administrators. For OA system administrators however, roles are directly mapped to iLO privilege levels. To access iLO’s management functions, OA provides a login bypass feature for currently authenticated system administrators. However, iLO also provides its own set of local accounts and privilege levels to authenticate system administrators directly interfacing with it, and it can also be configured to leverage existing LDAP repositories. Similarly, the VC management interface is only directly accessible and requires a local or external VC account, but functions provided by VC are not available through the OA management interfaces as they are with iLO. VC requires a dedicated OA account during initial configuration to communicate with OA components for server storage and networking functions.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE implements numerous self-tests (power-up self-tests, conditional self-tests, and critical self-test) to ensure that both the cryptographic functionality of the TOE and the BladeSystem components composing the TOE are functioning correctly. FIPS 140-2-required self-tests are performed on the iLO and OA cryptographic algorithms and cryptographic modules 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, KATs in firmware, and a cryptographic library integrity test. 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 tests, pairwise consistency tests, and firmware load/update tests. Critical self-tests are performed during power-up and conditionally. 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 modules, the tested code, and the BladeSystem hardware components by viewing the system logs of the iLO, OA, and VC devices. If the self-tests pass, each module will generate an audit log to note the TOE is operating correctly. If the self-tests fail, the module will error and not function properly until it is resolved. The TOE can also detect when a BladeSystem component is tampered with (that is when it is removed from the enclosure), when a component fails, and when a new BladeSystem component is added to the enclosure. It can alert the system administrators when these events occur. If a BladeSystem component fails, and if a comparable failover-ready component is installed, the TOE automatically fails-over to use the other component, thus providing uninterrupted service. The TOE performs numerous periodic BladeSystem component and communications tests to quickly and accurately detect actual and impending component failure.

Each TOE component also provides reliable time stamps. OA provides the capability to set its internal clock manually, while iLO time will be set to synchronize with an SNTP server. VC automatically synchronizes its time with an available OA.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_PHP.2, FPT_RCV.2, FPT_STM.1, FPT_TST.1(a), and FPT_TST.1(b).

7.1.7 Resource Utilization

If a BladeSystem component fails, and if a comparable failover-ready component is installed, the TOE automatically fails-over to use the other component. The automatic failover ensures the TOE's operations during the failure. The TOE performs numerous periodic BladeSystem component and communications tests to quickly and accurately detect actual and impending component failure.

TOE Security Functional Requirements Satisfied: FRU_FLT.2.

7.1.8 TOE Access

Inactive sessions can be terminated by the TOE after a configurable time interval of inactivity for iLO Web GUI, iLO CLI, iLO CHIF, iLO JIRC, iLO NIRC, OA Web GUI, OA CLI, OA SOAP Interface, VC Web GUI, and VC CLI. The TOE can be configured to display an arbitrary logon "banner" (a message that is displayed to every system administrator attempting to authenticate to the TOE's administrative interfaces, specifically iLO Web GUI, OA Web GUI, OA CLI, VC Web GUI, and VC CLI.) The TOE will also enforce a login delay between failed login attempts on the iLO Web GUI, iLO CLI, iLO CHIF, iLO UEFI/RBSU Interface, iLO REST API, OA Web GUI, and OA SOAP Interface.

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

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 5.

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

Table 18 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.CONFIG An unauthorized user or attacker, who is not a system administrator, could improperly gain access to user data if the product is misconfigured or does not enforce proper roles and permissions.	O.ACCESS The TOE must ensure that only authorized system administrators may access and configure the product.	O.ACCESS counters this threat by ensuring that system administrators properly configure access control for all system administrators of the TOE and that the TOE enforces this access control while in the evaluated configuration.
	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 system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must handle idle sessions and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that the TOE has identified and authenticated a system administrator before they are allowed to access any data.

Threats	Objectives	Rationale
T.FAILURE_OR_TAMPER Physical failure or tampering of a TOE component, by an unauthorized user or attacker, could go undetected or could cause a breach of the TSF.	O.FAILURE_OR_TAMPER The TOE must ensure that TSF services continue to be offered in case of physical component failure. The TOE must also ensure that physical tampering with (removal of) physical components is detected and system administrators are informed.	O.FAILURE_OR_TAMPER ensures that the TOE will detect when a failure occurs in a TOE physical component or when a TOE physical component is tampered with, and that such events will not cause a breach of the TSF.
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 system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must 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 could access data stored by the TOE by bypassing the protection mechanisms of 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.ADMIN ensures that access to TOE security data is limited to those system administrators with access to the management functions of the TOE.
	O.AUDIT The TOE must securely record audit events that include the resulting actions of the security functional policies and the identified system administrator (if applicable). The TOE must also provide the authorized system administrators with the ability to review the audit trail and 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.AUTHENTICATE The TOE must identify and authenticate system administrators prior to allowing access to TOE administrative functions and data. The TOE must identify authorized system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must 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 19 below gives a mapping of policies and the objectives that support them.

Table 19 – 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 system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must handle idle sessions and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that only authorized system administrators are granted access to the tools required to manage the TOE.

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

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 20 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 20 – 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 blade 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.

Assumptions	Objectives	Rationale
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 assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 21 below shows a mapping of the objectives and the SFRs that support them.

Table 21 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must ensure that only authorized system administrators may access and configure the product.	FDP_ACC.1 Subset access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.
	FDP_ACF.1 Security attribute based access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFC.1(a) Subset information flow control (VC to Blade Server)	The requirement meets this objective by ensuring that all system administrators are controlled by the VC Information Flow Control SFP.
	FDP_IFC.1(b) Subset information flow control (OA to iLO)	The requirement meets this objective by ensuring that all system administrators are controlled by the iLO Information Flow Control SFP.
	FDP_IFF.1(a) Simple security attributes (VC to Blade Server)	The requirement meets this objective by ensuring that all system administrators are controlled by the VC Information Flow Control SFP.
	FDP_IFF.1(b) Simple security attributes (OA to iLO)	The requirement meets this objective by ensuring that all system administrators are controlled by the iLO Information Flow Control SFP.
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_ACC.1 Subset access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.
	FDP_ACF.1 Security attribute based access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.
	FDP_RIP.1 Subset residual information protection	The requirement meets the objective by ensuring the TOE deallocates resources from 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 those system administrators with the appropriate privileges.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE enforces the Management Access Control SFP, iLO Information Flow Control SFP, and VC Information Flow Control SFP to restrict the ability to manipulate security attributes to only those system administrators with the appropriate privileges.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the TOE creates restrictive default values for security attributes that are used to enforce the Management Access Control SFP, iLO Information Flow Control SFP, and VC Information Flow Control SFP.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the system administrator's privileges.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates system administrators with roles to provide access to TSF management functions and data.
	FPT_TST.1(a) TSF testing (Cryptographic module)	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 and the identified system administrator (if applicable). The TOE must also provide the authorized system administrators with the ability to review the audit trail and 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 iLO, OA, and VC interfaces.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	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 ensuring that the TOE overwrites the oldest audit records if the audit trail becomes full.
	FPT_STM.1 Reliable time stamps	The TOE provides reliable time stamps for its own use.

Objective	Requirements Addressing the Objective	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 system administrators prior to allowing access to manipulate data. The TOE must display a logon banner to system administrators prior to their access of the system, and it must handle idle sessions and failed login attempts in a secure manner.	FDP_ACC.1 Subset access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.
	FDP_ACF.1 Security attribute based access control	The requirement meets this objective by ensuring that all system administrators of the iLO, OA, and VC components are controlled by the Management Access Control SFP.
	FIA_SOS.1(a) Verification of secrets (iLO)	The requirement meets this objective by ensuring that system administrators' passwords for iLO are of sufficient length.
	FIA_SOS.1(b) Verification of secrets (OA and VC)	The requirement meets this objective by ensuring that system administrators' passwords for OA and VC are of sufficient complexity and 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_UID.1 Timing of identification	The requirement meets the objective by ensuring that the 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 system 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_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE authenticates system administrators prior to allowing them access to manipulate security attributes. This is to ensure that only appropriately privileged system administrators may do so.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the TOE authenticates system administrators prior to allowing them access to manipulate security attributes. This is to ensure that only appropriately privileged system administrators may do so.
	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.

Objective	Requirements Addressing the Objective	Rationale
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that management 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 system administrators can configure an advisory warning message that will be displayed on the management interfaces when a system administrator attempts to authenticate.
	FTA_TSE.1 TOE session establishment	The requirement meets the objective by ensuring that the TOE will increase a delay between each successive failed login attempt on the management interfaces.
O.FAILURE_OR_TAMPER The TOE must ensure that TSF services continue to be offered in case of physical component failure. The TOE must also ensure that physical tampering with (removal of) physical components is detected and system administrators are informed.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that failure of any particular BladeSystem hardware component does not compromise the integrity of the TSF.
	FPT_PHP.2 Notification of physical attack	The requirement meets the objective by ensuring that the TOE will detect when a BladeSystem physical component is tampered with (removed or added).
	FPT_RCV.2 Automated recovery	The requirement meets the objective by ensuring that the TOE will failover to another similar installed component when a BladeSystem hardware component fails.
	FPT_TST.1(b) TSF testing (BladeSystem components)	The requirement meets the objective by ensuring that the TOE will detect when a BladeSystem physical component fails, is about to fail, or is added or removed.
	FRU_FLT.2 Limited fault tolerance	The requirement meets the objective by ensuring that the TOE will failover to another similar installed component when a BladeSystem hardware component fails.

8.5.2 Security Assurance Requirements Rationale

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

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 22 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 22 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_IFC.1(a)	FDP_IFF.1	✓	
FDP_IFC.1(b)	FDP_IFF.1	✓	
FDP_IFF.1(a)	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FDP_IFF.1(b)	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FDP_RIP.1	No dependencies	✓	
FIA_SOS.1(a)	No dependencies	✓	
FIA_SOS.1(b)	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	No dependencies	✓	
FPT_PHP.2	FMT_MOF.1	✓	
FPT_RCV.2	AGD_OPE.1	✓	
FPT_STM.1	No dependencies	✓	
FPT_TST.1(a)	No dependencies	✓	
FPT_TST.1(b)	No dependencies	✓	
FRU_FLT.2	FPT_FLS.1	✓	
FTA_SSL.3	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
FTA_TSE.1	No dependencies	✓	

9. Acronyms

Table 23 defines the acronyms used throughout this document.

Table 23 – Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AHS	Active Health System
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
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
CMVP	Cryptographic Module Validation Program
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVD	Digital Video Disk
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ERS	Embedded Remote Support
ESR	Extended Support Release
FC	Fibre Channel
FIPS	Federal Information Processing Standard
GB	Gigabyte
Gb	Gigabit
GCM	Galois Counter Mode
GUI	Graphical User Interface

Acronym	Definition
HA	High Availability
HBA	Host Bus Adapter
HMAC	Hash-based Message Authentication Code
HPE	Hewlett Packard Enterprise Development LP
HPONCFG	HPE Online Configuration Utility
HTTPS	Hypertext Transport Protocol Secure
I/O	Input/Output
I2C	Inter-Integrated Circuit
ID	Identification
IGMP	Internet Group Management Protocol
ILO	Integrated Lights-Out
iOS	iDevice Operating System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRS	Insight Remote Support
iSCSI	Internet Small Computer System Interface
IT	Information Technology
IV	Initialization Vector
JIRC	Java Integrated Remote Console
KAT	Known Answer Test
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
LP/FDR	Lost Password/Flash Disaster Recovery
MAC	Media Access Control
Mb	Megabit
N/A	Not Applicable
NAND	Negated AND
NIC	Network Interface Card
NIRC	.NET Integrated Remote Console
NIST	National Institute of Standards and Technology

Acronym	Definition
NMI	Non-Maskable Interrupt
OA	Onboard Administrator
OFB	Output Feedback
OS	Operating System
OSP	Organizational Security Policy
PKCS	Public Key Cryptography Standard
PP	Protection Profile
QoS	Quality of Service
RBSU	ROM-Based Setup Utility
REST	Representational State Transfer
RFC	Request for Comments
RJ	Registered Jack
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SAN	Storage Area Network
SAR	Security Assurance Requirement
SCSI	Small Computer Systems Interface
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMIF	Systems Management Interface
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Security Target
TAA	Trade Agreement Act
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation

Acronym	Definition
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface
URB	Utility Ready Blades
USB	Universal Serial Bus
UUID	Universally Unique Identifier
VC	Virtual Connect
VCM	Virtual Connect Manager
VLAN	Virtual Local Area Network
WWN	World Wide Name
XML	eXtensible Markup Language

Prepared by:
Corsec Security, Inc.

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

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