Hewlett Packard Enterprise Development LP

BladeSystem c7000 and c3000

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 2.1

Prepared for:

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

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

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the HP BladeSystem c7000 and c3000, 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 server blades, storage blades, 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 functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and 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 met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms 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 c7000 and c3000 Security Target
ST Version	Version 2.1
ST Author	Corsec Security, Inc.
ST Publication Date	December 15, 2015

[1] I/O – Input/Output

TOE Reference	HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (OA) (running firmware version 4.40), Virtual Connect (VC) (running firmware version 4.41), and HP Integrated Lights-Out (HP iLO) 4 (with the Advanced license running firmware version 2.11)
FIPS[2] 140-2 Status	Includes three FIPS 140-2 Level 1 validated cryptographic modules, certificate nos. [xxxx], [xxxx], and [xxxx].

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 c7000 and c3000 Enclosures

Figure 1 – HP BladeSystem c7000 Enclosure, With Example Blade and Module Load-Out

The HP BladeSystem c7000 and c3000 enclosures implement the BladeSystem c-Class architecture, and are optimized for enterprise data center applications (c7000) and midmarket applications (c3000). Figure 1 above shows an example of a fully populated c7000 enclosure. The enclosures fit into standard 19-inch racks; accommodates BladeSystem c-Class server blades, storage blades, and interconnect modules; and provides all the power, cooling, and I/O infrastructure needed to support them. The c7000 enclosure can be populated with the following physical hardware components:

- Up to 8 full-height or 16 half-height server, storage, or other option blades per enclosure. Each independent server blade provides support for running its own, unique instance of a general purpose operating system. Server blades leverage their own local storage or can be logically

[2] FIPS – Federal Information Processing Standard

attached to a storage network to provide bootable storage media. Storage, server, and other option blades include iLO technology (discussed below).
- Up to eight interconnect modules 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[3]. These interconnect modules include VC modules (discussed below).
- Up to 10 Active Cool 200 fan kits.
- Up to six power supplies.
- Redundant OA management modules.

The c3000 enclosure can be populated with the following physical hardware components:

- Up to four full-height or eight half-height server, storage, or other option blades per enclosure. Server blades run stand-alone installations of user-provided operating systems and applications. Storage, server, and other option blades include iLO technology (discussed below).
- Up to four interconnect modules simultaneously supporting a variety of network interconnect fabrics such as Ethernet, FC, InfiniBand, iSCSI, or Serial-attached SCSI. These interconnect modules include VC modules (discussed below).
- Up to six Active Cool 200 fan kits.
- Up to six power supplies.
- Single or redundant OA management modules.

The c7000 and c3000 enclosures include a shared 5-terabit-per-second, high-speed midplane for connection of server blades 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 server blades and interconnects.

The next three subsections provide more detail about the OA, VC, and iLO components. These components provide the majority of BladeSystem functionality.

1.3.2 Onboard Administrator (OA)

Figure 2 – HP BladeSystem OA Module (Example)

The heart of c-Class enclosure management is the OA module (shown in Figure 2 above) located in the enclosure. The OA is a Linux-based appliance that performs four management functions for the entire enclosure:

- Detecting component insertion and removal
- Identifying components and required connectivity
- Managing power and cooling
- Controlling components

An optional second OA in the c7000 and c3000 enclosures provides complete redundancy for these functions.

[3] SCSI – Small Computer Systems Interface

Administrators can access the OA in three different ways: remotely through the web browser graphical user interface (GUI); through the scriptable command line interface (CLI); or through the built-in diagnostic LCD[4] panel included in the front of the c7000 and c3000 enclosures.

The Embedded Remote Support (ERS) options are available through OA when using Insight Remote Support (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[5] environment.

The OA module allows for IPv6[6] addresses to be assigned when associated features are enabled and multiple addresses are supported.

1.3.2.1 Detecting component insertion and removal

The OA provides component control in c-Class enclosures. When a component is inserted into a bay, the OA immediately recognizes and identifies the component. If a component is removed from a bay, the OA deletes the information about that component from its internal list of installed components.

1.3.2.2 Identifying components

To identify a component, the OA reads a Field-Replaceable Unit (FRU) Electrically Erasable Programmable Read-Only Memory (EEPROM) that contains specific factory information about the component such as product name, part number, and serial number. All FRU EEPROMs in c-Class enclosures are always powered, even if the component is turned off, so the OA can identify the component prior to granting power. For devices, such as fans, power supplies, and HP Insight Display (a small display device that provides certain enclosure information), the OA reads the FRU EEPROMs directly. The OA accesses server blade FRU EEPROMs through their iLO management processors.

Server blades contain several FRU EEPROMs: one on the server board that contains server information and embedded network interface card (NIC) information, and one on each of the installed mezzanine option cards. Certain server blade management functions are performed via the OA. Server blade management functions include auto login to the iLO web interface and remote server consoles, virtual power control, and boot order control. Server blade management functions also include the control and configuring of extensive server hardware variables including BIOS[7] and iLO firmware versions, server name, NIC and option card port IDs[8], and port mapping. The OA provides easy-to-understand port mapping information for each of the server blades and interconnected modules in the enclosure.

From the NIC and mezzanine option FRU information, the OA determines the type of interconnects each server requires. For interconnect modules, the OA provides virtual power control, dedicated serial consoles, and management Ethernet connections, based on the specific interconnect features that are included.

1.3.2.3 Managing power and cooling

The most important OA tasks are power control and thermal management. The OA can remotely control the power state of all components in c-Class enclosures. For components in device bays in the front of an enclosure, the OA communicates with the iLO to control servers and communicates with a microcontroller to control options such as storage blades.

Once components are granted power, the OA begins thermal management with Thermal Logic. The Thermal Logic feature in the c-Class enclosures minimizes fan subsystem power consumption by reading

[4] LCD – Liquid Crystal Display
[5] IT – Information Technology
[6] IPv6 – Internet Protocol Version 6
[7] BIOS – Basic Input/Output System
[8] ID – Identification

numerous sensors located throughout the enclosure. Thermal Logic adjusts fan speed in the four different cooling zones within the enclosure to minimize power consumption and maximize cooling efficiency.

1.3.2.4 Controlling components

The OA uses embedded management interfaces to provide detailed information and health status for all bays in the enclosure. The OA also reports firmware versions for most components in the enclosure and can be used to update those components.

1.3.2.4.1 Internal management interfaces

The OA monitors and communicates with each bay in the enclosure via several hardware interfaces. The management hardware interfaces include unique presence pins[9], Inter-Integrated Circuit (I2C), serial, and Ethernet connections. These management interface connections are completely isolated from the server blade connections to interconnect modules, and are only accessible within the enclosure's private management network through logically separated management channels.

1.3.2.4.2 External management interfaces

Each enclosure has several external management interfaces connected to the OA. The primary external management interface is the management port for each OA, which is an RJ-45[10] jack providing Ethernet communications not only to each OA, but also to every device or interconnect bay with a management processor. This includes iLO communication for the server blades and any interconnect module using the c-Class embedded Ethernet management network, such as VC Manager (VCM). 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 the OA and is used for OA firmware flash recovery. USB[11] ports on the OA are used for recovering or writing enclosure configuration to a USB flash drive, or for supplying firmware images. The USB ports are also used to connect DVD[12] drives to the enclosure as an alternative to using the enclosure's built-in DVD drive.

1.3.2.5 Redundant enclosure management

Redundant enclosure management is an optional feature of the c3000 and c7000 enclosures. It requires installing a second OA module in the enclosure 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.

1.3.2.6 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 at located at HPE or inside the IT environment. The following information is sent over an HTTPS 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

[9] Unique presence pins – Used to detect whether a component is installed within a particular bay
[10] RJ – Registered Jack
[11] USB – Universal Serial Bus
[12] DVD – Digital Versatile Disc

- Enclosure manufacturer name
- Onboard Administrator firmware version
- Onboard Administrator IP[13] and MAC[14] 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 is sent about the enclosure hardware as well as populated system components including the LCD module, Onboard Administrator modules, enclosure fan modules, enclosure power supply modules, interconnect modules and server blades. Examples of data that is collected for these system components include:
  - Hardware module descriptors such as manufacturer, product name, serial number, UUID[15], 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

1.3.2.7 IPv6

OA modules support 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.

1.3.3 Virtual Connect (VC)

Figure 3 – HP BladeSystem VC Module (Example)

VC technology is a set of interconnect modules and embedded software for HP BladeSystem c-Class enclosures. VC simplifies the setup and administration of server connections. Figure 3 above shows an example VC module. The following VC-Enet[16] modules are available:

- HP VC Flex-10/10D Module
- HP VC Flex-10 10Gb[17] Ethernet Module
- HP VC FlexFabric 10Gb/24-port Module
- HP VC FlexFabric-20/40 F8 Module

[13] IP – Internet Protocol
[14] MAC – Media Access Control
[15] UUID – Universally Unique Identifier
[16] Enet – Ethernet
[17] Gb – Gigabit

VC-Enet modules enable connectivity to data center 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. VCM is embedded on VC-Enet modules and is accessed through a web-based GUI or CLI. These interfaces are also accessible from OA. FlexFabric modules enable connectivity of the enclosure to data center 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.

HP VC offers a unique approach to connecting and adapting server, LAN[18], and SAN[19] domains across the data center. When the LAN and SAN connections are made available to the pool of servers within the enclosure, the server administrator uses VCM to define a server connection profile for each server. It is an interconnect option for the HP BladeSystem designed to simplify the connection of blade servers to data center networks. Server administrators can automatically manage resources independent of server connections to network and storage resources in an HP BladeSystem, saving administrative time and effort.

With HP VC, an administrator can connect and pre-assign all the LAN and SAN connections that the server pool might ever need. Using VC Flex-10 and VC FlexFabric modules, administrators can choose how many NICs or HBAs[20] are on each server and dynamically set the bandwidth of each connection in increments of 100 Mb[21] between 100 Mb and 10 Gb (20Gb in the case of the FlexFabric-20/40 F8 module).

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

VC modules can be administered in two ways: directly, via the VC's onboard GUI and CLI; and indirectly, via an OA module installed in the BladeSystem chassis.

1.3.3.1 Pass-Thru Modules

Pass-Thru modules are interconnects designed for the HP BladeSystem c-Class enclosures with the same basic purpose as the VC modules but without the VC technology. These modules are used for applications where only a switch is needed such as basic data center connectivity, clusters, and remote locations. The following Pass-Thru modules are available:

- HP 1Gb Ethernet Pass-Thru Module for c-Class BladeSystem
- HP 4Gb FC Pass-Thru Module for c-Class BladeSystem

[18] LAN – Local Area Network
[19] SAN – Storage Area Network
[20] HBA – Host Bus Adapter
[21] Mb – Megabit

1.3.4 HP Integrated Lights-Out (HP iLO)

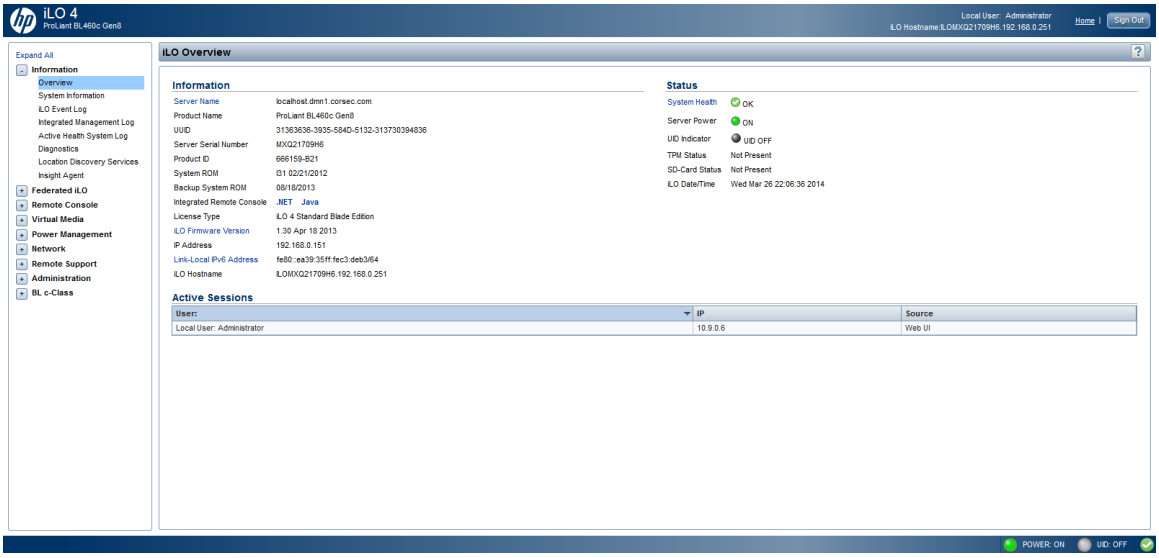

Figure 4 – HP iLO (Example Management Screen)

The HP iLO management built into BladeSystem blade servers and storage blades is an autonomous management subsystem embedded directly on the server. iLO helps simplify initial server setup, power and thermal optimization, remote server administration, and provides server health monitoring with the HP Active Health System (AHS). iLO also provides system administrators with true Agentless Management with SNMP[22] alerts from iLO, regardless of the state of the host server. ERS allows Gen8 and Gen9 servers IRS registration from iLO, regardless of the operating system software and without the need for additional host software, drivers, or agents. The HP AHS monitors and records changes in the server hardware and system configuration. iLO is 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 4 above shows an example screenshot of the iLO management interface. Supported server platforms include:

- HP ProLiant G8/G9 BL Blade Servers
- HP ProLiant G8/G9 ML Tower Servers
- HP ProLiant G8/G9 DL Rack Servers

Blade Servers are small form factor servers housed in blade enclosures, which are designed for modularity and high-density footprints allowing more servers in a smaller space. Tower Servers are upright, free-standing units that contain all the traditional server components: hard disks, motherboards and Central Processing Units (CPU), networking, cabling, power, etc. Rack Servers are complete servers specially designed for an ultra-compact vertical arrangement within a standardized 19-inch mounting rack or cabinet. No matter the form 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. BladeSystem 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, control over the server power and hardware reset functionality, and works with the server to enable remote network booting through a variety of methods. iLO provides GUI and CLI interfaces that can be accessed directly by typing in its IP address from a web browser. The common method for accessing iLO functionality is

[22] SNMP – Simple Network Management Protocol

mediated by the OA GUI. Using iLO Federation Management, an administrator may manage multiple servers from one system running the iLO GUI interface.

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

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

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

iLO stores files, such as Active Health System data, in non-volatile flash memory that is embedded on the system board. This flash memory is called the iLO NAND[23]. HP ProLiant Gen9 servers with a 4GB[24] iLO NAND allow you to use a 1GB non-volatile flash memory partition as if it were an SD[25] card attached to the server. When the Embedded User Partition is enabled, it can be accessed through the server operating system.

1.4 TOE Overview

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

The hardware-software TOE is the BladeSystem c7000 and c3000. In the evaluated configuration, the TOE allows for two modes of operation: VC Mode and Non-VC Mode. VC Mode comprises a BladeSystem c7000 or c3000 rack-mountable enclosure, one or more OA modules, one or more VC modules, one or more server blades that include iLO functionality, and one or more power supplies. Non-VC Mode includes all of the configuration parameters of VC Mode except there are no VC modules installed in the appliance. The VC modules are replaced with any of the compatible HP pass-through interconnect module options. All claims that are valid for only VC Mode are marked accordingly throughout this Security Target. In both modes, the OA modules are configured to function with only IPv4.

Table 2 below lists the versions of the hardware components included in the evaluated configuration of the TOE.

Table 2 – Evaluated Hardware Versions

Component	Versions
Blade Enclosure	HP BladeSystem c3000 Enclosure HP BladeSystem c7000 Enclosure

[23] NAND – Negated AND
[24] GB – Gigabyte
[25] SD – Secure Digital

Component	Versions
VC (VC Mode Only)	HP VC Flex-10 10Gb Ethernet Module HP VC Flex-10/10D Module HP VC FlexFabric 10 Gb/24-Port Module HP VC FlexFabric-20/40 F8 Module
Pass-Thru Modules (Non-VC Mode Only)	HP 1Gb Ethernet Pass-Thru Module HP 4Gb FC Pass-Thru Module
iLO[26]	HP iLO 4 with an Advanced license on ProLiant Gen8 server blades HP iLO 4 with an Advanced license on ProLiant Gen9 server blades
OA	HP BladeSystem c7000 DDR2[27] Onboard Administrator with KVM[28] [29] HP BladeSystem c3000 Tray with embedded DDR2 Onboard Administrator HP BladeSystem c3000 Dual DDR2 Onboard Administrator Module

The TOE is managed by appropriately privileged administrators through web interfaces and CLIs provided by the OA, iLO, and (in VC Mode) VC modules. To access the functions available via these interfaces remotely, an administrator must use a web browser or SSH[30] client to enter the IP address or hostname of an OA, iLO, or VC module. An administrator may also manage the TOE locally over a serial connection.

Figure 5 shows the details of the VC Mode deployment configuration of the TOE.

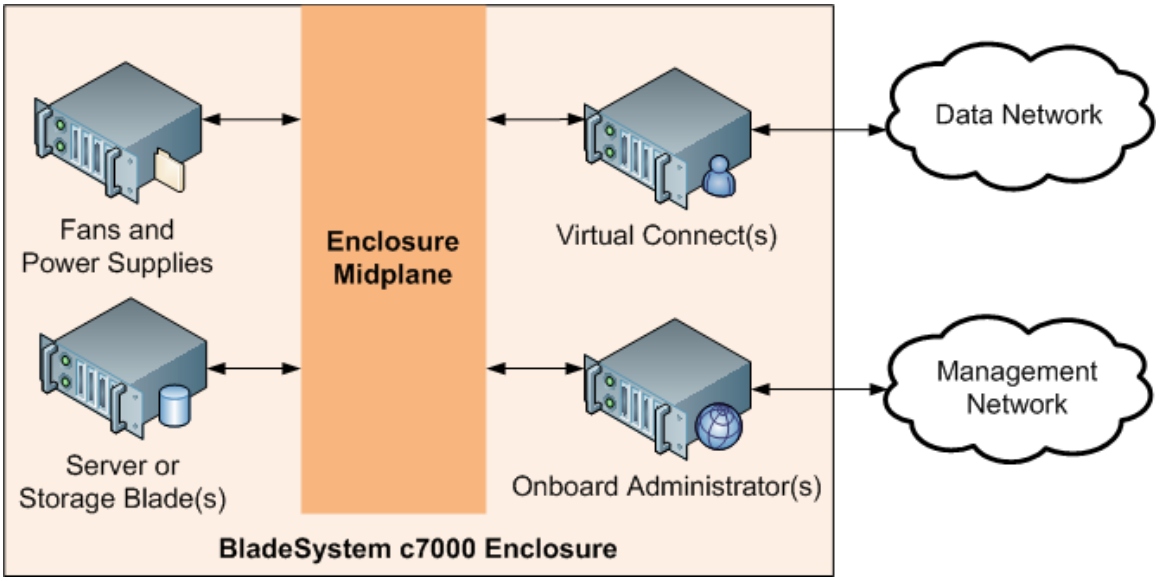

Figure 5 – VC Mode Deployment Configuration of the TOE

Figure 6 shows the details of the Non-VC Mode deployment configuration of the TOE.

[26] Only HP iLO for ProLiant server blades is part of the evaluated configuration.
[27] DDR2 – Double Data Rate 2
[28] KVM – Keyboard-Video-Mouse
[29] All OA modules provide support for KVM. The c3000 achieves KVM support using an attached link board located at the rear of the chassis. The KVM interface on the c7000 is integrated directly into the OA module. Prior c7000 OA modules did not support this feature.
[30] SSH – Secure Shell

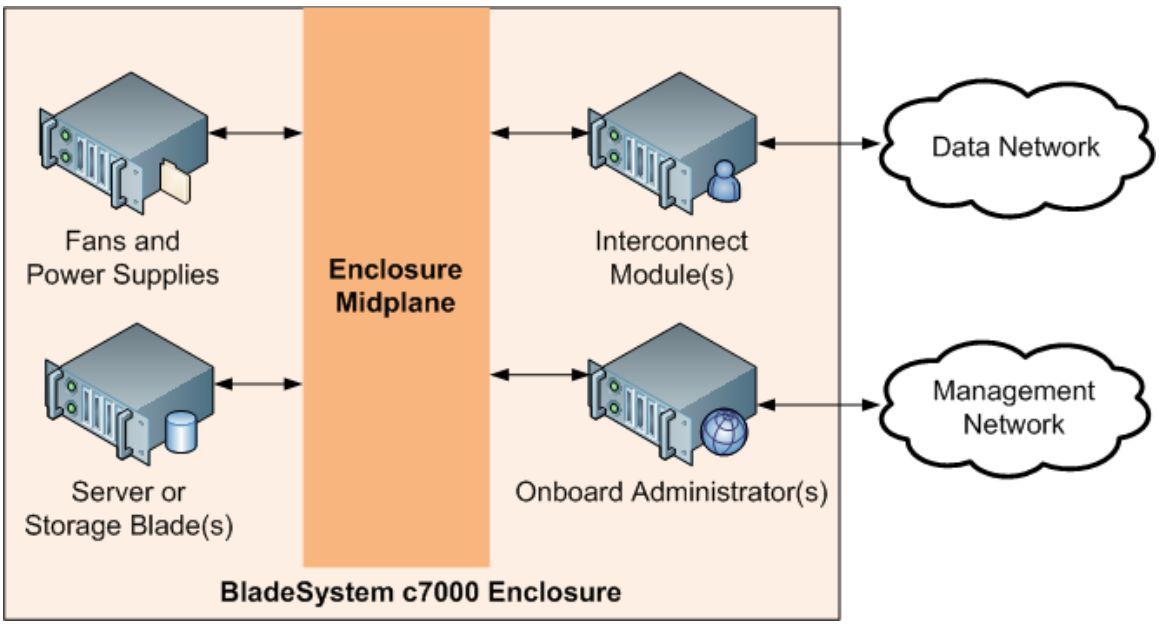

Figure 6 – Non-VC Mode Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a secure LAN with external workstations and servers managed by administrators operating under security policies consistent with those enforced by the administrators of the TOE. Table 3 lists the servers and their requirements to setup the TOE Environment:

Table 3 – TOE Environment

Device	Requirements
LDAP[31] Server	LDAPv3 (RFC[32] 4511)
SNMP Server	SNMPv3 (RFC 3411 - RFC 3418)
SNTP[33] Server	SNTPv4 (RFC 5905)

The LDAP server is used by OA, iLO, and VC for authenticating and identifying TOE users to assign their required roles. Communications for the LDAP server are sent over TLS[34]. The SNMP server, running SNMPv3, provides support for remote monitoring of the enclosure's health. The OA and VC devices will send SNMP traps to the SNMP server that contains encrypted data about the health of the enclosure and components. The SNMP alerts are used to actively notify administrators of critical errors or security incidents related to the TOE. 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 TOE users when interfacing with the TOE. The following third party software is required when interfacing with the TOE:

- Java Runtime Environment – Minimum version of 1.4.2_13; Recommended to use the latest

[31] LDAP – Lightweight Directory Access Protocol
[32] RFC – Request for Comments
[33] SNTP – Simple Network Time Protocol
[34] TLS – Transport Layer Security

- Adobe Flash Player – Minimum version of 11.2; Recommended to use the latest
- Microsoft .NET Framework – Minimum version of the 3.5; Recommended to use 4.5
- At least one of the following supported web browsers:
    - For OA interfaces:
        - Microsoft Internet Explorer 8.x, 9.x, 10.x, and 11.x
        - Mozilla Firefox ESR[35] 17.x and ESR 24.x
        - Google Chrome (latest version)
    - For iLO interfaces:
        - Microsoft Internet Explorer 8.x and 11.x
        - Mozilla Firefox ESR 24.x
        - Google Chrome (latest version)
    - For VC interfaces:
        - Microsoft Internet Explorer 10.x and 11.x
        - Mozilla Firefox ESR 31.x and 33.x

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 7 and Figure 8 illustrate the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

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

- BladeSystem c7000 or c3000 enclosure and support hardware (such as fans and power supplies)
- OA software and hardware
- VC software and hardware (VC Mode)
- HP pass-through interconnect module(s) (Non-VC Mode)
- Server Blade software and hardware (with iLO installed)
- TOE Environment servers listed in section 1.4.1
- External network(s) (not included in the TOE boundary)

[35] ESR – Extended Support Release

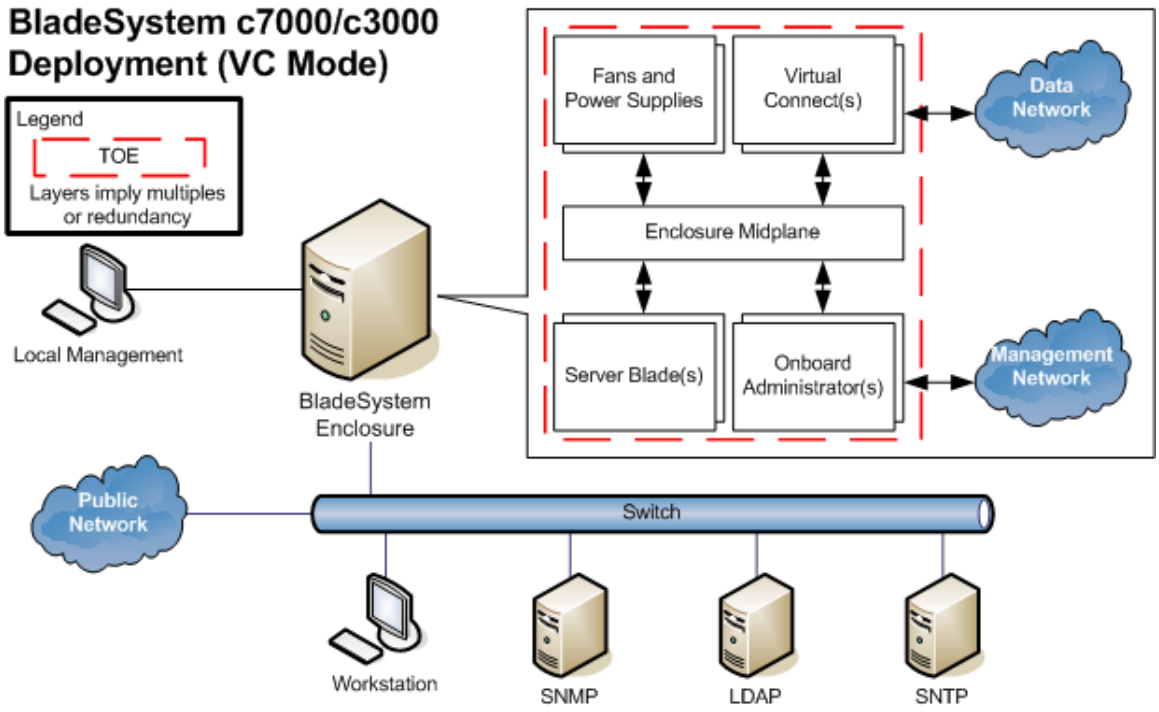

Figure 7 – Physical TOE Boundary – VC Mode

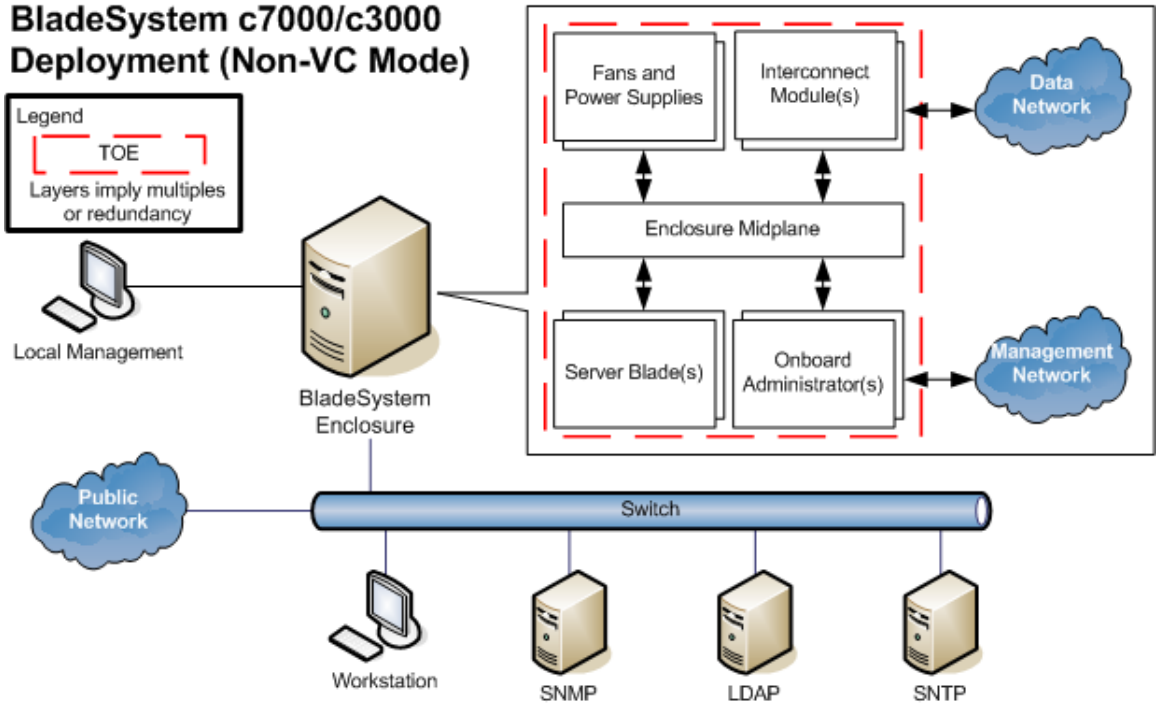

Figure 8 – Physical TOE Boundary – Non-VC Mode

1.5.1.1 Guidance Documentation

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

- Architecture and Technologies in the HP BladeSystem c3000 Enclosure; HP Part Number: 4AA4-8129ENW; Published: August 2013
- Architecture and Technologies in the HP BladeSystem c7000 Enclosure; HP Part Number: 4AA4-8125ENW; Published: August 2013
- HP BladeSystem c3000 Enclosure Quick Setup Instructions; HP Part Number: 446990-005; Published: October 2011; Edition: 5
- HP BladeSystem c3000 Enclosure Setup and Installation Guide; HP Part Number: 446987-005; Published: February 2013; Edition: 5
- HP BladeSystem c7000 Enclosure Quick Setup Instructions; HP Part Number: 411762-403; Published: February 2013; Edition: 12
- HP BladeSystem c7000 Enclosure Setup and Installation Guide; HP Part Number: 411272-401; Published: February 2013; Edition: 10
- HP BladeSystem c-Class Solution Overview; HP Part Number: 413339-006; Published: March 2012; Edition: 6
- HP ProLiant Gen8 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 658801-003; Published: November 2013; Edition: 3
- HP ProLiant Gen9 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 795673-001; Published: September 2014; Edition: 1
- Pass-Thru Installation Instructions for HP c-Class BladeSystem; HP Part Number: 413280-002; Published: June 2011; Edition: 2
- HP iLO 4 Release Notes 2.10; HP Part Number 684917-403; Published: March 2015; Edition: 1
- HP iLO 4 Scripting and Command Line Guide; HP Part Number 684919-009; Published: March 2015; Edition: 1
- HP iLO 4 User Guide; HP Part Number: 684918-009; Published: March 2015; Edition: 1
- HP iLO Federation User Guide; HP Part Number: 767159-003; Published: March 2015; Edition: 1
- HP Integrated Light-Out (iLO) QuickSpecs (Overview); HP Part Number DA-14276; Published: March 2015; Edition: 12
- Managing HP Servers Using the HP RESTful[36] API[37] for iLO; HP Part Number 795538-002; Published: March 2015; Edition: 1
- HP BladeSystem Onboard Administrator 4.40 Release Notes; HP Part Number: 778713-002; Published: March 2015; Edition: 2
- HP BladeSystem Onboard Administrator Command Line Interface User Guide; HP Part Number: 695523-007; Published: March 2015; Edition: 25
- HP BladeSystem Onboard Administrator User Guide; HP Part Number: 695522-008; Published: March 2015; Edition: 23
- HP BladeSystem c-Class Virtual Connect Support Utility Version 1.11.0 User Guide; HP Part Number: 805652-001; Published: February 2015; Edition: 1
- HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide Version 4.40; HP Part Number: 798321-001; Published: February 2015; Edition: 1
- HP Virtual Connect 4.40 Release Notes; HP Part Number: 798319-002; Published: March 2015; Edition: 2
- HP Virtual Connect for c-Class BladeSystem Version 4.40 User Guide; HP Part Number: 798322-001; Published: February 2015; Edition: 1
- HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version 4.40 User Guide; HP Part Number: 798320-001; Published: February 2015; Edition: 1
- Hewlett Packard Enterprise Development LP; BladeSystem c7000 and c3000; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: 1.7

[36] REST – Representational State Transfer
[37] API – Application Programming Interface

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements 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[38]
- Resource Utilization
- TOE Access

1.5.2.1 Security Audit

The TOE generates audit records for the startup and shutdown of the audit function, all administrative events, and critical system events and status events. 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 three FIPS 140-2 validated cryptographic modules that implement the AES[39], 3DES[40], SHA[41], RSA[42], and DSA[43] algorithms for OA, VC, and iLO. These cryptographic algorithms are used to secure management traffic between the administrators and the TOE. Communications sent to the LDAP and SNMP servers are also secured using the TOE's cryptographic modules.

1.5.2.3 User Data Protection

When OA, VC, or iLO 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 OA's the default Administrator account's password. To clear the OA's the default Administrator account's password the Lost Password/Flash Disaster Recovery (LP/FDR) mode must be used.

The TOE enforces three Security Functional Policies (SFPs):

- Management Access Control SFP
- VC Information Flow Control SFP (VC Mode Only)
- iLO Information Flow Control SFP

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

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

1.5.2.4 Identification and Authentication

The OA and VC components have a minimum password complexity and minimum password length specified for user authentication. The iLO component has a minimum password length specified for user authentication. The TOE provides basic enclosure information on the OA login page and access to the help links on the login page to OA, VC, and iLO, administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the LDAP server, the TOE is able to identify and authenticate users that use directory services.

1.5.2.5 Security Management

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

Administrators of the TOE can be authenticated directly by the TOE using an ID and password. 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. Administrators are assigned a "privilege level" (or role) and are also 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 OA component or the VC (VC Mode only) component through their 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 users; however, iLO also provides its own set of local user accounts and privilege levels to authenticate users directly interfacing with it, and 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 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 and thus provide uninterrupted service.

The OA, VC, and iLO components each provide reliable timestamps. iLO will be synchronized to an SNTP server for its reliable timestamp.

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 and thus ensuring the TOE's operations during the failure.

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 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 administrator inactivity.

1.5.3 Product Functionality not included in the TSF

Features and Functionality that are not part of the evaluated configuration of the TOE are:

- SNMP inbound GET/SET requests
- All iLO SNMP messages
- Remote CLI via Telnet session

- XML[44] Reply
- iLO and VC "System Maintenance Switches"
- ProLiant Server Blade operating systems
- Utility Ready Blades (URB)
- Insight Display and KVM (locked in FIPS mode)
- HP Online Configuration Utility (HPONCFG)
- HP Systems Management agent/driver
- Connecting to an IRS device using HP Insight Online
- iLO iOS application
- iLO Andriod application
- OA running with IPv6 enabled

[44] XML – eXtensible Markup Language

2 Conformance Claims

This section and Table 4 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

CC Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[45] as of April 15, 2015 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None.
EAL	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

[45] 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 with 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 three 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.)

All 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	A TOE user or attacker, who is not a TOE user, 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 a TOE user or attacker, could go undetected or could cause a breach of the TSF.
T.MASQUERADE	A user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	An unauthorized user 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 users.

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 software 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.ADMIN	The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must securely record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail. The TOE must act to preserve the most recent audit records in case of audit storage exhaustion.
O.AUTHENTICATE	The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must display a logon banner to users prior to their access of the system, and must handle idle administrative sessions and failed login attempts in a secure manner.
O.ACCESS	The TOE must ensure that only authorized users may access and configure the product
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 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.

Name	Description
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 TOE 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 Security Target reader.

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

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 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(a)	Audit data generation	✓	✓		✓
FAU_GEN.1(b)	Audit data generation (VC Mode Only)	✓	✓		✓
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(a)	Subset access control		✓		✓
FDP_ACC.1(b)	Subset access control (VC Mode only)		✓		✓
FDP_ACF.1	Security attribute based access control		✓		
FDP_IFC.1(a)	Subset information flow control (VC to Server Blade – VC Mode only)		✓		✓
FDP_IFC.1(b)	Subset information flow control (OA to iLO)		✓		✓

Name	Description	S	A	R	I
FDP_IFF.1(a)	Simple security attributes (VC to Server Blade – VC Mode only)		✓		✓
FDP_IFF.1(b)	Simple security attributes (OA to iLO)		✓		✓
FDP_RIP.1	Subset residual information protection	✓	✓		
FIA_SOS.1(a)	Verification of secrets		✓		✓
FIA_SOS.1(b)	Verification of secrets (VC Mode only)		✓		✓
FIA_UAU.1	Timing of authentication		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (VC Mode only)	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialization	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialization (VC Mode only)	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1(a)	Security roles		✓		✓
FMT_SMR.1(b)	Security roles		✓		✓
FMT_SMR.1(c)	Security roles (VC Mode only)		✓		✓
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(a) Audit data generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1(a).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 OA and iLO interfaces; critical system events and status*].
FAU_GEN.1(a).2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

FAU_GEN.1(b) Audit data generation (VC Mode only)
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1(b).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 VC interface; critical system events and status*].
FAU_GEN.1(b).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 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' column of Table 12*] that meet the following: [*FIPS 197, FIPS 46-3, FIPS 180-3, and FIPS 186-3*].

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

FCS_CKM.4.1

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

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

FCS_COP.1.1

The TSF shall perform [*the operation in the 'Cryptographic Operation' column of Table 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' column of Table 12*] that meet the following: [*FIPS 140-2*].

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

Module	Algorithm	Key Sizes (bits)	Cryptographic Operation	Certificate No.
OA	AES – CBC[46], CTR[47] mode	128, 192, 256	Encryption/Decryption	3333
	AES – GCM[48] mode	128, 192, 256	Encryption/Decryption/ Generation/Verification	3333
	3DES – CBC mode	(3) 56	Encryption/Decryption	1903
	RSA PKCS[49]#1	2048	Key Generation/ Signature Generation	1712
	RSA PKCS#1	1024, 2048	Signature Verification	1712
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160, 224, 256, 384, 512	Hashing	2766, 2767, and 2768
	HMAC[50] SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	160, 224, 256, 384, 512	Hashing; Message Authentication	2124
	CTR DRBG[51] (AES)	N/A[52]	Random Number Generation	780
iLO	AES – CBC and ECB[53] mode	128, 192, 256	Encryption/Decryption	3400
	AES – OFB[54] mode	128	Encryption/Decryption	3398, 3399, 3401
	AES – GCM mode	128, 192, 256	Encryption/Decryption/ Generation/Verification	3400
	3DES – CBC and ECB mode	(3) 56	Encryption/Decryption	1924
	RSA	2048, 3072	Key Generation/ Signature Generation	1740
	RSA	1024, 1536, 2048, 3072, 4096	Signature Verification	1740
	DSA	2048, 3072	Key Generation/ Signature Generation/ Signature Verification	959

[46] CBC – Cipher Block Chaining
[47] CTR – Counter
[48] GCM – Galois/Counter Mode
[49] PKCS – Public Key Cryptography Standard
[50] HMAC – Hash-based Message Authentication Code
[51] DRBG – Deterministic Random Bit Generator
[52] N/A – Not Applicable
[53] ECB – Electronic Codebook
[54] OFB – Output Feedback

Module	Algorithm	Key Sizes (bits)	Cryptographic Operation	Certificate No.
	ECDSA[55] for P-256 and P-384 curves	256, 384	Public Key Generation/ Public Key Verification/ Signature Generation/ Signature Verification	676
	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	Hashing	2814
	HMAC SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	Hashing; Message Authentication	2169
	CTR DRBG (AES 128-bit)	N/A	Random Number Generation	814
VC	AES – CBC, CTR mode	128, 192, 256	Encryption/Decryption	3334
	AES – GCM mode	128, 256	Encryption/Decryption/ Generation/Verification	3334
	3DES – CBC mode	(3) 56	Encryption/Decryption	1904
	RSA PKCS#1	2048	Key Generation/ Signature Generation/ Signature Verification	1713
	SHA-256, SHA-384, SHA-512	256, 384, 512	Hashing	2769
	HMAC SHA-256, SHA-384, SHA-512	256, 384, 512	Hashing; Message Authentication	2125
	CTR DRBG	N/A	Random Number Generation	776

[55] ECDSA – Elliptical Curve Digital Signature Algorithm

6.2.3 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1(a).1
The TSF shall enforce the [*Management Access Control SFP*] on
[
a) Subjects: Administrators
b) Objects: OA components, iLO components
c) Operations: Access, Configure
].

FDP_ACC.1(b) Subset access control (VC Mode only)
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1(b).1
The TSF shall enforce the [*Management Access Control SFP*] on
[
a) Subjects: Administrators
b) Objects: VC component
c) Operations: Access, 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:
[
Subject attributes:
a) Username
b) Privilege level
c) Component assignments
Object Attributes:
a) 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 Server Blade – VC Mode Only)
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
[
a) Subjects: BladeSystem server blades, external servers and workstations
b) Information: Network data
c) 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
[
a) Subjects: OA users
b) Information: BladeSystem server blade iLO data
c) Operations: Transmit
].

FDP_IFF.1(a) Simple security attributes (VC to Server Blade – VC Mode only)
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:
a) Unique subject identifier
Information Attributes:
a) Unique source identifier
b) 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 administrator configurable rule for that unique source identifier or unique destination identifier permits communication*].
FDP_IFF.1(a).3
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
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:
a) OA user unique identifier
b) OA user component assignment
Information Attributes:
a) BladeSystem server blade 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: [*a TOE user is allowed to transmit iLO data to a BladeSystem server blade via the OA component based on the OA user unique identifier, OA user component assignment, the BladeSystem server blade unique identifier, and if the OA configuration allows the TOE user and server blade 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 [deallocation of the resource from] the following objects: [*authentication information and settings for each iLO processor, OA module, and VC interconnect module*].

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1(a) Verification of secrets
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 OA user interfaces and the iLO user interfaces. Additionally, the OA mechanism shall verify that secrets are composed of at least three of the following four character types: upper case letters, lower case letters, numbers, and symbols*].

FIA_SOS.1(b) Verification of secrets (VC Mode only)
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 and are composed of at least three of the following four character types for the VC user interfaces: upper case letters, lower case letters, numbers, and symbols*].

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

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

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Class FMT: Security Management

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

FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [*listed in the 'Security Functions 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
OA	Administrator	Allows full configuration and access to all TOE functions, including configuration, firmware updates, user management and restoring factory 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
iLO	Administer User Accounts	Allows authorized users to add, modify, and delete local iLO user accounts. It also allows authorized users to alter privileges for all users
	Remote Console Access	Allows authorized users to remotely access the host system Integrated Remote Console and Remote Serial Console, including video, keyboard and mouse control
	Virtual Power and Reset	Allows authorized users to power-cycle or reset the host platform; can diagnose the system using the virtual NMI[56] button
	Virtual Media	Allows an authorized user to use virtual media on the host platform
	Configure iLO 4 Settings	Allows authorized users to configure most iLO 4 settings, including security settings. It enables users to remotely update iLO 4 firmware; Login
VC	Domain	Define local user accounts, passwords, and define roles; Import enclosures; Configure the VC domain; Set domain IP address; Administer SSL[57] certificates; Configure SNMP settings
	Network	Configure network default settings; Create, edit, and delete all network settings and configurations
	Storage	Select World Wide Name (WWN) to be used by the domain; Set up connections to external fabrics
	Server	Create, edit, delete server VC profiles; Assign and unassign profiles to device bays; Power on and power off server blades within enclosures
	User	Can view (but not modify) VC configuration

[56] NMI – Non-Maskable Interrupt
[57] SSL – Secure Sockets Layer

FMT_MSA.1(a) 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(a).1

The TSF shall enforce the [*Management Access Control SFP and iLO 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' column of Table 14*].

Table 14 – Management of Security Attributes

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

Module	Role	Security Attribute Access	Access Type
			Query Modify Delete Create
	Operator	OA user unique identifier	Query
		Privilege Level	Query
		OA user component assignment	Query
	User	OA user unique identifier	Query
		Privilege Level	
		OA user component assignment	Query

Application Note: *Users granted an OA role as defined in the table above are automatically mapped to the same role within iLO. This is only applicable for users accessing iLO through the OA interfaces. iLO maintains its own user database in which users 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", and "Virtual Media" iLO privilege levels. The Administrator includes all Operator privileges, and in addition, grants the "Administer User Accounts", and "Configure iLO Settings" privilege levels.*

FMT_MSA.1(b) Management of security attributes (VC Mode only)
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(b).1

The TSF shall enforce the [*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 15] to [*the authorized identified roles listed under the 'Role' column of Table* 15].

Table 15 – Management of Security Attributes (VC Mode Only)

Module	Role	Security Attribute Access	Access Type
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: *The Administrator role identified in the table above is a generic term that is assumed by users 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(a) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(a).1
The TSF shall enforce the [*Management Access Control SFP and iLO Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(a).2
The TSF shall allow the [*appropriately privileged administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(b) Static attribute initialization (VC Mode only)
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(b).1
The TSF shall enforce the [*VC Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(b).2
The TSF shall allow the [*appropriately privileged 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 list of operations listed in the 'Operations' column of Table 16 to*]] the [*objects listed in the 'Objects' column of Table 16*] to [*the privilege levels listed under the 'Privilege Level' column of Table 16*].

Table 16 – Management of TSF Data

Module	Object	Role/Privilege Level	Operations
OA[58]	Rack Overview	Everyone[59]	View
	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

[58] The OA operations of the Administrator, Operator, and User privilege levels are observed while access to all bays is enabled.
[59] Note that "Everyone" is not a role or privilege level. It refers to all roles and privilege levels managed by the currently referenced part of the TOE.

Module	Object	Role/Privilege Level	Operations
		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/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 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
	Active Onboard Administrator	Everyone	View and manage

Module	Object	Role/Privilege Level	Operations
	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

Module	Object	Role/Privilege Level	Operations
		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
	HP SSO Integration	Administrator	View and manage
	Two-Factor 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
iLO	Overview	Everyone	View
	System Information	Everyone	View
	iLO Event Log	Configure iLO Settings	Clear event logs
		Everyone	View
	Integrated Management Log	Configure iLO Settings	Mark as repaired, add maintenance notes, and clear event logs
		Everyone	View
	Active Health System Log	Configure iLO Settings	Enable/disable logging, and clear event logs
		Everyone	View
	Diagnostics	Configure iLO Settings	Reset iLO
		Virtual Power and Reset	Generate NMI and swap the Read Only Memory (ROM)
		Everyone	View
	Insight Agent	Everyone	View, and launch Insight Agent
	Remote Console	Remote Console Access	Launch remote consoles
		Configure iLO Settings	Reset and save hot key settings
		Everyone	View
	Virtual Media	Virtual Media	Use, eject, and insert media
		Virtual Power and Reset	Reset the server
		Configure iLO Settings	Manage
		Everyone	View

Module	Object	Role/Privilege Level	Operations
	Boot Order	Virtual Media and Configure iLO Settings	Manage (requires both privilege levels)
		Virtual Power and Reset	Reset the server
		Everyone	View
	Server Power	Configure iLO Settings	Manage
		Virtual Power and Reset	Use virtual power buttons
		Everyone	View
	Power Settings	Configure iLO Settings	Manage
		Everyone	View
	iLO Dedicated Network Port	Configure iLO Settings	Manage
		Everyone	View
	Registration	Configure iLO Settings	Manage
		Everyone	View
	Service Events	Configure iLO Settings	Manage
		Everyone	View
	Data Collections	Configure iLO Settings	Manage
		Everyone	View
	Firmware	Configure iLO Settings	Manage
		Everyone	View
	Licensing	Configure iLO Settings	Manage
		Everyone	View
	User Administration	Configure iLO Settings	Manage directory groups
		Administer User Accounts	Manage users
		Everyone	View, change personal password
	Access Settings	Configure iLO Settings	Manage
		Everyone	View
	Security	Administer User Accounts	Manage (only Secure Shell Keys)
		Configure iLO Settings	Manage (all except for Secure Shell Keys)
		Everyone	View
	Management	Configure iLO Settings	Manage
		Everyone	View
	Key Manager	Configure iLO Settings	Manage

Module	Object	Role/Privilege Level	Operations
		Everyone	View
	Active Onboard Administrator	Everyone	View, launch Onboard Administrator's GUI, and toggle the UID[60] light
VC	Home Screen	Everyone	View
	Configure	Domain	View and manage
		Network, Server, Storage, and User[61]	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
	LDAP Settings	Domain	View and manage
		Network, Server, Storage, and User	View
	Radius Settings	Domain	View and manage
		Network, Server, Storage, and User	View
	TACACS+ Settings	Domain	View and manage

[60] UID – Unique Identifier
[61] In VC, the User role is assumed when no privileges are assigned to a user's account.

Module	Object	Role/Privilege Level	Operations
		Network, Server, Storage, and User	View
	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 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

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

FMT_SMF.1 Specification of management functions
Hierarchical to: No other components.
Dependencies: No Dependencies
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
a) Management of security functions behavior;
b) Management of TSF data;
c) Management of security attributes
].

FMT_SMR.1(a) Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1(a).1
The TSF shall maintain the roles [*ADMINISTRATOR, OPERATOR, and USER*] for OA users.
FMT_SMR.1(a).2
The TSF shall be able to associate users with roles.

***Application Note**: The "roles" listed here are called "privilege levels" in BladeSystem vernacular.*

FMT_SMR.1(b) Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1(b).1
The TSF shall maintain the roles [*ADMINISTER USER ACCOUNTS, REMOTE CONSOLE ACCESS, VIRTUAL POWER AND RESET, VIRTUAL MEDIA, CONFIGURE iLO 4 SETTINGS*] for iLO users.
FMT_SMR.1(b).2
The TSF shall be able to associate users with roles.

***Application Note**: The "roles" listed here are called "privilege levels" in BladeSystem vernacular.*

FMT_SMR.1(c) Security roles (VC Mode only)
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1(c).1
The TSF shall maintain the roles [*DOMAIN, NETWORK, STORAGE, SERVER, and USER*] for VC users.
FMT_SMR.1(c).2
The TSF shall be able to associate users with roles.

***Application Note**: The "roles" listed here are called "privilege levels" in BladeSystem vernacular.*

***Application Note**: The "USER" role is assigned by default, and provides 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*].

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 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 OA and iLO*]].
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 [*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 components*]].

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 administrator inactivity*].

Application Note: *FTA_SSL.3 is enforced by OA (GUI, CLI, and SOAP[62] interfaces), iLO (CLI, GUI and Remote Consoles), and VC (GUI and 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 OA (GUI and CLI interfaces), iLO (GUI only), and VC (GUI and 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 OA (GUI and SOAP interfaces), and iLO (CLI, REST API, and GUI). All other external interfaces, including VC interfaces, are excluded from the scope.*

[62] SOAP – Simple Object Access Protocol

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 17 summarizes the requirements.

Table 17 – Assurance Requirements

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

7 TOE Security Specification

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

7.1 TOE Security Functions

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 18 lists the security functionality and their associated SFRs.

Table 18 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1(a)	Audit data generation
	FAU_GEN.1(b)	Audit data generation (VC Mode Only)
	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(a)	Subset access control
	FDP_ACC.1(b)	Subset access control (VC Mode only)
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1(a)	Subset information flow control (VC to Server Blade – VC Mode only)
	FDP_IFC.1(b)	Subset information flow control (OA to HP iLO)
	FDP_IFF.1(a)	Simple security attributes (VC to Server Blade – VC Mode only)
	FDP_IFF.1(b)	Simple security attributes (OA to HP iLO)
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_SOS.1(a)	Verification of secrets
	FIA_SOS.1(b)	Verification of secrets (VC Mode only)
	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(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes (VC Mode only)

TOE Security Functionality	SFR ID	Description
	FMT_MSA.3(a)	Static attribute initialization
	FMT_MSA.3(b)	Static attribute initialization (VC Mode only)
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1(a)	Security roles
	FMT_SMR.1(b)	Security roles
	FMT_SMR.1(c)	Security roles (VC Mode only)
Protection of TOE Security Functions	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

In VC Mode, the OA, VC, and iLO TOE components generate audit records for the startup and shutdown of their audit functions, all administrative events, and critical system events and status events that should be seen by administrators. Audit records are stamped with the actual time at which the event occurred. After authenticating to the TOE component, 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.

In Non-VC Mode, VC-related events will not be generated and are not present in the audit records. All other audit functionality in Non-VC Mode is identical to VC Mode audit functionality.

TOE Security Functional Requirements Satisfied: FAU_GEN.1(a), FAU_GEN.1(b), FAU_SAR.1, FAU_STG.1, and FAU_STG.4

7.1.2 Cryptographic Support

The TOE implements three FIPS 140-2 validated cryptographic modules (OA, VC, and iLO) that implement the AES, 3DES, SHA, RSA, and DSA algorithms. These cryptographic algorithms are used to secure management traffic between the administrators and the TOE. The OA, VC (VC Mode only), and iLO web interfaces are protected via the TLS protocol. The OA, VC (VC Mode only), and iLO command line interfaces are protected via the SSH protocol. Communications sent to the LDAP and SNMP servers are also secured using the TOE's cryptographic modules. The OA, VC (VC Mode only), and iLO devices will connect to the LDAP server using TLS to form LDAPS when identifying and authenticating TOE users. The OA and VC devices will send SNMPv3 traffic to the SNMP server that contains encrypted user data. The OA, VC, and iLO 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, FCS_COP.1

7.1.3 User Data Protection

When an authorized administrator triggers an iLO reset to factory defaults, this ensures any previous authentication information and settings for each iLO managed blade 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 are cleared from storage except for the default Administrator account's password. To de-allocate the default Administrator account's password the LP/FDR mode must be used. Once a FIPS transition is initiated in OA, the 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 that 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:

- Management Access Control SFP
- VC Information Flow Control SFP (VC Mode only)
- iLO Information Flow Control SFP

7.1.3.1 Management Access Control SFP

The Management Access Control SFP ensures that only authorized and appropriately privileged administrators can access or configure the TOE via the OA, VC (VC Mode only), and iLO components. The Management Access Control SFP governs the use of the Management TSF, described above. The TOE determines which administrators are allowed to access which OA, VC (VC Mode only), and iLO components (and to perform which operations on them) via an administrator's associated *username*, *privilege level*, and *component assignments*.

A *username* is an administrator's unique identifier within the TOE.

An OA user can have one of three *privilege levels*:

- **ADMINISTRATOR**: allows full configuration and access of all aspects of the TOE, including configuration, firmware updates, user 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 user 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.

Administrators have one or more *component assignments*, which are associations or bindings of the administrator to specific BladeSystem components (such as enclosure bays, VC modules, server blades, 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 component serial number or the enclosure bay in which a component is installed.

7.1.3.2 VC Information Flow Control SFP (VC Mode only)

The VC Information Flow SFP ensures that server blades within the enclosure only communicate with other internal server blades or entities on the external network(s) for which they have been configured by an administrator to communicate. The TOE determines which BladeSystem server blades and 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 administrator.[63]

The TOE controls information flow to ensure that server blades are permitted to transmit data to external networks only when explicitly assigned a profile[64] 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[65] 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 user 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.

7.1.3.3 iLO Information Flow Control SFP

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

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

[63] For example, a rule might specify that a server blade in bay #1 is allowed to communicate via an installed VC with a storage blade in bay #3, but that the server blade cannot communicate with another server blade in bay #2. Rules can be based on many types of source and destination identifiers, including IP address, media access control (MAC) address, etc. For detailed information about VC configuration and rules, information please refer to the VC administrative manuals.
[64] Profile – A collection of device-independent network and storage connection settings
[65] VLAN – Virtual Local Area Network

7.1.4 Identification and Authentication

Administrators can configure the TOE to require passwords for OA and VC (VC Mode only) of specific minimum character complexity and length. Administrators can also configure password length requirements for the iLO interfaces. The TOE provides basic enclosure information on the OA login page and access to the help links of OA, VC, and iLO. The OA login page provides a link to help about logging into OA (depicted as a question mark "?" in a box) and information about the enclosure that OA is connected to. The VC login page provides the "Sign-in help" link that displays helpful information about logging into VC. The iLO login page provides a link to help about logging into iLO (depicted as a question mark "?" in a box). Administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. Using the LDAP server, iLO, OA, and VC (VC Mode only) device are able to identify and authenticate users that use directory services.

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

7.1.5 Security Management

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

Administrators of the TOE can be authenticated directly by the TOE using an ID and password. Administrators of the TOE can also be authenticated by an external authentication server. 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.

Administrators are assigned a "privilege level" (sometimes called a "role") and are also 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 OA, iLO and VC (VC Mode only) components through their enforcement of the Management Access Control Security Functional Policy and VC Information Flow Control Policy.

Each of the OA, iLO, and VC management interfaces may be directly accessed by authorized users. For OA users however, roles are directly mapped to iLO privilege levels. To access iLO's management functions, OA provides a login bypass feature for currently authenticated users; however, iLO also provides its own set of local user accounts and privilege levels to authenticate users directly interfacing with it, and 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; however, 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(a),FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1(a), FMT_SMR.1(b), FMT_SMR.1(c)

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 OA, VC, and iLO cryptographic algorithms and cryptographic modules on the whole to ensure their proper function. During the power-up, the TOE performs the following self-tests: firmware integrity test, Known

Answer Tests (KATs) in hardware, 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[66] 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 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 OA, VC, and iLO 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 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 and thus provide 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 timestamps. 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), 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

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

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

[66] SP – Special Publication

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

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

Table 19 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.CONFIG A TOE user or attacker, who is not a TOE user, could improperly gain access to user data if the product is misconfigured or does not enforce proper roles and permissions.	O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) 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.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must display a logon banner to users prior to their access of the system, and must handle idle administrative sessions and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that the TOE has identified and authenticated a user before he is allowed to access any data.
	O.ACCESS The TOE must ensure that only authorized users may access and configure the product	O.ACCESS counters this threat by ensuring that administrators properly configure access control for users of the TOE, and to always enforce this access control while in the evaluated configuration.

Threats	Objectives	Rationale
T.FAILURE_OR_TAMPER Physical failure or tampering of a TOE component, by a TOE 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 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 A 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 users prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must display a logon banner to users prior to their access of the system, and must handle idle administrative sessions and failed login attempts in a secure manner.	O.AUTHENTICATE ensures that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
T.UNAUTH An unauthorized user 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 TOE users with the appropriate privileges (and only those TOE users) may exercise such control.	O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must securely record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail. The TOE must act to preserve the most recent audit records in case of audit storage exhaustion.	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.

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

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

8.2.2 Security Objectives Rationale Relating to Policies

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

Table 20 – Policies: Objectives Mapping

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

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

8.2.3 Security Objectives Rationale Relating to Assumptions

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

Table 21 – Assumptions: Objectives Mapping

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

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended 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 22 below shows a mapping of the objectives and the SFRs that support them.

Table 22 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must ensure that only authorized users may access and configure the product	FDP_ACC.1(a) Subset access control	The requirement meets this objective by ensuring that all administrators of the OA and HP iLO components are controlled by the Management Access Control SFP.
	FDP_ACC.1(b) Subset access control (VC Mode only)	The requirement meets this objective by ensuring that all administrators of the VC component 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 administrators are controlled by the Management Access Control SFP.
	FDP_IFC.1(a) Subset information flow control (VC to Server Blade – VC Mode only)	The requirement meets this objective by ensuring that all administrators are controlled by the Virtual Control Information Flow Control SFP.
	FDP_IFC.1(b) Subset information flow control (OA to HP iLO)	The requirement meets this objective by ensuring that all administrators are controlled by the HP iLO Information Flow Control SFP.
	FDP_IFF.1(a) Simple security attributes (VC to Server Blade – VC Mode only)	The requirement meets this objective by ensuring that all administrators are controlled by the Virtual Control Information Flow Control SFP.
	FDP_IFF.1(b) Simple security attributes (OA to HP iLO)	The requirement meets this objective by ensuring that all administrators are controlled by the HP iLO Information Flow Control SFP.

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) 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(a) Subset access control	The requirement meets this objective by ensuring that all administrators of the OA and HP iLO components are controlled by the Management Access Control SFP.
	FDP_ACC.1(b) Subset access control (VC Mode only)	The requirement meets this objective by ensuring that all administrators of the VC component 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 administrators 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 administrators with the appropriate privileges.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1(a) Management of security attributes	The requirement meets the objective by ensuring that the TOE enforces the Management Access Control SFP and HP iLO Information Flow Control to restrict the ability to manipulate security attributes to only those administrators with the appropriate privileges.
	FMT_MSA.1(b) Management of security attributes (VC Mode only)	The requirement meets the objective by ensuring that the TOE enforces the VC Information Flow Control SFP to restrict the ability to manipulate security attributes to only those administrators with the appropriate privileges.
	FMT_MSA.3(a) 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 and HP iLO Information Flow Control SFP.
	FMT_MSA.3(b) Static attribute initialization (VC Mode only)	The requirement meets the objective by ensuring that the TOE creates restrictive default values for security attributes that are used to enforce the 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 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(a) Security roles	The requirement meets the objective by ensuring that the TOE associates administrators with roles to provide access to TSF management functions and data.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.1(b) Security roles	The requirement meets the objective by ensuring that the TOE associates administrators with roles to provide access to TSF management functions and data.
	FMT_SMR.1(c) Security roles (VC Mode only)	The requirement meets the objective by ensuring that the TOE associates administrators with roles to provide access to TSF management functions and data while in VC mode.
	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 record events of security relevance at the "not specified level" of audit. The TOE must securely record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail. The TOE must act to preserve the most recent audit records in case of audit storage exhaustion.	FAU_GEN.1(a) 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 OA and HP iLO interfaces.
	FAU_GEN.1(b) Audit data generation (VC Mode Only)	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 VC interface.
	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 timestamps for its own use.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must identify authorized administrators prior to allowing access to manipulate data. The TOE must display a logon banner to users prior to their access of the system, and must handle idle administrative sessions and failed login attempts in a secure manner.	FDP_ACC.1(a) Subset access control	The requirement meets this objective by ensuring that all administrators of the OA and HP iLO components are controlled by the Management Access Control SFP.
	FDP_ACC.1(b) Subset access control (VC Mode only)	The requirement meets this objective by ensuring that all administrators of the VC component 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 administrators are controlled by the Management Access Control SFP.
	FIA_SOS.1(a) Verification of secrets	The requirement meets this objective by ensuring that administrator passwords are of sufficient complexity and length.
	FIA_SOS.1(b) Verification of secrets (VC Mode only)	The requirement meets this objective by ensuring that user passwords are of sufficient complexity and length.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that 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 administrators are identified before access to TOE functions is allowed.
	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing access to administrative functions to ensure that only appropriately privileged administrators may manage the security behavior of the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1(a) Management of security attributes	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged administrators may do so.
	FMT_MSA.1(b) Management of security attributes (VC Mode only)	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged administrators may do so.
	FMT_MSA.3(a) Static attribute initialization	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged administrators may do so.
	FMT_MSA.3(b) Static attribute initialization (VC Mode only)	The requirement meets the objective by ensuring that the TOE authenticates administrators prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged administrators may do so.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized administrators are allowed access to manipulate security attributes and applications.
	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.

Objective	Requirements Addressing the Objective	Rationale
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that administrators can configure an advisory warning message which will be displayed on the management interfaces when an 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 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 23 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 23 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1(a)	FPT_STM.1	✓	
FAU_GEN.1(b)	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_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1(a)	FDP_ACF.1	✓	
FDP_ACC.1(b)	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	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UID.1	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FMT_SMF.1	✓	
	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.3(a)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1(a)	FIA_UID.1	✓	
FMT_SMR.1(b)	FIA_UID.1	✓	
FMT_SMR.1(c)	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

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

Table 24 – Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AHS	Active Health System
API	Application Programming Interface
BIOS	Basic Input/Output System
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPU	Central Processing Units
CTR	Counter Mode
DDR2	Double Data Rate 2
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVD	Digital Video Disk
EAL	Evaluation Assurance Level
ECDSA	Elliptical Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
ERS	Embedded Remote Support
ESR	Extended Support Release
FC	Fibre Channel
FIPS	Federal Information Processing Standard
FRU	Field-Replaceable Unit
Gb	Gigabit
GB	Gigabyte
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HA	High Availability

Acronym	Definition
HBA	Host Bus Adapter
HMAC	Hash-based Message Authentication Code
HPONCFG	HP Online Configuration Utility
I2C	Inter-Integrated Circuit
ID	Identification
iLO	Integrated Lights-Out
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRS	Insight Remote Support
iSCSI	Internet Small Computer System Interface
IT	Information Technology
KAT	Known Answer Test
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LP/FDR	Lost Password/Flash Disaster Recovery
MAC	Media Access Control
Mb	Megabit
N/A	Not Applicable
NAND	Negated AND
NIC	Network Interface Card
NMI	Non-Maskable Interrupt
OA	Onboard Administrator
OFB	Output Feedback
OSP	Organizational Security Policy
PKCS	Public Key Cryptography Standard
PP	Protection Profile
REST	Representational State Transfer
RFC	Request for Comments
RJ	Registered Jack
RSA	Rivest, Shamir, Adleman
SAN	Storage Area Network

Acronym	Definition
SAR	Security Assurance Requirement
SCSI	Small Computer Systems Interface
SD	Secure Digital
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SNTP	Simple Network Time Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
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