Hewlett-Packard Development Company, L.P.

BladeSystem c7000 and c3000

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 1.16

Prepared for:

Hewlett-Packard Development Company, L.P.
20555 State Highway 249
Houston, TX 77070
United States of America

Phone: +1 281 370 0670
http://www.hp.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
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 Summary 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 - ST and TOE References

ST Title	Hewlett-Packard Development Company, L.P. BladeSystem c7000 and c3000 Security Target
ST Version	Version 1.16
ST Author	Corsec Security, Inc.
ST Publication Date	December 9, 2013
TOE Reference	HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (running firmware version 3.71 build 12/07/2012 @ 13:26), Virtual Connect (running firmware version 4.01), and HP Integrated Lights-Out 3 (version 1.50)
FIPS 140-2 Status	Includes Level 1 validated crypto modules, certificate nos. 2173 , and 2174, and CAVP-validated algorithms (see Table 11).

[1] I/O: Input/Output

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 attached to a storage network to provide bootable storage media. Storage, server, and other option blades include HP Integrated Lights-Out (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. These interconnect modules include Virtual Connect modules (discussed below).
- Up to 10 Active Cool 200 fan kits.
- Up to six power supplies.

- Redundant Onboard Administrator (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 HP Integrated Lights-Out (iLO) technology (discussed below).
- Up to four interconnect modules simultaneously supporting a variety of network interconnect fabrics such as Ethernet, Fibre Channel, InfiniBand, Internet Small Computer System Interface (iSCSI), or Serial-attached SCSI. These interconnect modules include Virtual Connect modules (discussed below).
- Up to six Active Cool 200 fan kits.
- Up to six power supplies.
- Single Onboard Administrator (OA) management module.

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 Onboard Administrator, Virtual Connect, and iLO components. These components provide the majority of BladeSystem functionality.

1.3.2 Onboard Administrator

Figure 2 - HP BladeSystem Onboard Administrator Module (Example)

The heart of c-Class enclosure management is the Onboard Administrator module (shown in Figure 2 above) located in the enclosure. The Onboard Administrator 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 Onboard Administrator in the c7000 and c3000 enclosures provide complete redundancy for these functions.

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[2] panel included in the front of the c7000 and c3000 enclosures.

[2] LCD: Liquid Crystal Display

1.3.2.1 Detecting component insertion and removal

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

1.3.2.2 Identifying components

To identify a component, the Onboard Administrator 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 Onboard Administrator 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 Onboard Administrator reads the FRU EEPROMs directly. The Onboard Administrator accesses server blade FRU EEPROMs through their Integrated Lights-Out (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 Onboard Administrator. Server blade management functions include auto login to the Integrated Lights-Out 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[3] and iLO firmware versions, server name, NIC and option card port IDs, and port mapping. The Onboard Administrator provides easy-to-understand port mapping information for each of the server blades and interconnect modules in the enclosure.

From the NIC and mezzanine option FRU information, the Onboard Administrator determines the type of interconnects each server requires. For interconnect modules, the Onboard Administrator 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 Onboard Administrator tasks are power control and thermal management. The Onboard Administrator 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 Onboard Administrator 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 Onboard Administrator begins thermal management with Thermal Logic. The Thermal Logic feature in the c-Class enclosures minimizes fan subsystem power consumption by reading 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 Onboard Administrator uses embedded management interfaces to provide detailed information and health status for all bays in the enclosure. The Onboard Administrator also reports firmware versions for most components in the enclosure and can be used to update those components.

[3] BIOS: Basic Input/Output System

1.3.2.4.1 Internal management interfaces

The Onboard Administrator monitors and communicates with each bay in the enclosure via several hardware interfaces. The management hardware interfaces include unique presence pins[4], 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 Onboard Administrator. The primary external management interface is the management port for each Onboard Administrator, which is an RJ-45[5] jack providing Ethernet communications not only to each Onboard Administrator, 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 Virtual Connect Manager. For redundant Onboard Administrators, both Onboard Administrator management ports are connected to the management network, providing redundant management network connections to each enclosure.

A serial port on each Onboard Administrator module provides full out-of-band CLI access to the Onboard Administrator and is used for Onboard Administrator firmware flash recovery. USB[6] ports on the Onboard Administrator 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[7] 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 c7000. It requires installing a second Onboard Administrator module in the c7000 enclosure to act as a completely redundant controller in an active-standby mode. Using redundant modules in the c7000 enclosure 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 Onboard Administrator.

1.3.3 Virtual Connect

Figure 3 - HP BladeSystem Virtual Connect Module (Example)

[4] Unique presence pins: Used to detect whether a component is installed within a particular bay
[5] RJ: Registered Jack
[6] USB: Universal Serial Bus
[7] DVD: Digital Versatile Disc

Virtual Connect technology is a set of interconnect modules and embedded software for c-Class enclosures that simplifies the setup and administration of server connections. Figure 3 above shows an example Virtual Connect module. The following Virtual Connect modules are available:

- HP Virtual Connect Flex-10 10 Gb Ethernet Module
- HP Virtual Connect FlexFabric 10 Gb/24-Port Ethernet Module
- HP Virtual Connect Flex-10/10D Module
- HP Virtual Connect Manager software
- HP 1Gb Ethernet Pass-Thru Module for c-Class BladeSystem (Non-VC Mode Only)
- HP 4Gb Fibre Channel Pass-Thru Module for c-Class BladeSystem (Non-VC Mode Only)

HP Virtual Connect offers a unique approach to connecting and adapting server, LAN[8], and SAN[9] 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 Virtual Connect Manager 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 Virtual Connect, an administrator can connect and pre-assign all the LAN and SAN connections that the server pool might ever need. Using Virtual Connect Flex-10 and VC[10] FlexFabric modules and FlexFabric adapters, administrators can choose how many NICs[11] or HBAs[12] are on each server and dynamically set the bandwidth of each connection in increments of 100 Mb[13] between 100 Mb and 10 Gb.

Like other Ethernet and Fibre Channel switches, Virtual Connect modules slide into the interconnect bays of c-Class enclosures. To support Fibre Channel, the enclosure must have at least one Virtual Connect Ethernet module, because the Virtual Connect Manager software runs on a processor that resides on the Ethernet module . Together, HP Virtual Connect modules and the Virtual Connect Manager 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.

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

[8] LAN: Local Area Network
[9] SAN: Storage Area Network
[10] VC: Virtual Connect
[11] NIC: Network Interface Card
[12] HBA: Host Bus Adapter
[13] Mb: Megabits

1.3.4 HP Integrated Lights-Out (iLO)

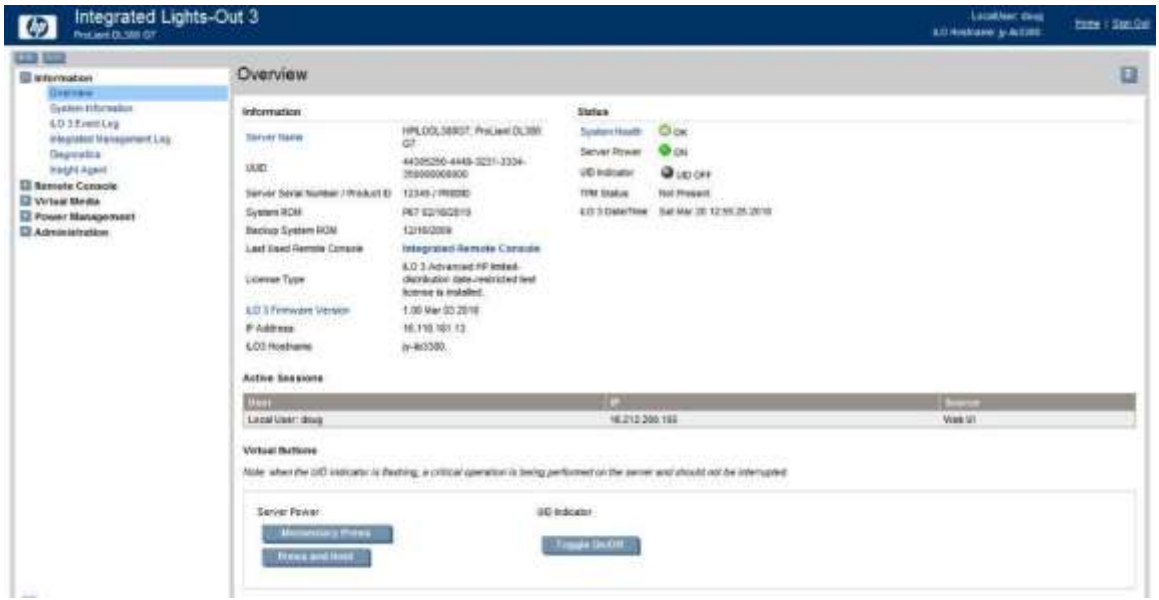

Figure 4 - HP Integrated Light-Out (Example Management Screen)

The Integrated Lights-Out management built into BladeSystem blade servers and storage blades is an autonomous management subsystem embedded directly on the server. iLO monitors each server's overall "health", reports issues, and provides a means for setup and managing of power and thermal settings. iLO is also the foundation of BladeSystem High Availability (HA) embedded server and fault management. iLO also provides system administrators with secure remote management capabilities regardless of server status or location. 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 ProLiant blades include:

- HP ProLiant BL2x220c
- HP ProLiant BL460c
- HP ProLiant BL465c
- HP ProLiant BL490c
- HP ProLiant BL620c
- HP ProLiant BL680c
- HP ProLiant BL685c

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 mediated by the Onboard Administrator GUI.

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 Onboard Administrator modules, one or more Virtual Connect 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 Virtual Connect modules installed in the appliance. The Virtual Connect 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.

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
Virtual Connect	HP Virtual Connect Flex-10 10 Gb Ethernet Module HP Virtual Connect FlexFabric 10 Gb/24-Port Module HP Virtual Connect Flex-10/10D Module
iLO[14]	HP iLO 3 Gromit LP on ProLiant G7 server blades HP iLO 3 Gromit XE on ProLiant G7 server blades
Onboard Administrator	HP BladeSystem c7000 DDR2[15] Onboard Administrator with KVM[16] [17] 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 Onboard Administrator and (in VC Mode) Virtual Connect modules. To access the functions available via these interfaces remotely, an administrator must use a web browser or SSH[18] client to enter the IP[19] address or hostname of an Onboard Administrator or Virtual Connect 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.

[14] Only iLO for ProLiant server blades is part of the evaluated configuration.
[15] DDR2: Double Data Rate 2
[16] KVM: Keyboard-Video-Mouse
[17] All Onboard Administrator modules provide support for KVM. The c3000 acheives 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 Onboard Administrator module. Prior c7000 Onboard Administrator modules did not support this feature.
[18] SSH: Secure Shell
[19] IP: Internet Protocol

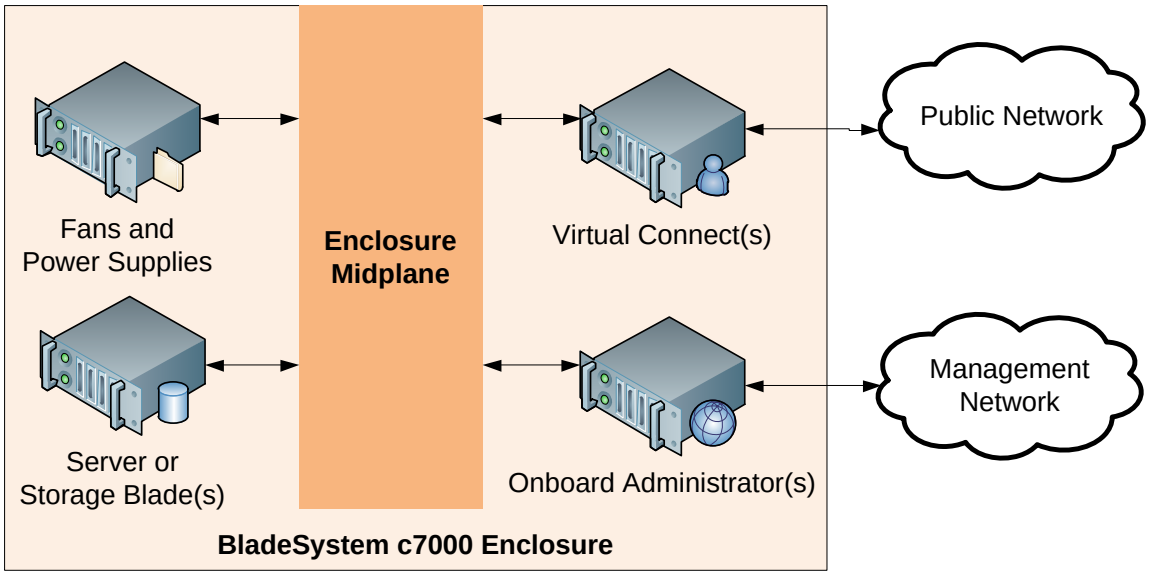

Figure 5 – VC Mode Deployment Configuration of the TOE

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

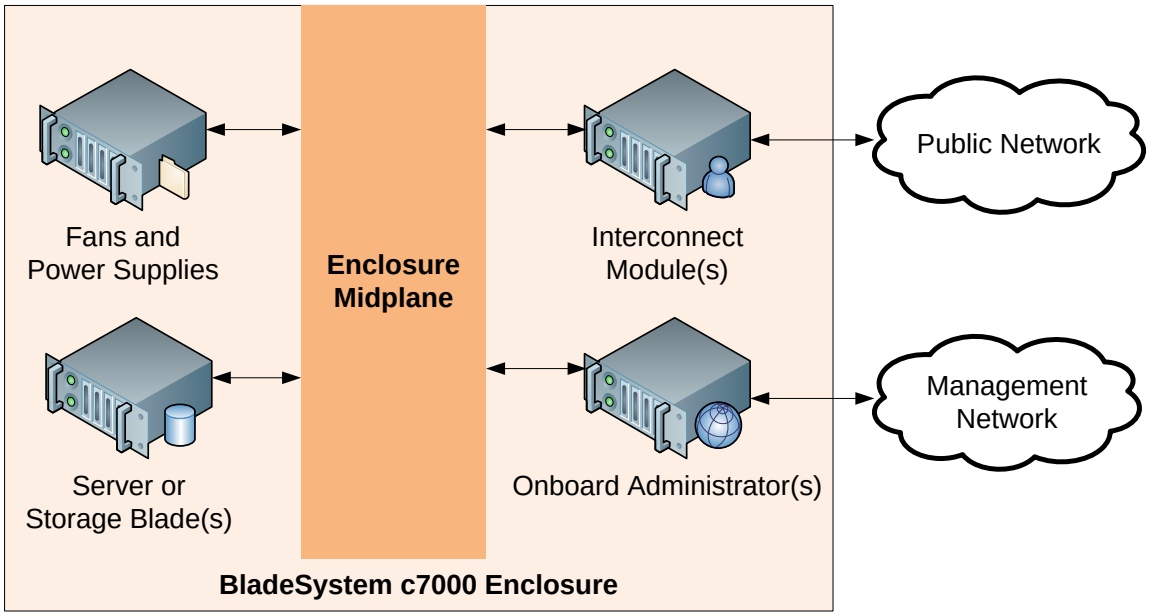

Figure 6 - Non-VC Mode Deployment Configuration of the TOE

1.5 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[20] with external workstations and servers managed by

[20] LAN: Local Area Network

administrators operating under security policies consistent with those enforced by the administrators of the TOE.

1.6 TOE Description

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

1.6.1 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)
- Onboard Administrator software and hardware
- Virtual Connect software and hardware (VC Mode)
- HP pass-through interconnect module(s) (Non-VC Mode)
- Server or Storage Blade software and hardware (with iLO installed)
- NTP and SNTP Servers
- External network(s) (not included in the TOE boundary)

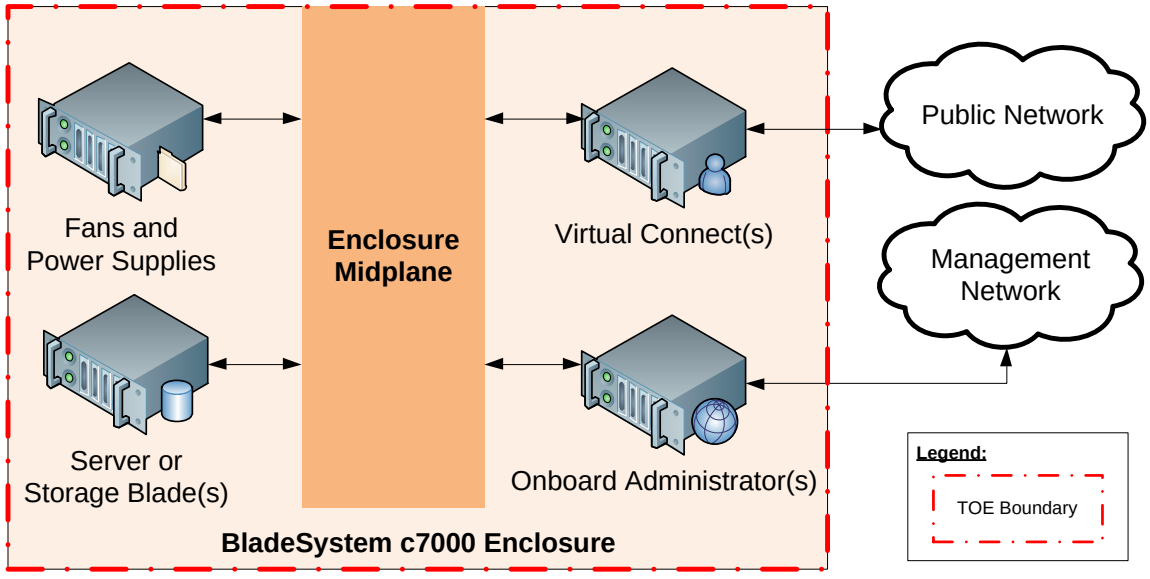

Figure 7 - Physical TOE Boundary – VC Mode

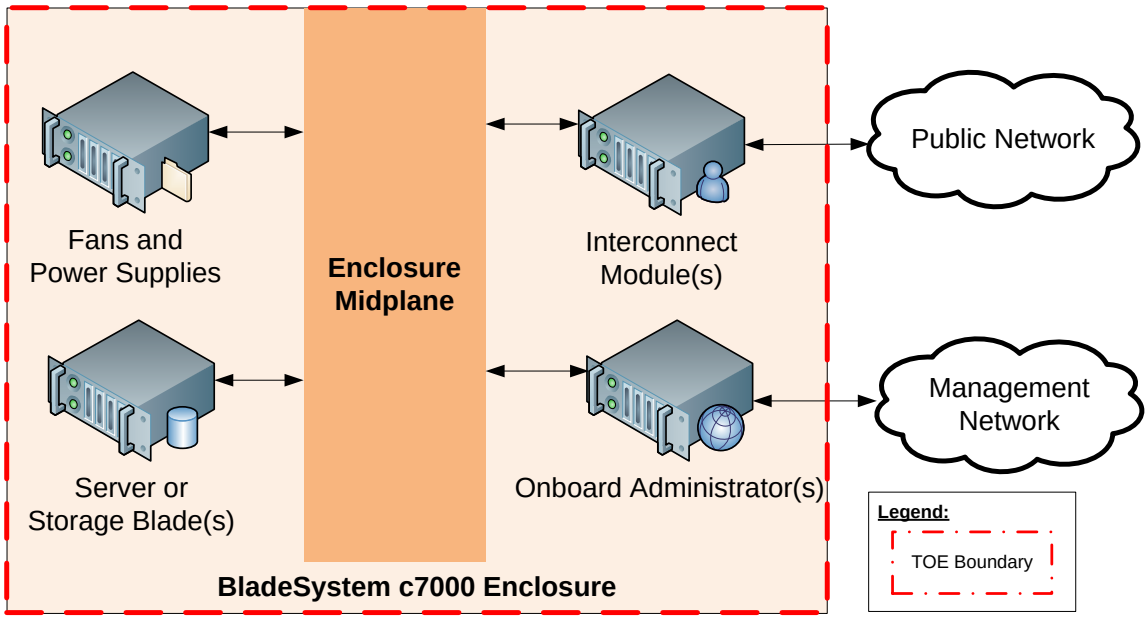

Figure 8 - Physical TOE Boundary – Non-VC Mode

1.6.1.1 Guidance Documentation

- Technologies in the HP BladeSystem c7000 Enclosure (Part Number 1108878 – December 2011)
- HP BladeSystem c-Class Solution Overview, Part Number 413339-006, March 2012 (Sixth Edition)
- HP Integrated Light-Out (iLO) for HP ProLiant Servers (Overview) Part Number DA-12362 September 2012
- HP Proliant iLO 3 Scripting and Command Line Guide, Part Number 616297-005, September 2013 (First Edition)
- HP Integrated Lights-Out security (Technology Brief, 7th Edition) Part Number 101208TB, December 2012
- HP iLO 3 User Guide, Part Number 616301-005, September 2013 (First Edition)
- HP BladeSystem Onboard Administrator Command Line Interface User Guide, Part Number 695523-003, September 2013 (20th Edition)
- HP BladeSystem Onboard Administrator User Guide, Part Number 695522-004, September 2013 (19th Edition)
- HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version v4.01 User Guide, Part Number 911532-002, June 2013 (Second Edition)
- HP Virtual Connect for c-Class BladeSystem Version 4.01 User Guide, Part Number 711534-002, June 2013 (Second Edition)
- HP BladeSystem Guidance Documentation Supplement Version 1.0, October 2013

1.6.2 Logical Scope

The TOE logical boundary is defined by the security functions that it implements. The security functions implemented by the TOE are usefully grouped under the following Security Function Classes:

- Audit
- Cryptographic Protection
- Failure and Physical Tamper Protection
- Management

- User Data Protection

1.6.2.1 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.

1.6.2.2 Cryptographic Protection

The TOE contains two FIPS[21] 140-2 validated cryptographic modules that implement the AES[22], 3DES[23], SHA[24], RSA, and DSS[25] algorithms for Onboard Administrator and iLO. In addition, Virtual Connect uses algorithms that are Cryptographic Algorithm Validation Program (CAVP) validated against FIPS[26] 140-2 requirements. These cryptographic algorithms are used to secure management traffic between the administrators and the TOE.

1.6.2.3 Failure and Physical Tamper Protection

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 can automatically failover to use the other component and thus provide uninterrupted service.

1.6.2.4 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[27] server[28]. Administrators are assigned a "privilege level" (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 Onboard Administrator component or the Virtual Connect (VC Mode only) component through their enforcement of the Management Access Control Security Functional Policy (detailed in Section 1.6.2.5 below). To access iLO's management functions, Onboard Administrator 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.

Administrators are authenticated by their usernames and passwords. Administrators can configure the TOE to require passwords of administrator-set minimum character complexity and length. The TOE provides no anonymous services: administrators must successfully authenticate before they are allowed to take any administrative actions.

[21] FIPS: Federal Information Processing Standard
[22] AES: Advanced Encryption Standard
[23] 3DES: Triple Data Encryption Standard
[24] SHA: Secure Hash Algorithm
[25] DSS: Digital Signature Specification
[26] FIPS – Federal Information Processing Standard
[27] LDAP: Lightweight Directory Access Protocol
[28] RADIUS and TACACS+ functionality is only available for Virtual Connect (VC Mode).

1.6.2.5 User Data Protection

The TOE enforces three Security Functional Policies (SFPs):

- Management Access Control SFP
- Virtual Connect 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 Virtual Connect Information Flow SFP (VC Mode only) 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 iLO Information Flow Control SFP ensures that only appropriately privileged administrators are allowed to use the iLO functionality of installed server blades.

1.6.3 Product Functionality not included in the TSF

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

- SNMP[29] inbound GET/SET requests
- Remote CLI via Telnet session
- iLO CLI via SSH session
- XML[30] Reply
- iLO and VC "System Maintenance Switches"
- ProLiant Server Blade operating systems
- Utilty Ready Blades (URB)
- Insight Display and KVM (locked in FIPS mode)
- HP Online Configuration Utility (HPONCFG)
- HP Systems Management agent/driver

[29] SNMP: Simple Network Management Protocol
[30] XML: eXtensible Markup Language

2 Conformance Claims

This section provides 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 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of January 5, 2011 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None.
EAL	EAL4+ augmented with Flaw Remediation (ALC_FLR.2)

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[31] 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.)
- TOE Developer: They develop the components of the TOE and are assumed to have physical access to the TOE during assembly.

All three are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[32] 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. The following threats are applicable:

Table 4 - Threats

Name	Description
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.
T.IMPROPER_CONFIG	A TOE user or Attackers who are 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	Failure of a TOE physical component due to a TOE developer mistake during TOE development could go undetected or could cause a breach of the TSF.
T.TAMPER	A TOE user could unintentionally tamper with a physical component of the TOE, which could go undetected or could cause a breach of the TSF.
T.FLOWS	An unauthorized person may send impermissible information through

[31] IT: Information Technology
[32] TSF: TOE Security Functionality

Name	Description
	the TOE that results in the exploitation of resources on the networks governed by the TOE.
T.WEAKCIPHERS	A TOE user may unintentionally access the TOE using a web browser or SSH client that does not support FIPS-approved algorithms.

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. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 5 - 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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 - Assumptions

Name	Description
A.CRYPTO	Only FIPS-approved ciphers are used by connecting clients (SSH and HTTPS clients) to access VC interconnect modules.
A.LOCATE	The TOE is located within a controlled access facility. If the optional external authentication mechanisms are used, such as LDAP, those external authentication servers are also located within the same controlled access facility and physically and logically on the same secure network as the TOE.
A.MANAGE	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 as follows:

Table 7 - 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.
O.FLOWS	The TOE must mediate the flow of all information between end-users, servers, and network devices located on internal and external networks governed by the TOE.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 - IT Security Objectives

Name	Description
OE.OS	The operating systems running on the blade servers must be appropriately configured to prevent unauthorized administrative access to the TSF.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.CLIENTS	The TOE environment must make use of FIPS-validated ciphers for clients connecting to the TOE (e.g., SSH clients and web browsers.)

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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 9 - Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects. Optional external authentication servers will be located within the same physically secure site and on the same secure network.

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 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 - 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 (Virtual Connect to Server Blade - VC Mode only)*		✓		✓

Name	Description	S	A	R	I
FDP_IFC.1(b)	Subset information flow control (Onboard Administrator to iLO)		✓		✓
FDP_IFF.1(a)	Simple security attributes (Virtual Connect to Server Blade - VC Mode only)		✓	✓	✓
FDP_IFF.1(b)	Simple security attributes (Onboard Administrator to iLO)		✓	✓	✓
FDP_RIP.1(a)	Subset residual information protection	✓	✓		✓
FDP_RIP.1(b)	Subset residual information protection	✓	✓		✓
FIA_SOS.1(a)	Verification of secrets		✓	✓	✓
FIA_SOS.1(b)	Verification of secrets (VC Mode only)		✓	✓	✓
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
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 initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation (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.
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 Onboard Administrator 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*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1 (b) Audit data generation (VC Mode only)
Hierarchical to: No other components.
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 Virtual Connect 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*].
Dependencies: FPT_STM.1 Reliable time stamps

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

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
FAU_STG.1.1
The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2
The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

FAU_STG.4.1

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

Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
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 11*] and specified cryptographic key sizes [*listed in the 'Key Sizes' colum of Table 11*] that meet the following: [*FIPS 197, FIPS 46-3, FIPS 180-3, and FIPS 186-3*].
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application Note: Onboard Administrator and iLO both implement CMVP validated modules. Virtual Connect, on the other hand, implements CAVP-validated algorithms for purposes of protecting TSF data for SSH and HTTPS sessions. Therefore, FCS_CKM.1 is not applicable to VC, following the guidance of CCS Instruction #4.

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
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*].
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]

Application Note: Onboard Administrator and iLO both implement CMVP validated modules. Virtual Connect, on the other hand, implements CAVP-validated algorithms for purposes of protecting TSF data for SSH and HTTPS sessions. Therefore, FCS_CKM.4 is not applicable to VC, following the guidance of CCS Instruction #4.

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1
The TSF shall perform [*the operation in the 'Cryptographic Operation' column of Table 11*] in accordance with a specified cryptographic algorithm [*listed in the 'Algorithm' column of Table 11*] and cryptographic key sizes [*listed in the 'Key Sizes' column of Table 11*] that meet the following: [*FIPS 140-2*].
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

Table 11 – Cryptographic Algorithm and Key Sizes for OA, iLO, and VC

Module	Algorithm	Key Sizes	Cryptographic Operation	Certificate No.
Onboard Administrator	AES – CBC[33], OFB[34], CTR[35] mode	128-, 192-, and 256-bit keys	Encryption/Decryption	2289
	TDES – CBC mode	(3) 56-bit keys	Encryption/Decryption	1439
	RSA[36] PKCS#1	1024- to 2048- bit keys	Key Generation; Signature Generation/Verification	1178
	DSA	1024- bit keys	Key generation, Signature Generation/Verification	716
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160-, 224-, 256-, 384-, and 512-bit	Hashing	1972, 1973,
	HMAC SHA-1	160-bit	Hashing; Message Authentication	1406
	ANSI x9.31 Appendix A.4.2 Pseudo Random Number Generator	128-bit key	Random Number Generation	1140
Integrated Lights-Out	AES – CBCmode	128- and 256- bit keys	Encryption/Decryption	2294, 2295, 2296
	AES – OFB[37] mode	128- bit keys	Encryption/Decryption	2297, 2298
	TDES – CBC mode	(3) 56- bit keys	Encryption/Decryption	1443, 1444, 1445
	RSA PKCS#1	1024- to 4096- bit keys	Signature Verification	1182, 1183
	DSA	1024-bit keys	Signature Verification	720
	SHA-1, SHA-512	160-, and 512- bit	Hashing	1977, 1978, 1979

[33] CBC: Cipher Block Chaining
[34] OFB: Output Feedback
[35] CTR: Counter
[36] RSA: Rivest Shamir Adleman
[37] OFB: Output Feedback

Module	Algorithm	Key Sizes	Cryptographic Operation	Certificate No.
	HMAC SHA-1	160- bit	Hashing; Message Authentication	1410
Virtual Connect	AES – CBC	128-, 192-, and 256-bit keys	Encryption/Decryption	2600
	TDES – CBC mode	(3) 56- bit keys	Encryption/Decryption	1567
	RSA PKCS#1	1024- to 2048- bit keys	Signature Generation/Verification	1328
	DSA	1024- bit keys	Signature Verification	788
	SHA-1, SHA-256, SHA-512	160-, 256-, and 512-bit	Hashing	2184
	HMAC SHA-1, HMAC SHA-256, HMAC SHA-512	160-, 256-, and 512-bit	Hashing; Message Authentication	1607

Application Note: Onboard Administrator and iLO both implement CMVP validated modules. Virtual Connect, on the other hand, implements CAVP-validated algorithms for purposes of protecting TSF data for SSH and HTTPS sessions.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 (a) Subset access control
Hierarchical to: No other components.
FDP_ACC.1 (a).1
The TSF shall enforce the [*Management Access Control SFP*[38]] on
[
a) Subjects: Administrators
b) Objects: Onboard Administrator components, iLO components
c) Operations: Access, Configure
].
Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
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.1.3a
The TSF shall explicitly authorise access of subjects to objects based on ~~the following~~ **no** additional rules: [~~assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*~~].
FDP_ACF.1.4a
The TSF shall explicitly deny access of subjects to objects based on **no additional rules** ~~the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].~~
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

[38] SFP: Security Functional Policy

FDP_IFC.1(a) Subset information flow control (Virtual Connect to Server Blade – VC Mode Only)
Hierarchical to: No other components.
FDP_IFC.1(a).1
The TSF shall enforce the [*Virtual Connect Information Flow Control SFP*] on
[
a) Subjects: BladeSystem server blades, external servers and workstations
b) Information: Network data
c) Operations: Transmit
].
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(a) Simple security attributes (Virtual Connect to Server Blade – VC Mode only)
Hierarchical to: No other components.
FDP_IFF.1(a).1
The TSF shall enforce the [*Virtual Connect 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 Virtual Connect component only if the administrator configurable rule for that unique source identifier or unique desitination identifier permits communication*].
FDP_IFF.1(a).3(a)
The TSF shall enforce the **[***information flow so that data tagged with a unique destination identifier will be forwarded to only the interfaces configured with the same destination identifier*].
FDP_IFF.1(a).3(b)
The TSF shall enforce the **[***distinct separation of data traffic so that it is not interfered with by any other data traffic when it is within the TOE's scope of control*].
FDP_IFF.1(a).4
The TSF shall explicitly authorise an information flow based on **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]~~.
FDP_IFF.1(a).5
The TSF shall explicitly deny an information flow based on **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]~~.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFC.1(b) Subset information flow control (Onboard Administrator to iLO)
Hierarchical to: No other components.
FDP_IFC.1(b).1
The TSF shall enforce the [*iLO Information Flow Control SFP*] on
[
a) Subjects: Onboard Administrator users
b) Information: BladeSystem server blade iLO data
c) Operations: Transmit
].
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(b) Simple security attributes (Onboard Administrator to iLO)

Hierarchical to: No other components.

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) Onboard Administrator user unique identifier

b) Onboard Administrator 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 Onboard Administrator component based on the Onboard Administrator user unique identifier, Onboard Administrator user component assignment, the BladeSystem server blade unique identifier, and if the Onboard Administrator configuration allows the TOE user and server blade to communicate*].

FDP_IFF.1(b).3

The TSF shall enforce **no additional rules** ~~the [assignment: additional information flow control SFP rules]~~.

FDP_IFF.1(b).4

The TSF shall explicitly authorise an information flow based on **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]~~.

FDP_IFF.1(b).5

The TSF shall explicitly deny an information flow based on **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]~~.

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

FDP_RIP.1(a) Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1(a)

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: [*cryptographic keys used by the OA and iLO cryptographic modules*].

Dependencies: No dependencies

FDP_RIP.1(b) Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1(b)

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*].

Dependencies: No dependencies

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1 (a) Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1 (a).1

The **Onboard Administrator user interface and the iLO user interface** ~~TSF~~ shall provide a mechanism to verify that secrets meet [*a configurable minimum character length. Additionally, the Onboard Administrator 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*].

Dependencies: No dependencies

FIA_SOS.1 (b) Verification of secrets (VC Mode only)
Hierarchical to: No other components.
FIA_SOS.1 (b).1

The **Virtual Connect user interface** ~~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: upper case letters, lower case letters, numbers, and symbols*].

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1

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

Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*listed in the 'Security Functions Behaviour Permissions' column of Table 12*] to [*the authorized identified roles listed under the 'Role/Privilege Level' column of Table 12*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Table 12 - Management of Security Functions Behaviour by Role

Module	Role/Privilege Level	Security Functions Behavior Permissions
Onlboard Administrator	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
Integrated Lights-Out	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
	Remoste 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[39] button
	Virtual Media	Allows an authorized user to use virtual media on the host platform
	Configure iLO 3 Settings	Allows authorized users to configure most iLO 3 settings, including security settings. It enables users to remotely update iLO 3 firmware; Login
Virtual Connect	Domain	Define local user accounts, passwords, and define roles; Import enclosures; Configure the VC domain; Set domain IP address; Administer SSL certificates; Configure SNMP settings
	Network	Configure network default settings; Create, edit, and delete all network settings aond 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

[39] NMI: Non-Maskable Interrupt

FMT_MSA.1 (a) Management of security attributes

Hierarchical to: No other components.

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 13*] to [*the authorized identified roles listed under the 'Role' column of Table 13*].

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

Table 13 - Management of Security Attributes

Module	Role	Security Attribute Access	Access Type
Onboard Administrator	Administrator	Onboard Administrator user unique identifier	Change default Query Modify Delete Create
		Privilege Level	Change default Query Modify Delete Create
		Onboard Administrator user component assignment	Change default Query Modify Delete Create
	Operator	Onboard Administrator user unique identifier	Query
		Privilege Level	Query
		Onboard Administrator user component assignment	Query
	User	Onboard Administrator user unique identifier	Query
		Privilege Level	Query
		Onboard Administrator user component assignment	Query
Intehrated Lights Out	Administrator	Onboard Administrator user unique identifier	Change default Query Modify Delete Create
		Privilege Level	Change default Query

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

FMT_MSA.1 (b).1

The TSF shall enforce the [*Virtual Connect 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].

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

Table 14 - Management of Security Attributes (VC Mode Only)

Module	Role	Security Attribute Access	Access Type
Virtual Connect	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 initialisation

Hierarchical to: No other components.

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.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3 (b) Static attribute initialisation (VC Mode only)

Hierarchical to: No other components.

FMT_MSA.3 (b).1

The TSF shall enforce the [*Virtual Connect 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.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [change_default, query, modify, delete, clear, [*create*]] the [*security attributes*] to [*appropriately privileged administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions
Hierarchical to: No other components.
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
].
Dependencies: No Dependencies

FMT_SMR.1 (a) Security roles
Hierarchical to: No other components.
FMT_SMR.1 (a).1
The TSF shall maintain the roles [*ADMINISTRATOR, OPERATOR, and USER*] for Onboard Administrator 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.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1 (b) Security roles
Hierarchical to: No other components.
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 3 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.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1 (c) Security roles (VC Mode only)
Hierarchical to: No other components.
FMT_SMR.1 (c).1
The TSF shall maintain the roles [*DOMAIN, NETWORK, STORAGE, SERVER, and USER*] for Virtual Connect 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 Virtual Connect.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*failure of BladeSystem hardware components*].
Dependencies: No dependencies.

FPT_PHP.2 Notification of physical attack
Hierarchical to: FPT_PHP.1 Passive detection of physical attack
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.
Dependencies: FMT_MOF.1 Management of security functions behaviour

FPT_RCV.2 Automated recovery
Hierarchical to: FPT_RCV.1 Manual recovery
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.
Dependencies: AGD_OPE.1 Operational user guidance

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

FPT_TST.1(a) TSF testing (cryptographic module)
Hierarchical to: No other components.
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 authorised 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 authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: No dependencies

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

Hierarchical to: No other components.

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 authorised 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 authorised users with the capability to verify the integrity of [[*BladeSystem hardware components*]].

FPT_TST.1(b).3

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

Dependencies: No dependencies

6.2.7 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance
Hierarchical to: FRU_FLT.1 Degraded fault tolerance
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*].
Dependencies: FPT_FLS.1 Failure with preservation of secure state

6.2.8 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
FTA_SSL.3.1
The TSF shall terminate an interactive session after a [*configurable time interval of administrator inactivity*].
Dependencies: No dependencies

Application Note: ***FTA_SSL.3 is enforced by Onboard Administrator (GUI, CLI, and SOAP[40] interfaces), iLO (GUI and Remote Consoles), and Virtual Connect (GUI and CLI). All otherexternal interfaces are excluded from the scope.***

FTA_TAB.1 Default TOE access banners
Hierarchical to: No other components.
FTA_TAB.1.1
Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.
Dependencies: No dependencies

Application Note: ***FTA_TAB.1 is enforced by Onboard Administrator (GUI and CLI interfaces), iLO (GUI only), and Virtual Connect (GUI and CLI). All otherexternal interfaces are excluded from the scope.***

FTA_TSE.1 TOE session establishment
Hierarchical to: No other components.
FTA_TSE.1.1
The TSF shall be able to deny session establishment based on [*TSF-enforced login delays between failed login attempts*].
Dependencies: No dependencies

Application Note: ***FTA_TSE.1 is enforced by Onboard Administrator (GUI and SOAP interfaces), and iLO (GUI). All other external interfaces, including Virtual Connect interfaces, are excluded from the scope.***

[40] 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 EAL4 augmented with ALC_FLR.2. Table 15 summarizes the requirements.

Table 15 - 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.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused Vulnerability analysis

7 TOE Summary 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 the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 16 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
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
	FPT_STM.1	Reliable time stamps
Cryptographic Protection	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FDP_RIP.1(a)	Subset residual information protection
	FPT_TST.1(a)	TSF testing (cryptographic module)
Failure and Physical Tamper Protection	FDP_RIP.1(b)	Subset residual information protection
	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.2	Notification of physical attack
	FPT_RCV.2	Automated recovery
	FPT_TST.1(b)	TSF testing (BladeSystem components)
	FRU_FLT.2	Limited fault tolerance
Management	FIA_SOS.1(a)	Verification of secrets
	FIA_SOS.1(b)	Verification of secrets (VC Mode only)
	FIA_UAU.2	User authentication before any action

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
	FMT_MOF.1	Management of security functions behaviour
	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 initialisation
	FMT_MSA.3(b)	Static attribute initialisation (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)
	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
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 (Virtual Connect to Server Blade - VC Mode only)
	FDP_IFC.1(b)	Subset information flow control (Onboard Administrator to iLO)
	FDP_IFF.1(a)	Simple security attributes (Virtual Connect to Server Blade - VC Mode only)
	FDP_IFF.1(b)	Simple security attributes (Onboard Administrator to iLO)

7.1.1 Audit

In VC Mode, the Onboard Administrator, Virtual Connect, 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.

Each TOE component also provides reliable timestamps. Onboard Administrator provides the capabilitiy to synchronize their internal clocks with an external NTP server, while iLO time may be synchronized with an external SNTP[41] server. Virtual Connect automatically synchronizes its time with an available Onboard Administrator.

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) (VC Mode Only), FAU_SAR.1, FAU_STG.1, FAU_STG.4, FPT_STM.1.

7.1.2 Cryptographic Protection

The TOE implements two FIPS 140-2 validated cryptographic modules (OA and iLO) that implement the AES, 3DES, SHA, RSA, and DSS algorithms. Virtual Connect uses algorithms that are CAVP-validated against FIPS[42] 140-2 requirements. These cryptographic algorithms are used to secure management traffic between the administrators and the TOE. The Onboard Administrator, Virtual Connect (VC Mode only), and iLO web interfaces are protected via the TLS[43] protocol, and the Onboard Administrator and Virtual Connect (VC Mode only) command line interfaces are protected via the SSH[44] protocol. The OA and iLO cryptographic modules generate and zeroize cryptographic keys in a FIPS 140-2 validated manner. FIPS 140-2-required self-tests are performed on the OA and iLO cryptographic algorithms and cryptographic modules on the whole to ensure their proper function.

The OA and iLO modules ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the cryptographic keys. In addition, 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.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_RIP.1(a), FPT_TST.1(a).

7.1.3 Failure and Physical Tamper Protection

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 (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 can automatically failover 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.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_PHP.2, FPT_TST.1(b), FPT_RCV.2, FRU_FLT.2, FDP_RIP.1(b).

[41] SNTP – Simple Network Time Protocol
[42] FIPS – Federal Information Processing Standard
[43] TLS: Transport Layer Security
[44] SSH: Secure Shell

7.1.4 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 Virtual Connect 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. OA supports LDAP directories such as Microsoft Active Directory for authentication and authoirzation. iLO supports Kerberos and LDAP for authentication, and LDAP may also be used for 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 Onboard Administrator, iLO and Virtual Connect (VC Mode only) components through their enforcement of the Management Access Control Security Functional Policy and Virtual Connect 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.

Administrators can configure the TOE to require passwords for Onboard Administrator and Virtual Connect (VC Mode only) of specific minimum character complexity and length and to require passwords for iLO of a specific length. Administrators can also configure password length requirements for the iLO interfaces. The TOE provides no anonymous services – administrators must successfully authenticate before they are allowed to take any administrative actions.

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 Onboard Abministrator GUI and CLI, iLO GUI, and Virtual Connect GUI and CLI). The TOE can also be configured to enforce a login delay between failed login attempts on the Onboard Administrator GUI and SOAP interfaces, and iLO GUI interface. Inactive administrative sessions can be terminated by the TOE after a configurable time interval of administrator inactivity for Onboard Administrator GUI. CLI and SOAP, iLO GUI, and Remote Consoles, and Virtual Connect GUI and CLI.

TOE Security Functional Requirements Satisfied: FIA_SOS.1 (a), FIA_SOS.1 (b) (VC Mode only), FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MSA.1 (a),FMT_MSA.1 (b) (VC Mode only), FMT_MSA.3 (a), FMT_MSA.3 (b) (VC Mode only), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 (a), FMT_SMR.1 (b), FMT_SMR.1 (c) (VC Mode only), FTA_SSL.3, FTA_TAB.1, FTA_TSE.1.

7.1.5 User Data Protection

The TOE implements three Security Functional Policies (SFPs):

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

7.1.5.1 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 Onboard Administrator, Virtual Connect (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 Onboard Administrator, Virtual Connect (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. 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, Virtual Connect 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.

7.1.5.2 Virtual Connect Information Flow Control SFP (VC Mode only)

The Virtual Connect 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 Virtual Connect module by an appropriately privileged administrator.[45]

The TOE controls information flow to ensure that server blades are permitted to transmit data to external networks only when explicitly assigned a profile[46] 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

[45] For example, a rule might specify that a server blade in bay #1 is allowed to communicate via an installed Virtual Connect 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 Virtual Connect configuration and rules, information please refer to the Virtual Connect administrative manuals.

[46] Profile: A collection of device-independent network/storage connection settings

configured with matching unique identifiers. For example, packets tagged with a particular VLAN ID[47] 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.

7.1.5.3 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 Onboard Administraor module by an appropriately privileged administrator.

TOE Security Functional Requirements Satisfied: FDP_ACC.1 (a), FDP_ACC.1 (b) (VC Mode only), FDP_ACF.1, FDP_IFC.1 (a) (VC Mode only), FDP_IFF.1 (a) (VC Mode only), FDP_IFC.1(b), FDP_IFF.1(b).

[47] VLAN ID: Virtual Local Area Network Identification

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

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 17 - Threats:Objectives Mapping

Threats	Objectives	Rationale
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	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.

Threats	Objectives	Rationale
	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.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.
T.IMPROPER_CONFIG A TOE user or Attackers who are 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 counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	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 only authorized users with the correct privilege levels may access and configure the TOE
T.FAILURE Failure of a TOE physical component due to a TOE developer mistake during TOE development 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 and that such an event will not cause a breach of the TSF.

Threats	Objectives	Rationale
T.TAMPER A TOE user could unintentionally tamper with a physical component of the TOE, which 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 TOE physical component is tampered with and that such an event will not cause a breach of the TSF.
T.FLOWS An unauthorized person may send impermissible information through the TOE that results in the exploitation of resources on the networks governed by the TOE.	O.FLOWS The TOE must mediate the flow of all information between end-users, servers, and network devices located on internal and external networks governed by the TOE.	O.FLOWS requires that all information that passes through the networks is mediated by the TOE and that no impermissible information is transmitted.
T.WEAKCIPHERS A TOE user may unintentionally access the TOE using a web browser or SSH client that does not support FIPS-approved algorithms.	OE.CLIENTS The TOE environment must make use of FIPS-validated ciphers for clients connecting to the TOE (e.g., SSH clients and web browsers.)	OE.CLIENTS ensures that only FIPS-approved algorithms are utilized when accessing the TOE.

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 18 - 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	O.AUTHENTICATE ensures that only authorized users are granted access to the tools required to manage the TOE.

Policies	Objectives	Rationale
	administrative sessions and failed login attempts in a secure manner.	

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 19 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.CRYPTO Only FIPS-approved ciphers are used by connecting clients (SSH and HTTPS clients) to access VC interconnect modules.	OE.CLIENTS The TOE environment must make use of FIPS-validated ciphers for clients connecting to the TOE (e.g., SSH clients and web browsers.)	The TOE environment provides client software capable of using FIPS-approved algorithms to connect to VC interconnect modules. OE.CLIENTS satisfies this assumption.
A.LOCATE The TOE is located within a controlled access facility. If the optional external authentication mechanisms are used, such as LDAP, those external authentication servers are also located within the same controlled access facility and physically and logically on the same secure network as the TOE.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects. Optional external authentication servers will be located within the same physically secure site and on the same secure network.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. NOE.PHYSICAL satisfies this assumption.
A.MANAGE 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.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL ensures that the sites deploying the TOE will provide only non-hostile, appropriately trained administrators that 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.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and	NOE.PHYSICAL ensures that the TOE's IT environment protects the TOE from interference and tampering by untrusted subjects.

Assumptions	Objectives	Rationale
	tampering by untrusted subjects. Optional external authentication servers will be located within the same physically secure site and on the same secure network.	
	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.

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 20 - 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 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 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

Objective	Requirements Addressing the Objective	Rationale
		the Management Access Control SFP.
O.ADMIN The TOE must include a set of functions that allow efficient and secure management of its functions and data, ensuring that 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 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 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(a) Subset residual information protection	The requirement meets this objective by ensuring that the TOE zeroizes cryptographic keys to prevent their compromise.
	FDP_RIP.1(b) 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 behaviour	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 restricts 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 restricts the ability to manipulate security attributes to only those administrators with the appropriate privileges.
	FMT_MSA.3(a) Static attribute initialisation	The requirement meets the objective by ensuring that the TOE creates restrictive default values for security attributes.
	FMT_MSA.3(b) Static attribute initialisation (VC Mode only)	The requirement meets the objective by ensuring that the TOE creates restrictive default values for security attributes.
	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.
	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

Objective	Requirements Addressing the Objective	Rationale
		data.
	FPT_TST.1(a) TSF testing (cryptographic module)	The requirement meets the objective by ensuring that FIPS 140-2-validated self-tests will be performed by the cryptographic module.
O.AUDIT The TOE must 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.
	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.
	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.
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 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 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)	The requirement meets this

Objective	Requirements Addressing the Objective	Rationale
	Verification of secrets	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.2 User authentication before any action	The requirement meets the objective by ensuring that administrators are authenticated before access to TOE functions is allowed.
	FIA_UID.2 User identification before any action	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 behaviour	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 behaviour of the TOE.
	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 initialisation	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

Objective	Requirements Addressing the Objective	Rationale
		so.
	FMT_MSA.3(b) Static attribute initialisation (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.
	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	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
	Automated recovery	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.
O.FLOWS The TOE must mediate the flow of all information between end-users, servers, and network devices located on internal and external networks governed by the TOE.	FDP_IFC.1(a) Subset information flow control (Virtual Connect 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 (Onboard Administrator to iLO)	The requirement meets this objective by ensuring that all administrators are controlled by the iLO Information Flow Control SFP.
	FDP_IFF.1(a) Simple security attributes (Virtual Connect 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 (Onboard Administrator to iLO)	The requirement meets this objective by ensuring that all administrators are controlled by the iLO Information Flow Control SFP.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor, assuming that 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. The TOE 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 EAL4+, the TOE will have incurred a search for 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

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 21 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 21 - 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_CKM.4	✓	
	FCS_COP.1	✓	
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(a)	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FDP_IFF.1(a)	FDP_IFC.1(a)	✓	
	FMT_MSA.3	✓	
FDP_IFF.1(b)	FDP_IFC.1(b)	✓	
	FMT_MSA.3	✓	
FDP_RIP.1(a)	No dependencies.	✓	
FDP_RIP.1(b)	No dependencies.	✓	
FIA_SOS.1(a)	No dependencies.	✓	
FIA_SOS.1(b)	No dependencies.	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this

SFR ID	Dependencies	Dependency Met	Rationale
			dependency.
FIA_UID.2	No dependencies.	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies.	✓	
FMT_SMR.1(a)	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FMT_SMR.1(b)	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FMT_SMR.1(c)	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	No dependencies.	✓	
FPT_PHP.2	FMT_MOF.1	✓	
FPT_RCV.2	AGD_OPE.1	✓	
FPT_STM.1	No dependencies.	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FPT_TST.1(a)	No dependencies.	✓	
FPT_TST.1(b)	No dependencies.	✓	
FRU_FLT.2	FPT_FLS.1	✓	
FTA_SSL.3	No dependencies.	✓	
FTA_TAB.1	No dependencies.	✓	
FTA_TSE.1	No dependencies.	✓	

9 Acronyms

Table 22 - Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
CAVP	Cryptograpihc Algorithm Validation Program
CC	The Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
CM	Configuration Management
CTR	Counter
DDR2	Double Data Rate 2
DSS	Digital Signature Specification
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standard
FRU	Field Replaceable Unit
Gb	Gigabit
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HBA	Host Bus Adapter
I/O	Input/Output
iLO	Integrated Lights-Out
IP	Internet Protocol
IT	Information Technology
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
Mb	Megabit
NIC	Network Interface Card

Acronym	Definition
NMI	Non-Maskable Interupt
NTP	Network Time Protocol
OA	Onboard Administrator
OFB	Output Feedback
OS	Operating System
PP	Protection Profile
RJ	Registered Jack
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
URB	Utility Ready Blades
USB	Universal Serial Bus
VC	Virtual Connect
VLAN ID	Virtual Local Area Network Identification
WWN	World Wide Name
XML	eXtensible Markup Language

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

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