Dell MX7000 Modular Chassis

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2100-000-D102
Version: 1.5
23 December 2019

Dell Technologies
1 Dell Way
Round Rock, Texas, USA
78682

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell MX7000 Modular Chassis Security Target
ST Version:	1.5
ST Date:	23 December 2019

1.3 TOE REFERENCE

TOE Identification: Dell MX7000 Modular Chassis with Management Module 1.00.10 firmware

TOE Developer: Dell Technologies

TOE Type: Modular Chassis (Network and Network-Related Devices and Systems)

1.4 TOE OVERVIEW

The MX7000 chassis provides the infrastructure to support compute, storage and Input/Output (I/O) within a centrally managed system.

The Dell PowerEdge MX7000 chassis is designed for the software-defined data center with the ability to support a combination of dense virtualization, software-defined storage, and software-defined networking. This allows customers to tailor compute and storage configurations to their own requirements and benefit from shared pools of disaggregated resources to respond to changing requirements.

The Dell PowerEdge MX7000 includes the following components:

- **Dell EMC PowerEdge MX7000 chassis** - The modular chassis provides the hardware foundation with support for multiple server processor generations, in a scalable system with end-to-end lifecycle management and a single interface for all components. This 7U chassis includes eight bays to accommodate a variety of single- and double-width compute and storage combinations.
- **Dell EMC PowerEdge MX740c and MX840c compute sleds** - Two- and four-socket blade sleds provide compute functionality. The single-width MX740c and double-width MX840c provide up to six terabytes of memory.
- **Dell EMC PowerEdge MX5016s storage sled** - This full-width storage sled holds up to 16 hot-pluggable SAS storage hard disk drives, with a maximum of seven MX5016s sleds in the MX chassis for up to 112 drives of direct-attached storage. These drives can be individually mapped to one or more servers.
- **Dell EMC PowerEdge MX Ethernet and Fibre Channel switching modules** - These low latency, high-bandwidth switching modules for multi-chassis environments include automated processes for topology compliance, quality of service and autonomous healing for peak network performance with the PowerEdge MX management interface.

The MX7000 chassis is managed using the Dell EMC OpenManage Enterprise-Modular (OME-M) application, which is embedded on the MX9002m management module. OME-M facilitates configuration and management of a PowerEdge MX chassis and its sleds using a single Graphical User Interface (GUI) or RESTful API. OME-M can be used to deploy servers, update firmware, and manage the

overall health of the chassis and the chassis components including compute sleds, network devices, input or output modules (IOMs), and storage devices. The front of the chassis provides a touch screen panel, and access, via Quick Sync 2, to the OpenManage Mobile application, which allows authenticated administrators to manage the device locally over an encrypted Bluetooth Low Energy (BLE) or dedicated Wifi connection at the chassis.

A Security-enhanced Linux (SELinux) kernel is used within the MX7000. SELinux uses mandatory access controls within its architecture to restrict access of user programs and system services. Minimizing privileges reduces the ability of programs or daemons to cause harm. As a result, new vulnerabilities will have a reduced impact on the security of the chassis and its components when they arise.

The MX7000 Modular Chassis provides the following security functionality:

- Comprehensive audit capabilities
- Administrator alerts for critical events, including notification of hardware attacks
- Secure communications
- Controlled access to management functions
- Failure tolerance
- Secure boot

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following network components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Active Directory	Windows Server 2012	General Purpose Computer Hardware
Email Server	Windows Server 2012	General Purpose Computer Hardware
Management Workstation	Windows 10	General Purpose Computer Hardware
Mobile Management Device	Android 6.0 running OpenManage Mobile version 3.0	General Purpose Mobile Device

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

The MX7000 Modular Chassis is a 7U modular enclosure that supports the following components:

- Up to eight standard height, single-width sleds, or four standard height, double-width compute sleds
- Up to seven Storage sleds
- Up to six hot swappable power supply units
- Up to two hot swappable management modules
- Up to six I/O modules
- Four front accessible hot swappable cooling fans
- Five rear accessible hot swappable cooling fans

Figure 1 shows a front view of the chassis, identifying the following components:

1. Left control panel
2. Single-width compute sled
3. Sled blank
4. Front fan (4)
5. Double-width compute sled
6. Single-width storage sled
7. Right control panel
8. Information tag
9. Power supply unit (6)

Figure 1 – MX7000 Front View

Figure 2 shows a rear view of the chassis, identifying the following components:

1. Slot for Fabric A1
2. Slot for Fabric A2
3. Rear fans (5)
4. Slot for Fabric B1
5. Slot for Fabric B2
6. Slot for Fabric C2
7. Power cable connection status LED
8. C22 Power inlet connectors (6)
9. Management Module 2
10. Management Module 1
11. Slot for Fabric C1

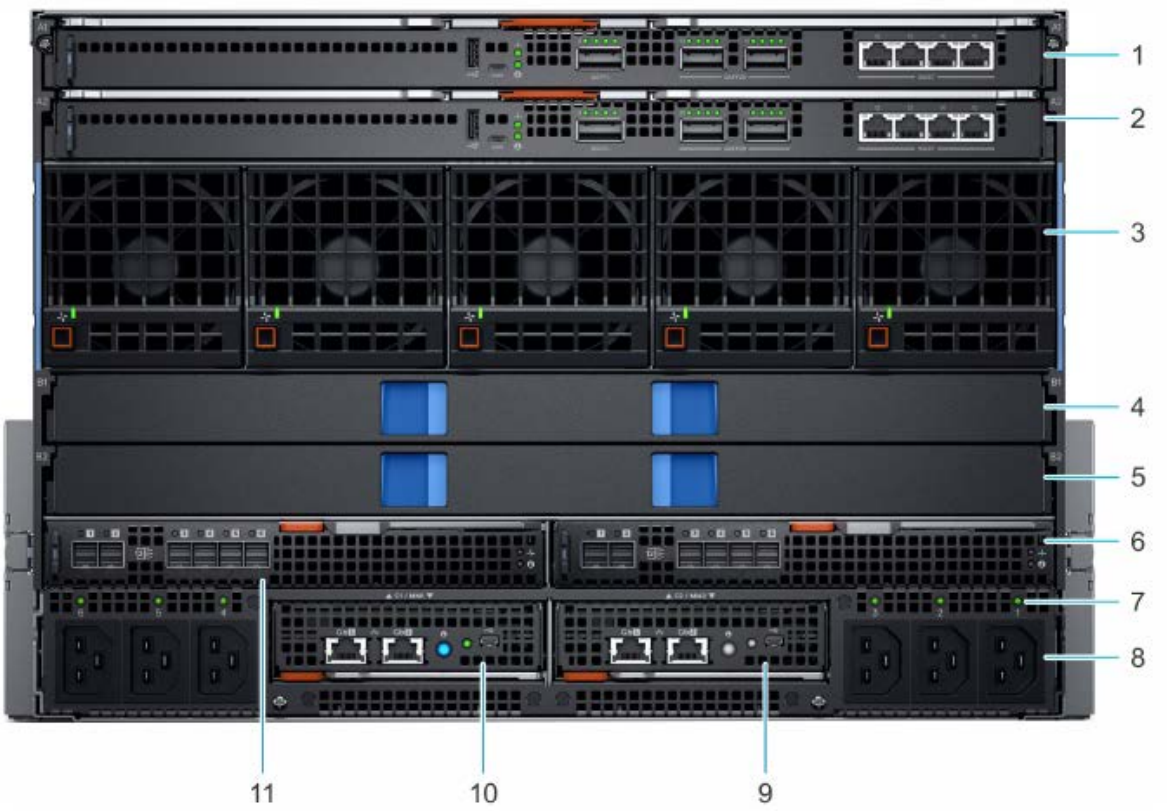

Figure 2 – MX7000 Rear View

1.5.1 Physical Scope

In the evaluated configuration, the TOE is an MX7000 chassis with the following components:

- 2 x MX9002m
- 2 x MX740c sleds
- MX840c sled
- MX5016s
- MX5000S
- MX9116n
- MX10 GB base T pass through module
- MX25 GB base T pass through module

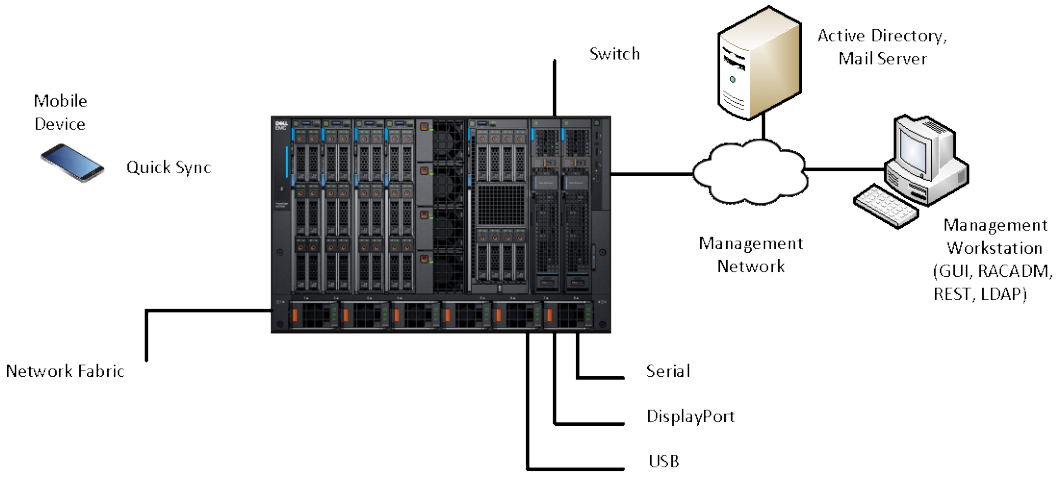

Figure 3 – TOE Deployment Diagram

1.5.1.1 TOE Delivery

The MX7000 chassis and its components are delivered together or separately from the factory by courier, or through resellers.

Documentation may be downloaded from the Dell support site (https://www.dell.com/support) in .pdf format.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation:

- Dell EMC OpenManage Enterprise-Modular Edition Version 1.00.01 for PowerEdge MX Chassis User's Guide, 2018 – 09, Rev. A00
  - openmanage-enterprise-modular-v10001-poweredge-mx7000_users-guide4_en-us.pdf
- Dell EMC PowerEdge MX7000 Enclosure Installation and Service Manual, 2018 - 09, Rev. A00
  - poweredge-mx7000_owners-manual_en-us.pdf
- Dell EMC PowerEdge MX7000 Enclosure Technical Specifications, 2018 - 09, Rev. A00
  - poweredge-mx7000_owners-manual2_en-us.pdf
- Dell EMC OpenManage Mobile Version 3.0 User's Guide (Android), 2018 - 09, Rev. A00
  - openmanage-mobile-v30_users-guide_en-us.pdf
- OpenManage Enterprise and OpenManage Enterprise - Modular Edition RESTful API Guide version 1.0, 2018 – 09, Rev. A00
  - openmanage-enterprise-modular-v10001-poweredge-mx7000_api-guide_en-us.pdf

- Dell EMC OpenManage Enterprise Modular Edition Version 1.00.01 for PowerEdge MX Chassis RACADM Command Line Reference Guide, 2018 – 09, Rev. A00
    - openmanage-enterprise-modular-v10001-poweredge-mx7000_cli-guide2_en-us.pdf

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events, and indicate the user responsible for the event. The audit logs are stored and protected from unauthorized modification and deletion and may be reviewed by authorized administrators. Administrators are alerted to potential security issues.
Cryptographic Support	Cryptographic functionality is provided to protect communications with the TOE.
User Data Protection	The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE. The TOE restricts access to iDRAC functions based on user account details and role.
Identification and Authentication	Users must identify and authenticate prior to accessing TOE management functions. Basic functions are available prior to login for users with physical access to the TOE. Users are locked out after a configurable number of failed authentication attempts. Passwords must meet minimum requirements, and are obscured as they are entered. Both local and Active Directory authentication are supported in the evaluated configuration.
Security Management	The TOE provides management capabilities via a Web-Based GUI, accessed via HTTPS. Management functions allow the administrators in the appropriate role to configure alert responses, review audit records, configure authentication mechanisms, and configure users and roles.
Protection of the TSF	The TOE continues to operate after the loss of one Management Module. The TOE provides notification of physical attack. The TOE provides verification of the digital signature on firmware prior to boot. Reliable time stamps are provided to support TOE functions, including the generation of audit records.

Functional Classes	Description
Resource Utilization	A secure state is preserved in the case of loss of both Management Modules.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using HTTPS.

Table 2 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Up to 20 chassis may be connected in a stacked configuration
- Optional LCD without Quick Sync 2

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 3 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.MISUSE	A malicious user could gain access to the TOE hardware or firmware and attempt to replace it with counterfeit hardware or firmware in order to bypass security functionality.
T.UNDETECT	Authorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 4 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.CRYPTO	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information transferred between the TOE and administrators,

OSP	Description
	communications between the TOE and trusted products, encryption of data at rest and verification of the firmware digital signature at boot time.
P.MONITOR	The TOE shall provide a means of monitoring its own health.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.NETWORK	An internal management network is provided for the sole use of management of internal resources, and is physically separate from data networks.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.ALERT	The TOE must be able to alert administrators to potential issues.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and must clearly associate the event with the identity of the user that caused the event. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. Audit records must be stored securely.
O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure or misuse of passwords.
O.PROTECT	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure, and must provide notification of physical tampering of the TOE. The TOE must protect against corrupt or illegitimate firmware.
O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.

Security Objective	Description
O.TIME	The TOE must provide reliable timestamps.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.NETWORK	The operational environment will provide an internal management network separate from the primary network for management of network resources.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCOUNT	T.MISUSE	T.PRIVILEGE	T.UNDETECT	P.CRYPTO	P.MONITOR	A.LOCATE	A.MANAGE	A.NETWORK
O.ACCESS	X								
O.ADMIN	X		X			X			
O.ALERT		X				X			
O.AUDIT				X					
O.CRYPTO					X				
O.IDENTAUTH	X		X	X					
O.PROTECT		X	X						
O.SECURE			X						
O.TIME				X					
OE.ADMIN								X	
OE.NETWORK									X
OE.PHYSICAL							X		

Table 8 – Mapping Between Objectives, Threats, OSPs, and Assumption

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat: **T.ACCOUNT**	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.

	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure or misuse of passwords.
Rationale:	O.ACCESS mitigates this threat by ensuring that users may only access the functions and data for which they are authorized. O.ADMIN provides the functions to administer the TOE, and to limit access to those functions. O.IDENTAUTH provides the identifying information that determines a user's authorized access.	

Threat: **T.MISUSE**	A malicious user could gain access to the TOE hardware or firmware and attempt to replace it with counterfeit hardware or firmware in order to bypass security functionality.	
Objectives:	O.ALERT	The TOE must be able to alert administrators to potential issues.
	O.PROTECT	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure, and must provide notification of physical tampering of the TOE. The TOE must protect against corrupt or illegitimate firmware. The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure, and must provide notification of physical tampering of the TOE. The TOE must protect against corrupt or illegitimate firmware.
Rationale:	O.ALERT mitigates this threat by notifying administrators of potential malicious access events. O.PROTECT mitigates this threat by providing for notification of physical tampering, and protection against the implementation of corrupt or illegitimate firmware.	

Threat: **T.PRIVILEGE**	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ADMIN	The TOE will provide all the functions and

		facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure or misuse of passwords.
	O.PROTECT	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure, and must provide notification of physical tampering of the TOE. The TOE must protect against corrupt or illegitimate firmware.
	O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE. O.PROTECT mitigates this threat by protecting against the implementation of counterfeit firmware to bypass access permissions. O.SECURE mitigates the threat by ensuring that system management data in transit is protected.	

Threat: **T.UNDETECT**	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and must clearly associate the event with the identity of the user that caused the event. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. Audit records must be stored securely.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure or misuse of passwords.
	O.TIME	The TOE must provide reliable timestamps.

Rationale:	O.AUDIT ensures that audit records are maintained for the use of TOE functions. It also ensures that the records are stored securely, and are available to authorized administrators. O.IDENTAUTH ensures that user identity is captured by the TOE for inclusion in the audit records. O.TIME provides reliable timestamps for audit records.

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **P.CRYPTO**	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information transferred between the TOE and administrators, communications between the TOE and trusted products, encryption of data at rest and verification of the firmware digital signature at boot time.	
Objectives:	O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
Rationale:	O.CRYPTO supports this policy by ensuring that validated cryptographic algorithms are provided in support of cryptographic operations.	

Policy: **P.MONITOR**	The TOE shall provide a means of monitoring its own health.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.ALERT	The TOE must be able to alert administrators to potential issues.
Rationale:	O.ADMIN ensures that functionality is in place to manage the security of the TOE. O.ALERT ensures that critical issues are identified and brought to the attention of an administrator.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.ADMIN supports this assumption by ensuring that trained individuals are in place to manage the TOE, and that these individuals have been specifically chosen to be careful, attentive and non-hostile.	

Assumption: A.NETWORK	An internal management network is provided for the sole use of management of internal resources, and is physically separate from data networks.	
Objectives:	OE.NETWORK	The operational environment will provide an internal management network separate from the primary network for management of network resources.
Rationale:	OE.NETWORK supports this assumption by ensuring the availability of an internal management network.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

a. Secure boot (FPT_SCB _EXT.1)

5.1.1 Family FPT_SCB_EXT: Secure initiation

Secure initiation functions are used to verify the authenticity of firmware prior to execution. The Secure initiation family is modeled after FPT_TST: TSF self test. FPT_SCB_EXT.1 Secure boot is modelled after FPT_TST.1 TSF testing.

Family Behavior

This family defines the requirements for secure initiation.

Component Levelling

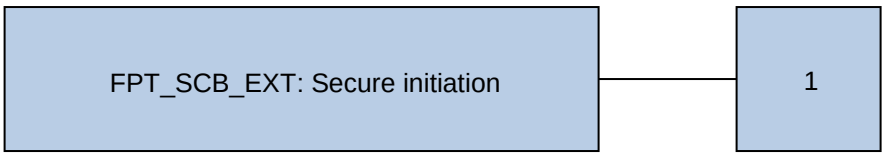

Figure 4 – FPT_SCB_EXT: Secure Initiation Component Levelling

Management

There are no management activities foreseen.

Audit

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

a) Minimal: failure of the signature verification

5.1.1.1 FPT_SCB_EXT.1 Secure boot

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_SCB_EXT.1.1 The TSF shall verify the digital signature on the firmware image before boot up.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets, and italics within the brackets, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 9.

Class	Identifier	Name
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage

Class	Identifier	Name
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (RBAC)
	FDP_ACC.1(2)	Subset access control (iDRAC access)
	FDP_ACF.1(1)	Security attribute based access control (RBAC)
	FDP_ACF.1(2)	Security attribute based access control (iDRAC access)
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (RBAC)
	FMT_MSA.1(2)	Management of security attributes (iDRAC access)
	FMT_MSA.3(1)	Static attribute initialisation (RBAC)
	FMT_MSA.3(2)	Static attribute initialisation (iDRAC access)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

Class	Identifier	Name
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.2	Notification of physical attack
	FPT_STM.1	Reliable time stamps
	FPT_SCB_EXT.1	Secure boot
Resource Utilization (FRU)	FRU_FLT.1	Degraded fault tolerance
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [*display an alert message in the GUI, email an alert to a designated administrator*] upon detection of a potential security violation.

6.2.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) [*user login and logout*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*IP address*].

6.2.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.2.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*one or more events meeting the alert definition*] known to indicate a potential security violation;

b) [*no other rules*].

6.2.1.5 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*all authorised 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.

6.2.1.6 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering*] of audit data based on [*Severity, Start Time, End Time, User, Source Address, Category, Description, Message ID*].

6.2.1.7 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm in Table 10*] and specified cryptographic key sizes [*cryptographic key sizes in Table 10*] that meet the following: [*list of standards in Table 10*].

Usage	Key Generation Algorithm	Key Size (bits)	Standard
RSA[1]	RSA Key Generation	2048 bit	FIPS[2] 186-4
AES[3]	Deterministic Random Bit Generator	128, 256	SP[4] 800-90A

Table 10 – Cryptographic Key Generation

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*key zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

[1] Rivest, Shamir and Adleman

[2] Federal Information Processing Standards

[3] Advanced Encryption Standard

[4] Special Publication

FCS_COP.1.1 The TSF shall perform [*cryptographic operations in Table 11*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm in Table 11*] and cryptographic key sizes [*cryptographic key sizes in Table 11*] that meet the following: [*list of standards in Table 11*].

Operation	Algorithm	Key or Digest Size (bits)	Standards
Signature Generation and Verification	RSA	2048 (generation) 1024, 2048 (verification)	FIPS 186-4
Symmetric Encryption/ Decryption	AES	128, 256	FIPS 197
Keyed-Hash Message Authentication Code	HMAC[5]-SHA[6]-1	160	FIPS 198
	HMAC-SHA-256	256	FIPS 198
Secure Hash	SHA	160	FIPS 180-4
	SHA-256	256	FIPS 180-4

Table 11 – Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1(1) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] on [
Subjects: administrative users
Objects: Security management data and functions
Operations: view, create, delete, execute
].

6.2.3.2 FDP_ACC.1(2) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*iDRAC Login SFP*] on [
Subjects: administrative users
Objects: Security management data and functions
Operations: view, create, delete, execute
].

[5] Hash Message Authentication Code

[6] Secure Hash Algorithm

6.2.3.3 FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] to objects based on the following: [

Subjects: Administrators
Subject Attributes: Role, source subnet
Objects: Security management data and functions
Object Attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an administrator may access security management data and functions if the user is assigned to a role that includes that privilege and the user connection originates from an allowed subnet*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.2.3.4 FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*iDRAC Login SFP*] to objects based on the following: [
Subjects: Administrators
Subject Attributes: Role
Objects: iDRAC security management data and functions
Object Attributes: none].

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 user for the Modular System Manager in the Compute Manager role may access iDRAC security management data and functions on the iDRAC interfaces for that chassis*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*2 and 16*]] unsuccessful authentication attempts occur related to [*failed authentication attempts*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user out for a configurable period of time*].

6.2.4.2 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*the following requirements:*

- *At least 8 characters in length*
- *Include at least one of the following:*
  - *Number*
  - *Special character*
  - *Uppercase letter*
  - *Lowercase letter*].

6.2.4.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing of system information, basic configuration, connecting to OpenManage Mobile*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*local and Active Directory (AD) authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following rules:*

- *For local authentication, the user enters the username and password*
- *For AD, the user enters the AD user credentials*].

6.2.4.5 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.

6.2.4.6 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*viewing of system information, basic configuration, connecting to OpenManage Mobile*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of] the functions [*notification of hardware removal and replacement*] to [*users in the Chassis Administrator role*].

6.2.5.2 FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Role, source subnet*] to [*users in the Chassis Administrator role*].

6.2.5.3 FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*iDRAC Login SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Role*] to [*users in the Chassis Administrator role*].

6.2.5.4 FMT_MSA.3(1) Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [*Role Based Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users in the Chassis Administrator rol*e] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_MSA.3(2) Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [*iDRAC Login SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users in the Chassis Administrator rol*e] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*configure alert response, review audit records, configure authentication mechanisms, configure users and roles*].

6.2.5.7 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Chassis Administrator, Compute Manager, Storage Manager, Fabric Manager, Viewer*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*loss of the Management Modules*].

6.2.6.2 FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

Dependencies: FMT_MOF.1Management of security functions behaviour

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 [*removable hardware components within the chassis*], the TSF shall monitor the devices and elements and notify [*the designated administrator*] when physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.6.3 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.6.4 FPT_SCB_EXT.1 Secure boot

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_SCB_EXT.1.1 The TSF shall verify the digital signature on the firmware image before boot up.

6.2.7 Resource Utilization (FRU)

6.2.7.1 FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [*all user services*] when the following failures occur: [*loss of one Management Module*].

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*administration*]].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	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
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Assurance Class	Assurance Components	
	Identifier	**Name**
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.ALERT	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.SECURE	O.TIME
FAU_ARP.1			X						
FAU_GEN.1				X					
FAU_GEN.2				X					
FAU_SAA.1			X						
FAU_SAR.1		X		X					
FAU_SAR.3		X		X					
FAU_STG.1				X					
FCS_CKM.1					X				
FCS_CKM.4					X				
FCS_COP.1					X				
FDP_ACC.1(1)	X								
FDP_ACC.1(2)	X								
FDP_ACF.1(1)	X								
FDP_ACF.1(2)	X								

	O.ACCESS	O.ADMIN	O.ALERT	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.SECURE	O.TIME
FIA_AFL.1						X			
FIA_SOS.1						X			
FIA_UAU.1						X			
FIA_UAU.5						X			
FIA_UAU.7		X				X			
FIA_UID.1						X			
FMT_MOF.1		X							
FMT_MSA.1(1)		X							
FMT_MSA.1(2)		X							
FMT_MSA.3(1)		X							
FMT_MSA.3(2)		X							
FMT_SMF.1		X							
FMT_SMR.1		X							
FPT_FLS.1							X		
FPT_PHP.2							X		
FPT_STM.1									X
FPT_SCB_EXT.1							X		
FRU_FLT.1							X		
FTP_TRP.1								X	

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control
	FDP_ACC.1(2)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACF.1(2)	Security attribute based access control
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) limit access to security management data and functions based on role. FDP_ACC.1(2) and FDP_ACF.1(2) restrict access to iDRAC security management data and functions to administrators with the proper account and role.	

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FIA_UAU.7	Protected authentication feedback
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes
	FMT_MSA.1(2)	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation
	FMT_MSA.3(2)	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MOF.1 provides for the functionality to manage notification of hardware removal and replacement. FMT_MSA.1(1) and FMT_MSA.3(1) provide the functionality to control access to other security management functions. FMT_MSA.1(2) and FMT_MSA.3(2) provide the functionality to control access to iDRAC security management functions. FMT_SMF.1 provides the security management functions required to administer the security features of the TOE. FMT_SMR.1 provides roles that are used to restrict the use of security management functions.	

	FAU_SAR.1 and FAU_SAR.3 provide the functionality to review audit records. FIA_UAU.7 ensures that passwords are obscured as they are entered to prevent inadvertent access.

Objective: **O.ALERT**	The TOE must be able to alert administrators to potential issues.	
Security Functional Requirements:	FAU_ARP.1	Security alarms
	FAU_SAA.1	Potential violation analysis
Rationale:	FAU_SAA.1 provides a means of identifying critical security issues, and FAU_ARP.1 ensures that these are brought to the administrator's attention.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions, and must clearly associate the event with the identity of the user that caused the event. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. Audit records must be stored securely.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_GEN.2 ensures that the user associated with the event is clearly identified. FAU_SAR.1 ensures that the functionality to read audit records is provided, and FAU_SAR.3 ensures that the functionality to filter these logs is provided. FAU_STG.1 ensures that audit records are stored securely.	

Objective: **O.CRYPTO**	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.	
Security Functional	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction

Requirements:	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 ensure that validated cryptographic functions are used for key generation, key destruction and operation in support of TLS1.2 protection of remote administrative sessions, communications between the TOE and trusted products, encryption of data at rest and verification of the firmware digital signature at boot time.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure or misuse of passwords.	
Security Functional Requirements:	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Rationale:	FIA_UID.1 and FIA_UAU.1 ensure that users may access data required to identify a system and connect to OpenManage Mobile prior to authentication, and that users are identified and authenticated prior to being granted access to administrative functions. FIA_UAU.5 describes the authentication mechanisms used. FIA_UAU.7 protects against the inadvertent exposure of passwords while they are entered. FIA_AFL.1 protects against a brute force attack on passwords. FIA_SOS.1 ensures that passwords meet minimum security requirements.	

Objective: **O.PROTECT**	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure, and must provide notification of physical tampering of the TOE. The TOE must protect against corrupt or illegitimate firmware.	
Security Functional Requirements:	FPT_FLS.1	Failure with preservation of the secure state
	FRU_FLT.1	Degraded fault tolerance
	FPT_PHP.2	Notification of physical attack

	FPT_SCB_EXT.1	Secure boot
Rationale:	FPT_FLS.1 ensures that a secure state is maintained in the case of the loss of one or more Management Modules. FRU_FLT.2 ensures that the TOE continues to operate in case of the loss of one Management Module. FPT_PHP.2 ensures that the TSF provides notification of physical attack when tampering of the TOE is detected. FPT_SCB_EXT.1 ensures that the digital signature on the firmware is verified prior to allowing the TOE to complete boot up.	

Objective: **O.SECURE**	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.	
Security Functional Requirements:	FTP_TRP.1	Trusted path
Rationale:	FTP_TRP.1 provides the means of protecting the communications path between the TOE and a remote administrator.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 ensures the provision of reliable time stamps.	

6.4.3 Dependency Rationale

Table 14 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_ARP.1	FAU_SAA.1	✓	
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1(1)	FDP_ACF.1	✓	
FDP_ACC.1(2)	FDP_ACF.1	✓	
FDP_ACF.1(1)	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(2)	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_SOS.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	None	N/A	
FPT_PHP.2	FMT_MOF.1	✓	
FPT_STM.1	None	N/A	
FPT_SCB_EXT.1	None	N/A	
FRU_FLT.1	FPT_FLS.1	✓	
FTP_TRP.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

7.1.1 Audit Logging

The MX7000 logs events in the audit log (application activity), the hardware log, the Management Module (MM) log and the iDRAC logs. Startup and shutdown of the device are shown in the hardware logs.

For audit events resulting from actions of identified users, the logs identify the user and include the IP address for that user.

Users in all of the administrative roles can view the audit records using the GUI. The GUI allows users to filter the logs viewed based on Severity, Start Time, End Time, User, Source Address, Category, Description, or Message ID.

The logs are protected from deletion by the embedded CentOS operating system on which they are stored. A factory command is required to remove the logs.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1.

7.1.2 Security Alarms

The MX7000 monitors its own system health in accordance with administrator defined policies. Alert definitions allow notification to trigger on severity of the alert, the message ID of the alert, the alert message, category or subcategory of the alert. When a condition that meets the alert definition is recognized, the GUI will display the alert and an email message is sent to a designated administrator.

TOE Security Functional Requirements addressed: FAU_ARP.1, FAU_SAA.1.

7.2 CRYPTOGRAPHIC SUPPORT

The MX7000 includes the 'Dell Crypto Library for Dell iDRAC, Dell CMC, and Dell OME-M' cryptographic module, a Federal Information Processing Standards (FIPS)-validated cryptographic module (CMVP certificate # 2861). The cryptographic module is used to support Transport Layer Security (TLS) 1.2 protection for all communications between the MX7000 and trusted products or users. Cryptography is also used for data at rest encryption (D@RE) of private keys used for TLS and for user information. Additionally, the digital signature on the firmware is verified at boot time, and when the firmware is updated.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

7.3.1 Role Based Access Control

Login to the MX7000 interfaces, including the OpenManager, is restricted to authorized users with the appropriate role who are originating from a designated subnet.

The roles and associated privileges are shown in Table 15.

Privilege	Role				
	Chassis Administrator	**Compute Manager**	**Storage Manager**	**Fabric Manager**	**Viewer**
Viewing application information	Yes	Yes	Yes	Yes	Yes
Setting up applications such as network, NTP, and proxy	Yes	No	No	No	No
Setting up users, security login policies, and certificates	Yes	No	No	No	No
Monitoring alert policies and alert destinations	Yes	No	No	No	No
Device power control	Yes	Yes	Yes	Yes	No
Device configuration actions—Applying templates, migrating profiles, and managing storage mappings	Yes	Yes	Yes	Yes	No
Operating system deployment	Yes	Yes	No	No	No
Updating device firmware	Yes	Yes	Yes	Yes	No

Privilege	Role				
	Chassis Administrator	Compute Manager	Storage Manager	Fabric Manager	Viewer
Creating and managing device templates, identity pools, and logical networks	Yes	Yes	Yes	Yes	No
Managing firmware catalogs and baseline policies	Yes	Yes	Yes	Yes	No
Power budget configuration and management	Yes	Yes	No	No	No

Table 15 – Roles and Privileges

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACF.1(1).

7.3.2 iDRAC Login with OME-M Credentials

The MX7000 allows users with the appropriate credentials to login to the iDRAC interfaces of the sleds within the chassis. In order to be able to login, the administrator must be a valid administrator on the chassis, or must be in the Compute Manager role.

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.4 IDENTIFICATION AND AUTHENTICATION

With physical access to the chassis, administrators are able to view system information, and perform some configuration functions prior to login. Users are able to access the following information and functions from the LCD touch panel:

- View Welcome Screen
  - Allows the user to select a language and the default LCD home page
- Main Menu
  - Allows the user to access the LCD functionality such as Identify, Settings, QuickSync, Alerts, Help, and Powered off
- QuickSync
  - Allows the user to connect OpenManage Mobile to the enclosure; however, the user must authenticate in order to access the OpenManage functions

- Alerts
  - Allows the user to view a list of all the critical and warning alerts of the enclosure
- Network Settings
  - Allows the user to view (IPv4/IPv6) and configure (IPv4 only) the chassis management IP address
- Settings
  - Allows the user to edit the Network settings, LCD Language, and Home screen
- System Info
  - Displays the Model number, Asset tag, and Service tag of the enclosure
- Chassis Powered Off
  - Notifies the user that the chassis power has been turned off

Administrator passwords are created by the administrator that creates the user account and cannot be changed by the user. The passwords must be between 8-32 characters in length and must contain one of each of the following:

- Number
- Special character – the special characters are
  < = > | _ - , ; : ! ? / . ' " ( ) [ ] { } § @ $ * & # % +
- Uppercase letter
- Lowercase letter

Passwords are obscured as they are entered. Typically dots are used to obscure the characters as they are entered; however, this is dependent upon the browser used to access the GUI.

After the configured number of unsuccessful login attempts, users are locked out for an administrator configurable period of time. The unsuccessful login attempts may be determined based on the user name, or on the IP address from which the authentication attempts originate.

The MX7000 supports both local authentication and Active Directory authentication in the evaluated configuration. For local authentication, the user enters the username and password. For AD authentication, the user enters the AD user credentials, which include the domain name.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1.

7.5 SECURITY MANAGEMENT

Administrators in the Chassis Administrator role are able to configure the behaviour of alerts when a hardware change is detected. An alert is automatically generated when hardware is removed from the chassis, and when new hardware is added. An alert is also generated when new hardware cannot be authenticated. The Chassis Administrator may configure this alert to be sent off box to a specified email address.

The MX7000 security management functionality provides administrators with the ability to:

- configure alert responses, including the email address to which alert notification is sent
- review audit records
- configure user authentication mechanisms
- configure users and roles

The roles available are described in Section 7.3.1.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_SMF.1, FMT_SMR.1.

7.5.1 Role Based Access Control Attributes

Only users in the Chassis Administrator role are able to query, modify and delete user accounts and login policies. By default, a user does not have a role until assigned by an administrator. Therefore, the default values are considered to be restrictive. By default, there are no restrictions on the source subnet.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.3(1).

7.5.2 iDRAC Login Attributes

Only users in the Chassis Administrator and Compute Manager roles are able to query, modify and delete user accounts and login policies. By default, a user does not have a role until assigned by an administrator. Therefore, the default values are considered to be restrictive.

TOE Security Functional Requirements addressed: FMT_MSA.1(2), FMT_MSA.3(2).

7.6 PROTECTION OF THE TSF

7.6.1 Preservation of the Secure State

Each chassis includes two Management Modules (MMs), which actively synchronize during normal operation. In the case of the loss of one MM, the other MM seamlessly assumes control and normal operation continues.

If both MMs become inoperable, the chassis maintains a secure state. A hash of the root password is backed up within the hardware in flash memory. This memory is not user accessible. In the case where both MMs become inoperable, they may be removed and replaced with operable devices. The new MMs will then restore the ability to use the root password from the stored hash. In this way, the secure state is maintained even in the case of the loss of both MMs.

TOE Security Functional Requirements addressed: FPT_FLS.1.

7.6.2 Detection of Physical Attack

An alert is automatically generated when hardware is removed from the chassis, and when new hardware is added. When new hardware is added to the chassis, the chassis performs an authentication function to verify that the new hardware is a valid Dell component. If this authentication fails, an alert is generated. Depending upon the chassis configuration, this alert can be sent off box to an administrator at a specified email address.

TOE Security Functional Requirements addressed: FPT_PHP.2.

7.6.3 Reliable Time Stamps

The MX7000 and the removable hardware components have Real-time Clock (RTC) components which are synchronized internally using Network Time Protocol. An administrator may configure the clock to use an external time source. Time is synchronized when device boot up is complete.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.6.4 Secure Boot

When the MX7000 is turned on, the Unified Extensible Firmware Interface (UEFI) verifies the digital signature on the firmware using an embedded public key and the cryptographic module described in Section 7.2. This verifies that the firmware has been signed by the Dell private key, and is therefore genuine. This verification applies to the firmware in the front end or MM portion of the chassis. If the firmware verification fails, the device will attempt to use a second, backup image.

TOE Security Functional Requirements addressed: FPT_SCB_EXT.1.

7.7 RESOURCE UTILIZATION

Each chassis includes two MMs, which actively synchronize during normal operation. In the case of the loss of one MM, the other MM seamlessly assumes control and normal operation continues.

TOE Security Functional Requirements addressed: FRU_FLT.1.

7.8 TRUSTED PATH / CHANNELS

When the Management Interface (GUI, remote RACADM, or REST) is used, the connection between the Mx7000 and the remote administrator's browser or application is protected from modification and disclosure using TLS1.2 over Transmission Control Protocol (TCP)/Internet Protocol (IP). This connection is logically distinct from other communication channels. The Mx7000 end point is identified by the user when attempting to access the chassis, and the user is authenticated prior to being granted any access to security management functions on these interfaces.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Management Module	The Management Module hardware and firmware provide the management functionality for the TOE. This component is made up of the Modular System Manager and the Enclosure Controller.
Quick Sync	Quick Sync allows an administrator to connect to the TOE via Bluetooth or wireless access to access the mobile management application. Authentication to the mobile management application is required to perform management functions.

Table 16 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
D@RE	Data at rest Encryption
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
I/O	Input/Output
ID	Identification
IOM	Input or Output Module
IP	Internet Protocol

Acronym	Definition
IT	Information Technology
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MM	Management Module
NTP	Network Time Protocol
OME-M	OpenManage Enterprise - Modular
OSP	Organizational Security Policy
PP	Protection Profile
RBAC	Role-Based Access Control
REST	Representational State Transfer
RSA	Rivest, Shamir and Adleman
SELinux	Security-Enhanced Linux
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface

Table 17 – Acronyms