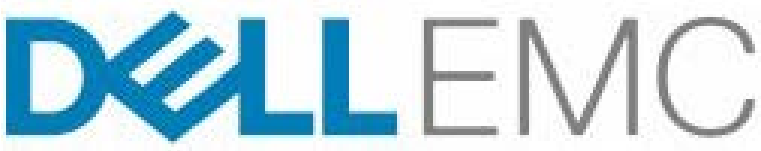
Dell EMC™ XtremIO® v6.3.1

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2133-000-D102
Version: 1.7
13 October 2020



Dell EMC
176 South Street
Hopkinton, MA, USA
01748

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 EMC™ XtremIO® v6.3.1 Security Target
ST Version:	1.7
ST Date:	13 October 2020

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ XtremIO® v6.3.1-5 with the 6.3.1-5 Storage Controller Software

TOE Developer: Dell EMC

TOE Type: Data Storage (Other Devices and Systems)

1.4 TOE OVERVIEW

EMC XtremIO is an all-flash system providing storage for enterprise applications, based on a scale-up and scale-out architecture. The system uses building blocks, called X-Bricks, which can be clustered together. The XtremIO Storage Array provides a very high level of performance that is consistent over time, system conditions and access patterns. It is designed for high granularity true random I/O. Each X-Brick contains two storage nodes in a group of Self Encrypting Drives (SEDs) used in performing Data at Rest Encryption (D@RE) of all data stored on the TOE.

The system operation is controlled via a stand-alone dedicated server (using a proprietary hardened Linux OS), called the XtremIO Management Server (XMS). Each XtremIO cluster requires its own XMS host appliance. The array continues to operate if it is disconnected from the XMS, but cannot be configured or monitored until the connection is restored.

The XMS enables you to control and manage the XtremIO cluster, including:

- Creating, formatting, and initializing new clusters
- Monitoring cluster health and events
- Monitoring cluster performance
- Collecting cluster performance statistics
- Providing GUI and CLI services to administrators
- Implementing volume management and data protection groups operation logic
- Providing operational support functions such as stopping and starting the cluster or any of the Storage Controllers.

The system Graphical User Interface (GUI) is implemented using HTML5. The GUI provides easy-to-use tools for performing most of the cluster operations (certain management operations must be performed using the CLI). Additionally, operations on multiple components, such as creating multiple volumes, can only be performed using the GUI.

The system's Command Line Interface (CLI) allows administrators and other XtremIO cluster users to perform supported management operations, including the review of audit records. It is preinstalled on the XMS and can be accessed using the standard SSH protocol or via CLI window in the GUI.

Users of the CLI and GUI must authenticate with the XMS before they may access controlled functions or data. Authentication can be performed locally or through a third party Lightweight Directory Access Protocol (LDAP) server. Individual user accounts are configured in XMS, and one of three roles can be assigned to each user. The management capabilities provided to each user are determined by their role.

Host Initiators (or Enterprise storage servers) access data on the XtremIO system via the Internet Small Computer Systems Interface (iSCSI) protocol. Volumes within XtremIO are only exposed to initiators that they have been mapped to, and may further be restricted by Virtual Local Area Networks (VLANs).

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

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

Component	Operating System	Hardware
Host Initiator (external storage server)	CentOS 6	Independent storage host supporting an iSCSI interface.
LDAP Server	Windows Server 2012 R2	General Purpose Computer Hardware
Management Workstation	Windows 10	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the components identified in Table 2. The deployment configuration and TOE boundary are shown in Figure 1.

TOE Component	Description
XtremIO X2R Hardware	Dell EMC X2R hardware appliance with the XIOS 6.3.1 storage controller software.
XMS hardware	Dell EMC XMS hardware appliance with the XMS 6.3.1 software.

Table 2 - TOE Components

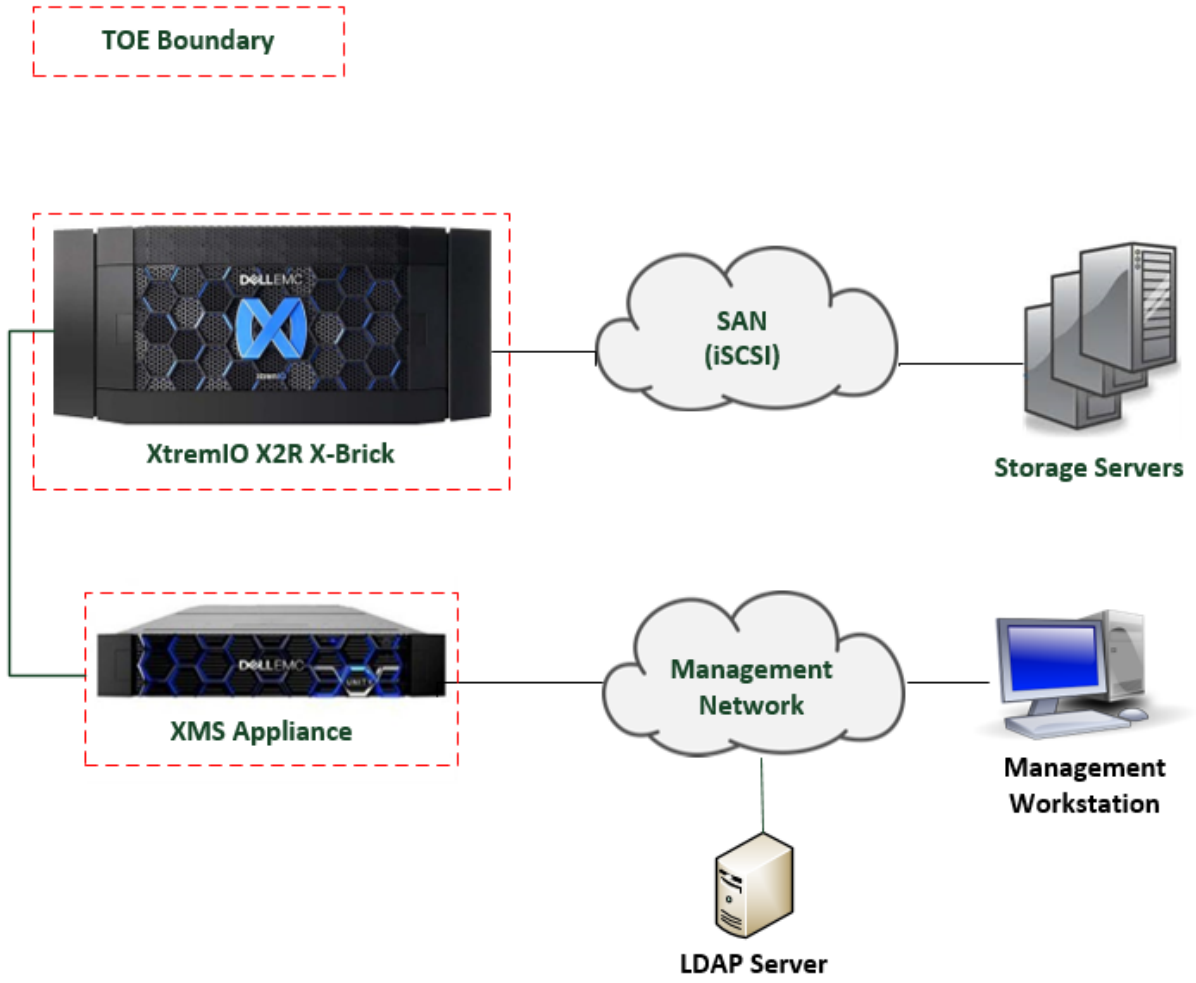


Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation. The documents may be downloaded from the Dell EMC support website in pdf format with the indicated file names:

- Dell EMC XtremIO Storage Array X1 and X2 Cluster Types XMS Versions 6.2.0 and 6.2.1, XIOS Versions 4.0.15, 4.0.25, 4.0.26, 4.0.27, 6.0.0, 6.0.1, 6.0.2, 6.1.0, 6.2.0 and 6.2.1 User Guide, REV. 06, Published April 2019
    - *XtremIO_X1-X2_XMS-6-2-0_6-2-1_XIOS-4-0-15_4-0-25_4-0-26_4-0-27_6-0_6-0-1_6-0-2_6-1-0_6-2-0_6-2-1_User-Guide_302-004-991_Rev-06.pdf*

- Dell EMC XtremIO Storage Array X1 and X2 Cluster Types XMS Versions 6.2.0 and 6.2.1, XIOS Versions 4.0.15, 4.0.25, 4.0.26, 4.0.27, 6.0.0, 6.0.1, 6.0.2, 6.1.0, 6.2.0 and 6.2.1 Security Configuration Guide, REV 03, Published April 16, 2019
    - *docu90464_XtremIO-Storage-Array-X1-and-X2-Cluster-Types-with-XMS-Ver.-6.2.0-and-6.2.1-and-XIOS-Ver.-4.0.15-and-4.0.25-and-4.0.26-and-4.0.27-Security-Configuration-Guide.pdf*
- Dell EMC XtremIO Storage Array X1 and X2 Cluster Types XMS Versions 6.2.0 and 6.2.1, XIOS Versions 4.0.15, 4.0.25, 4.0.26, 4.0.27, 6.0.0, 6.0.1, 6.0.2, 6.1.0, 6.2.0 and 6.2.1 Admin CLI Guide, REV. 03, Published April 2019
    - *docu90453_XtremIO-Storage-Array-X1-and-X2-Cluster-Types-with-XMS-Ver.-6.2.0-and-6.2.1-and-XIOS-Ver.-4.0.15-and-4.0.25-and-4.0.26-and-4.0.27-Admin-CLI-Guide.pdf*
- Dell EMC XtremIO Storage Array X2 Cluster Type XMS Versions 6.2.0 and 6.2.1, XIOS Versions 6.0.0, 6.0.1, 6.0.2, 6.1.0, 6.2.0 and 6.2.1 Site Preparation Guide, REV 03, Published April 18, 2019
    - docu90466_XtremIO-Storage-Array-X2-Cluster-Type-with-XMS-Ver.-6.2.0-and-6.2.1-and-XIOS-Ver.-6.0.0-and-6.0.1-and-6.0.2-and-6.1.0-and-6.2.0-and-6.2.1-Site-Preparation-Guide.pdf

The following Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- Dell EMC™ XtremIO® Common Criteria Guidance Supplement, Version 1.4
    - *XtremIO_EAL2_AGD_1.4.pdf*

Note: All guidance is applicable to the TOE 6.3.1 version.

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 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs may be reviewed by authorized administrators.
Cryptographic Support	Cryptographic functionality provides for Data at Rest Encryption (D@RE) of all data stored on the TOE.
User Data Protection	The TOE provides administrative and volume access control capabilities to ensure that only authorized administrators and storage host initiators are able to access the TOE.

Functional Classes	Description
Identification and Authentication	Users must identify and authenticate prior to gaining TOE access. Authentication can be performed locally or via LDAP. Obscured feedback is displayed to the user during password collection.
Security Management	The TOE provides management capabilities via a Web-based GUI and CLI. Management functions allow the administrators to configure users, storage volumes, and storage access controls. The TOE supports an administrative role which determines access to the management functions.
Protection of the TSF	The TOE provides reliable time stamps used in the generation of audit records.
TOE Access	User sessions with the TOE may be terminated at any time by the user. Sessions may also be terminated automatically by the TOE based on an administrator configurable time interval of user inactivity. A banner is presented on user login.

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

In addition to the X2R hardware, XtremIO 6.3.1 is supported on the X2S and X2T appliances. The X2T hardware is available with either FIPS or non-FIPS validated SEDs, is limited to a 1.92TB capacity, with 36 SSDs and only one Brick per cluster. The X2R is also available with non FIPS validated SEDs. XMS may also be deployed as a Virtual Machine on supported ESXi VMware platforms. This is not included in the evaluated configuration.

The following features are excluded from this evaluation:

- Public Key Authentication
- Challenge-Handshake Authentication Protocol (CHAP) authentication of Host Initiators
- High availability
- Support Assist Enterprise (SAE) – *formerly Dell EMC Secure Remote Services*
- OpenStack

The following interfaces are not used in the evaluated configuration:

- Representational State Transfer Application Program Interface (REST API)
- PowerShell API

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 conformant
- 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 4 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.UNAUTHSERVER	An unauthorized user may direct a server to attempt to access user data (volumes) that it is not authorized to access.
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.
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 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 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.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.MANAGE	The TOE shall be managed only by authorized users.
P.PROTECT	The TOE shall incorporate mechanisms to protect against potential disclosure of the data it has been entrusted to store.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

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.

Table 6 – 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.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
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.
O.SERVERACCESS	The TOE must only allow authorized servers access to stored user data.
O.TIME	The TOE must provide reliable time stamps.

Table 7 – 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.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected, trained for proper operation of the TOE, and follow all guidance.
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 8 – 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.UNAUTHSERVER	T.UNDETECT	T.PRIVILEGE	P.ACCOUNT	P.MANAGE	P.PROTECT	A.LOCATE	A.MANAGE
O.ACCESS		X	X		X			
O.ADMIN	X	X	X					
O.AUDIT		X		X				
O.CRYPTO						X		
O.IDENTAUTH		X	X	X	X			
O.SERVERACCESS	X							
O.TIME		X		X				
OE.CREDENTIALS		X			X			
OE.PERSON		X	X		X			X
OE.PHYSICAL							X	

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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

Threat: T.UNAUTHSERVER	An unauthorized user may direct a server to attempt to access user data (volumes) that it is not authorized to access.	
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.SERVERACCESS	The TOE must only allow authorized servers access to stored user data.
Rationale:	O.ADMIN mitigates this threat by providing authorized administrators with the management functionality required to restrict server access to user data stored on the TOE. O.SERVERACCESS mitigates this threat by ensuring that only authorized servers can access data stored on the TOE.	

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.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.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	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.

	O.TIME	The TOE must provide reliable time stamps.
	OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected, trained for proper operation of the TOE, and follow all guidance.
Rationale:	O.ACCESS mitigates this threat by limiting user access to appropriate TOE functions and data. O.ADMIN ensures that the TOE functions necessary to support administration of the TOE is available to users. O.AUDIT ensures audit records are generated for use of the TOE. O.TIME provides reliable time stamps for the audit records. O.IDENTAUTH mitigates this threat by ensuring that users are identified and authenticated prior to allowing access to TOE functions and data. OE.CREDENTIALS mitigates this threat by ensuring that users cannot mask their identity. OE.PERSON ensures that only trusted, properly trained administrators are authorized to operate the TOE.	

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.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.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected, trained for proper operation of the TOE, and

		follow all guidance.
Rationale:	O.ACCESS mitigates this threat by limiting user access to appropriate TOE functions and data. O.ADMIN ensures that the TOE functions necessary to support administration of the TOE is available to users. O.IDENTAUTH ensures that users are identified and authenticated thus eliminating unauthorized access to TOE functions and data. OE.PERSON ensures that only trusted, properly trained administrators are authorized to operate the TOE.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.ACCOUNT**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	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.
	O.TIME	The TOE must provide reliable time stamps.
Rationale:	O.AUDIT addresses this policy by ensuring that a record of all user activity is recorded. O.TIME ensures that reliable time stamps are used for the audit records O.IDENTAUTH addresses this policy by ensuring that users are identified prior to gaining access to the TOE. The user identity is affixed to the audit records.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	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.
	OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected, trained for proper operation of the TOE, and follow all guidance.
Rationale:	O.ACCESS addresses this policy by limiting user access to appropriate TOE functions and data. O.IDENTAUTH addresses this policy by ensuring that users are identified and authenticated prior to allowing access to TOE functions and data. OE.CREDENTIALS addresses this policy by protecting all authentication data. OE.PERSON ensures that competent administrators will manage the TOE.	

Policy: **P.PROTECT**	The TOE shall incorporate mechanisms to protect against potential disclosure of the data it has been entrusted to store.	
Objectives:	O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
Rationale:	O.CRYPTO addresses this policy by ensuring that data stored on the TOE is encrypted.	

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 ensuring that authorized administrators provide for physical protection of the TOE.	

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.PERSON	Personnel working as authorized administrators shall be carefully selected, trained for proper operation of the TOE, and follow all guidance.
Rationale:	OE.PERSON supports this assumption by ensuring that all authorized administrators are trusted, qualified and trained to manage the TOE.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

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 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, 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.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 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 logins, changes to TSF data*].

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, [*user specified parameters for configuration changes*].

6.2.1.2 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.

6.2.1.3 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 records from the events log*] 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.

6.2.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

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 [*Deterministic Random Bit Generator*] and specified cryptographic key sizes [*256 bits*] that meet the following: [*SP800-90A*].

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 [*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

FCS_COP.1.1 The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES*] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS 197*].

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Volume Access control SFP*] on [

Subjects: Host Initiators

Objects: Storage Volumes

Operations: read and write].

6.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

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

Subjects: Host Initiators

Subject attributes: Initiator ID, Initiator Group

Objects: Storage Volumes (LUN)

Object attributes: Target ID, Target VLAN,].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. *An Initiator may access a Target if all of the following conditions are satisfied:*
   a. *The Supplied Target ID matches a configured Target ID;*
   b. *The Initiator ID matches a configured Initiator ID;*
   c. *No Target VLAN is configured for the Supplied Target ID, or the VLAN used by the Initiator matches the Target VLAN.*
2. *An Initiator may access a LUN if all of the following conditions are satisfied:*
   a. *The Initiator may access the Target being used;*
   b. *The Initiator is included in the Initiator Group that the LUN is mapped to*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, role*].

6.2.4.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

6.2.4.3 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*local authentication, LDAP authentication*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*order of the configured authentication mechanisms*].

6.2.4.4 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.

6.2.4.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Volume Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*host security attributes (Host port address, Initiator Group) storage volume security attributes (LUN)*] to [*authorised administrative users*].

6.2.5.2 FMT_MSA.3 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 [*Volume 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 Configuration or Admin role*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 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: [

- *User management*
- *Volume management*
- *Initiator management*
- *LUN mapping*
- *Review of audit records*].

6.2.5.4 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 [*Read-Only*, *Configuration*, *Admin*].

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_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.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a**n** [*administrator configurable time interval of user inactivity*].

6.2.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.7.3 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 11.

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 11 – 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.AUDIT	O.CRYPTO	O.IDENTAUTH	O.SERVERACCESS	O.TIME
FAU_GEN.1			X				
FAU_GEN.2			X				
FAU_SAR.1	X	X	X				
FAU_SAR.2	X	X	X				
FCS_CKM.1				X			
FCS_CKM.4				X			
FCS_COP.1				X			
FDP_ACC.1						X	
FDP_ACF.1						X	
FIA_ATD.1					X		
FIA_UAU.2					X		
FIA_UAU.5					X		
FIA_UAU.7					X		
FIA_UID.2					X		

	O.ACCESS	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENTAUTH	O.SERVERACCESS	O.TIME
FMT_MSA.1	X	X					
FMT_MSA.3	X	X					
FMT_SMF.1		X					
FMT_SMR.1	X	X					
FPT_STM.1			X				X
FTA_SSL.3		X					
FTA_SSL.4		X					
FTA_TAB.1		X					

Table 12 – 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:	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMR.1	Security roles
Rationale:	FAU_SAR.1 and FAU_SAR.2 support this objective by allowing authorized administrators to access the audit records. FMT_MSA.1 and FMT_MSA.3 support this objective by restricting the ability to manipulate the Volume Access Control SFPs. FMT_SMR.1 supports this objective by providing user roles that limit access to the TOE functions and data.	

Objective:	The TOE will provide all the functions and facilities necessary to

O.ADMIN	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.2	Restricted audit review
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
Rationale:	FAU_SAR.1 and FAU_SAR.2 support this objective by ensuring authorized administrators have the ability to review audit records. FMT_MSA.1 and FMT_MSA.3 define the access permissions for management of the Volume access control SFP. FMT_SMF.1 specifies the management functionality required for effective management of the TOE. FMT_SMR.1 defines the roles required to provide effective management capabilities for different categories of users. FTA_SSL.3 and FTA_SSL.4 support this objective by defining session termination mechanisms to protect against idle sessions being used by unauthorized users. FTA_TAB.1 provides a mechanism to warn unauthorized users against unauthorized access.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 supports this objective by generating audit records for auditable events.	

	FAU_GEN.2 supports this objective by associating a user identity with each auditable event generated. FPT_STM.1 ensures a time stamp is provided for each auditable event. FAU_SAR.1 and FAU_SAR.2 support this objective by providing a means of reviewing the generated audit records.

Objective: **O.CRYPTO**	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 support this objective by providing the cryptographic functionality required to protect the confidentiality of data stored on the TOE.	

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.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identity before any action
Rationale:	FIA_ATD.1 supports this objective by ensuring that each user has assigned security attributes. FIA_UAU.2 and FIA_UID.2 support this objective by ensuring users are identified and authenticated prior to gaining access to the TOE and TOE functions. FIA_UAU.5 defines the mechanisms used in the enforcement of user authentication. FIA_UAU.7 protects passwords from being observed, thus preventing unauthorized access to the TOE.	

Objective:	The TOE must only allow authorized servers access to stored user data.

O.SERVERACCESS		
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Rationale:	FDP_ACC.1 and FDP_ACF.1 support this objective by enforcing access control policies on servers accessing data stored by the TOE.	

Objective: **O.TIME**	The TOE must provide reliable time stamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 supports this objective by ensuring reliable time stamps are provided.	

6.4.3 Dependency Rationale

Table 13 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_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1

SFR	Dependency	Dependency Satisfied	Rationale
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTA_TAB.1	None	N/A	

Table 13 – 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 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

Audit records are generated for user login events, and changes to the TSF data and TOE configuration. Startup of the audit function is equivalent to a power on event. It is not possible to shut down the audit function. The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (if applicable),
- The configuration parameters specified by the user.

Users assigned any of the supported roles may view the audit records via the CLI and GUI by displaying events with a category of “Audit”.

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

7.2 CRYPTOGRAPHIC SUPPORT

XtremIO protects stored data using D@RE. The encryption is based on Self Encrypting Drives (SEDs). These drives have a specially designed hardware component that performs the encryption without causing any performance degradation. The encryption key — Media Encryption Key (MEK) — is generated on board the drive and never leaves the drive.

Encryption is enabled by default. The cluster generates an Authentication Key (AK) PIN that is used to lock and unlock the drives. The AK PIN can be modified to comply with key rollover requirements. During the process, the software generates a new PIN per each Solid State Drive (SSD). Old PINs are kept for as long as the operation continues, to ensure access to SSDs that are not yet changed. When the process is complete, the new PINs are kept in memory and the old PINs are retired.

All cryptographic operations are performed by a Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module, Cryptographic Module Validation Program (CMVP) certificate # 3290. The cryptographic module, the KIOXIA TCG Enterprise SSC Crypto Sub-Chip, is located on the chip of each SED. The cryptographic algorithms used for key generation, and the encryption and decryption of data are identified in the following table:

Function	Algorithm	CAVP Certificate Number
Key Generation	Deterministic Random Bit Generator (DRBG)	1890
Encryption and Decryption	Advanced Encryption Standard (AES)	5067, 5068

Table 14 - Cryptographic Algorithms

Keys are zeroized when no longer required, in accordance with FIPS 140-2.

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

7.3 USER DATA PROTECTION

The TOE manages access to the storage arrays by enforcing the Volume Access Control SFP. Initiators are only permitted to access LUNs based on Initiator ID, Target ID, and configured VLANs. Additionally, Initiators can be assigned to an Initiator Group in order to access a volume's disk space. When a volume is mapped to an Initiator Group, a LUN is automatically assigned. Initiator Groups can be mapped to multiple volumes.

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

7.4 IDENTIFICATION AND AUTHENTICATION

Users may access the TOE management functions via a web-based GUI or CLI. Both methods require users to authenticate with a valid username and password prior to gaining access to any TOE functions. The TOE can be configured to use local authentication or external authentication through Lightweight Directory Access Protocol (LDAP). Once successfully authentication, users are bound to their assigned role.

Obscured feedback is displayed to users during password collection. Only dots are echoed by the GUI, and no characters are echoed for the CLI.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2.

7.5 SECURITY MANAGEMENT

The GUI and CLI interfaces provide functionality for authorized users to manage the TOE. Each user session is bound to a role upon login, and that role determines access permissions. The TOE supports three roles: Read-Only, Configuration, and Admin.

Users assigned the Admin role can perform all user commands and manage all user accounts. Users assigned the Configuration role can perform all storage array configuration actions but cannot manage users. Users assigned the Read-Only role can view all storage array information but cannot perform any configuration changes.

When volumes are created, initially no mappings to Initiators exist. Users with the Admin and Configuration roles have the ability to configure mappings to expose the volumes to Initiators.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

The TOE provides reliable time stamp information used in the generation of audit records. Time is obtained from the system clock.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.7 TOE ACCESS

The TOE can be configured to display an advisory message to users on login, warning of unauthorized use. Authenticated user sessions may be terminated by the user at any time, or be terminated by the TOE after a configured amount of time of inactivity.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
X-Brick	An X-Brick is the basic building block of an XtremIO array. Also referred to as a “cluster”, one X-Brick may consists of up to five or six storage nodes.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
AK	Authentication Key
API	Application Program Interface
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
D@RE	Data at Rest Encryption
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
ID	Identification
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number

Acronym	Definition
MEK	Media Encryption Key
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
REST	Representational State Transfer
SAE	Support Assist Enterprise
SAN	Storage Area Network
SED	Self Encrypting Drive
SFP	Security Function Policy
SFR	Security Functional Requirement
SSD	Solid State Drive
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VLAN	Virtual Local Area Network
XMS	XtremIO Management Server

Table 16 – Acronyms