Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2059-000-D102
Version: 1.6
15 March 2021

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

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. This 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™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978 Security Target
ST Version:	1.6
ST Date:	March 15, 2021

1.3 TOE REFERENCE

TOE Identification:	Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978.444.444, Solutions Enabler 9.1 and Unisphere for PowerMax 9.1 with security patches: DSA-2019-186, DSA-2019-193, DSA-2020-062, DSA-2020-065, DSA-2020-130, DSA-2020-221
TOE Developer:	Dell EMC
TOE Type:	Data Storage (Other Devices and Systems)

1.4 TOE OVERVIEW

VMAX All Flash and PowerMax provide a platform for large scale storage operations, enabling organizations to grow, easily share, and cost effectively manage massive amounts of block storage.

The core element of VMAX All Flash is the V-Brick. Each V-Brick has one engine, two Disk Array Enclosures (DAEs), and usable capacity with fully redundant components. Flash Capacity Packs are used to scale up to 4 petabytes. The VMAX All Flash scales by aggregating up to eight V-Bricks as a single system with fully shared connectivity, processing, and capacity resources. Each V-Brick supports up to 72 central processing unit (CPU) cores, scaling to a maximum of 576 cores per array.

The core element of PowerMax is the Brick. Each Brick includes an engine with two PowerMax directors, packaged software, cache, and two 24-slot Drive Array Enclosures. Drive capacity for each Brick can be expanded to support a total usable capacity of up to 1.0 petabytes of effective capacity (PBe) on the PowerMax 2000 and up to 4.0 PBe on the PowerMax 8000.

The PowerMaxOS is an open storage and hypervisor converged operating system that provides direct access to hardware resources. PowerMaxOS provides the following services:

- Provides functional support for the PowerMax and VMAX hardware
- Manages system resources and provides support for I/O interfaces
- Provides maintenance and serviceability support
- Provides support for system availability including fault monitoring, detection, and fault correction
- Defines the priority of tasks, including basic system maintenance, I/O processing, and application processing. Interrupts and prioritizes tasks from microprocessors (e.g. ensures that fencing off failed areas takes precedence over other operations)

VMAX All Flash and PowerMax offer Redundant Array of Independent Disks (RAID) protection levels 5 and 6 to match different data protection requirements.

Security management may be performed using the Solutions Enabler Command Line Interface (CLI), or the Unisphere for PowerMax Graphical User Interface

(GUI). Either application may be used by authorized administrators to configure access from host devices to the storage resources. Audit records provide evidence of all such configuration operations.

The TOE is a combined software and hardware TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is made up of the VMAX All Flash and PowerMax models with PowerMaxOS 5978, Solutions Enabler and Unisphere for PowerMax, as described in Table 1.

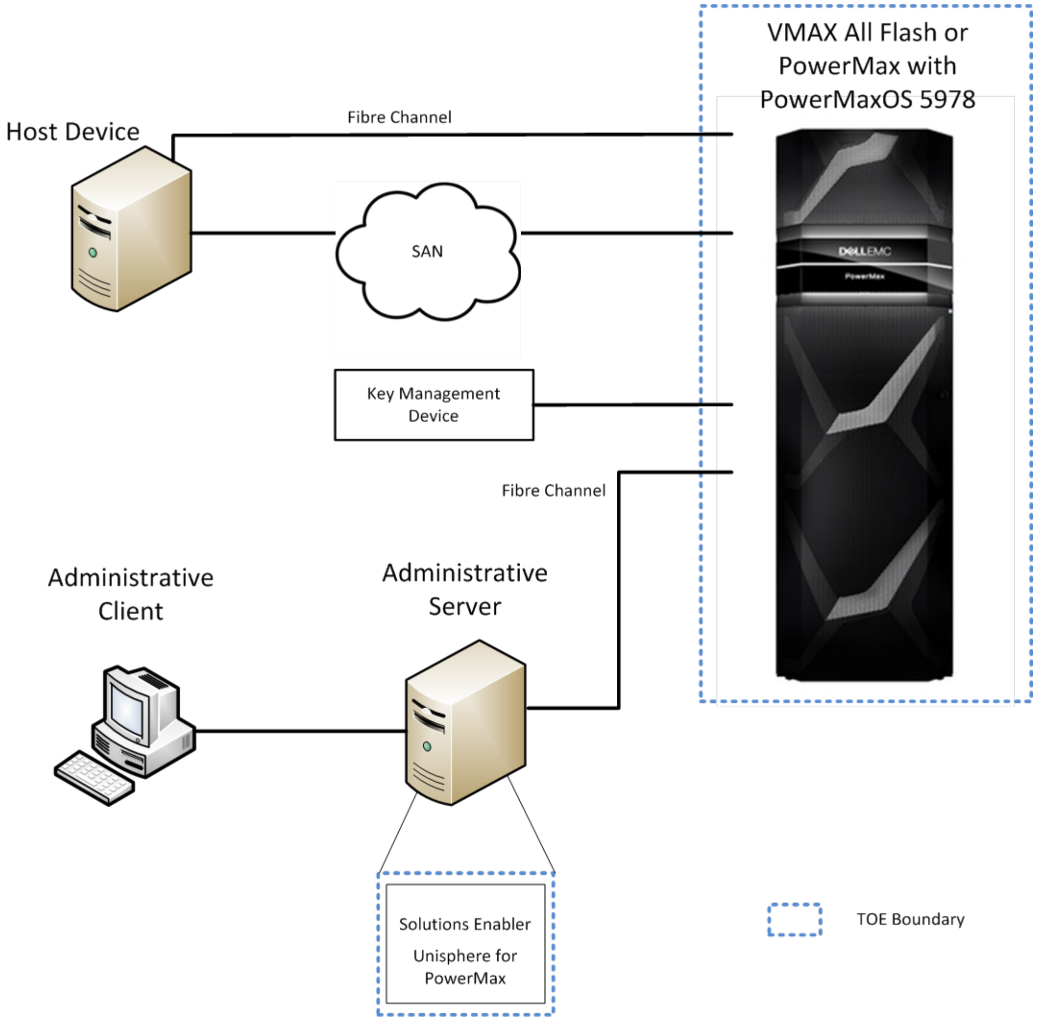

Figure 1 – VMAX/PowerMax TOE Diagram

TOE Component	Model/Version
VMAX All Flash	250F

TOE Component	Model/Version
(hardware)	950F
PowerMax (hardware)	2000
	8000
PowerMaxOS (software)	Version 5978.444.444
Solutions Enabler (software)	9.1
Unisphere for PowerMax (software)	9.1

Table 1 – TOE Hardware and Software

Host devices communicate with VMAX or PowerMax over Fibre Channel or Fibre Channel over Ethernet (FCoE). The administrative client communicates with the administrative server over Hypertext Transfer Protocol Secure (HTTPS) for the GUI and Secure Shell (SSH) for the CLI.

1.5.1.1 TOE Delivery

The TOE is delivered to customers via commercial carrier, such as UPS or FedEx. When the TOE is delivered, the customer receives:

- The VMAX or PowerMax hardware with the PowerMaxOS software. The customer is not required to load software on the hardware
- A CD-ROM with:
  - The user guidance documentation (in Portable Document Format (PDF))
  - Solutions Enabler software (as an executable file (.exe) for Windows)
  - Unisphere for PowerMax software (as an executable file (.exe) for Windows)

1.5.2 TOE Environment

The following operating system, hardware and network components are required for operation of the TOE in the evaluated configuration.

Non-TOE Component	Software and Hardware
Administrative Client	• Windows 10 • Firefox (55.0) • General purpose computing hardware

Non-TOE Component	Software and Hardware
Administrative Host	• Windows Server 2016 • General purpose computing hardware
Host Device	• Windows Server 2016 • Host Bus Adapter connected to a Storage Area Network (SAN) • General purpose computing hardware

Table 2 – Non-TOE Hardware and Software

1.5.3 TOE Guidance

The TOE includes the following guidance documentation (**Note:** this guidance can also be applied to v9.1):

- Dell EMC PowerMax Family Security Configuration Guide, Revision 01, Published May 2018
- Dell EMC™ Unisphere for PowerMax™ Version 9.0.0 Installation Guide REV 01, Published May 2018
- Dell EMC™ Unisphere for PowerMax™ Version 9.0.0 Online Help (PDF version), Published May 2018
- Dell EMC™ Solutions Enabler Version 9.0 Installation and Configuration Guide REV 01, Published May 2018
- Dell EMC™ Solutions Enabler Version 9.0 CLI Reference Guide REV 01, Published May 2018

1.5.4 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 and filtered by authorized administrators.
User Data Protection	The Block Storage Access Control SFP ensures that only authorized host devices may access data stored on the TOE. The TOE ensures that residual information is inaccessible when storage resources are reassigned. RAID functionality protects from potential data loss due to integrity errors in the data.

Functional Classes	Description
Identification and Authentication	Administrative users must be identified and authenticated prior to being granted access to the TOE. User authentication information is obscured as it is entered.
Security Management	The TOE provides management capabilities via a Web-Based GUI (over HTTPS), or a CLI (over SSH). Management functions allow the administrators to configure the attributes associated with the Block Storage Access Control SFP, perform user management, and to view audit logs. Security roles are provided to limit administrator access to a subset of the security management functions.
Protection of the TSF	Reliable timestamps are provided in support of audit record creation.

Table 3 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

Secure Shell (SSH) between the Administrative Client and the Administrative Server is supported on the TOE by OpenSSL 1.0.2 as part of Solutions Enabler. Likewise, Transport Layer Security (TLS) between the Administrative Client and the Administrative Server is supported on the TOE by a Java8 implementation within Unisphere for PowerMax. This functionality is not addressed by the security claims.

The following features are excluded from this evaluation:

- Data at Rest Encryption (D@RE)
- File, Open Systems and Mainframe storage
- Unisphere for VMAX and Solutions Enabler is supported on 64 bit Windows and Linux operating systems
- Unisphere for VMAX works with Firefox (30 or higher) and Chrome (21.0.1180 or higher)

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 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

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

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.

Threat	Description
T.ACCESS	Access to storage data could be improperly granted to host devices which should not have access to it.
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.DATALOSS	An unauthorized user could gain access to data on a disk if the logical disk has been allocated to another subject.
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.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICY

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 describes the OSP that is presumed to be imposed upon the TOE by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.RAID	User data must be protected from loss due to disk failure.

Table 5 – Organizational Security Policy

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.NOEVIL	The authorized 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 protect the data that it has been entrusted to store from unauthorized access.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide a means of logging security related events. The audit records must be viewable, and users must be able to filter the records by date and user.
O.IDAUTH	The TOE must be able to ensure that administrative users are identified and authenticated prior to allowing access to administrative functions and TSF data.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
O.PROTECT	The TOE must protect against inadvertent access to data. The TOE must ensure that data is removed prior to reallocation of the resource.
O.TIME	The TOE must provide reliable timestamps.

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.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator 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.ACCESS	T.ACCOUNT	T.DATALOSS	T.UNDETECT	P.RAID	A.LOCATE	A.NOEVIL
O.ACCESS	X						
O.ADMIN	X	X		X			
O.AUDIT				X			
O.IDAUTH		X		X			
O.INTEGRITY					X		
O.PROTECT	X		X				
O.TIME				X			

	T.ACCESS	T.ACCOUNT	T.DATALOSS	T.UNDETECT	P.RAID	A.LOCATE	A.NOEVIL
OE.ADMIN							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 back to the threats addressed by the TOE.

Threat: **T.ACCESS**	Access to storage data could be improperly granted to host devices which should not have access to it.	
Objectives:	O.ACCESS	The TOE must protect the data that it has been entrusted to store from unauthorized access.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.PROTECT	The TOE must protect against inadvertent access to data. The TOE must ensure that data is removed prior to reallocation of the resource.
Rationale:	O.ACCESS mitigates this threat by allowing only authorized host devices access to protected data. O.ADMIN mitigates this threat by only allowing authorized administrators the ability to manage TOE access functions. O.PROTECT mitigates this threat by ensuring that data is removed prior to reallocation of a disk.	

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.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to ensure that administrative users are identified and authenticated prior to allowing access to administrative functions and TSF data.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. O.IDAUTH mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.	

Threat: **T.DATALOSS**	An unauthorized user could gain access to data on a disk if the logical disk has been allocated to another subject.	
Objectives:	O.PROTECT	The TOE must protect against inadvertent access to data. The TOE must ensure that data is removed prior to reallocation of the resource.
Rationale:	O.PROTECT mitigates this threat by providing removal of data on reallocation of the resource.	

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.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.AUDIT	The TOE must provide a means of logging security related events. The audit records must be viewable, and users must be able to filter the records by date and user.
	O.IDAUTH	The TOE must be able to ensure that administrative users are identified and authenticated prior to allowing access to

		administrative functions and TSF data.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.AUDIT counters this threat by ensuring that the TOE maintains a record of all management functions performed on the TOE. O.IDAUTH mitigates this threat by ensuring that all administrative users are identified and authenticated prior to gaining access to the TOE security management functions. O.TIME mitigates this threat by providing reliable timestamps for use with the audit records, thereby ensuring an accurate accounting of security related events.	

4.3.2 Security Objectives Rationale Related to the OSP

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

Policy: **P.RAID**	User data must be protected from loss due to disk failure.	
Objectives:	O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
Rationale:	O.INTEGRITY supports this policy by ensuring that the TOE provides the ability to protect data in the case of disk failure.	

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.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.ADMIN supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

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 TOE 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_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback

Class	Identifier	Name
	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_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps

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) [*modification of user roles, storage access configuration changes*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

6.2.1.2 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 [*users in the role of Administrator, SecurityAdmin, StorageAdmin or Auditor*] 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.

6.2.1.3 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 [*date, username*].

6.2.2 User Data Protection (FDP)

6.2.2.1 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 [*Block Storage Access Control SFP*] on
[*Subjects: host devices*
Objects: storage objects
Operations: read from and write to storage].

6.2.2.2 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 [*Block Storage Access Control SFP*] to objects based on the following: [
Subjects: host devices
Subject attributes: initiator
Objects: storage objects
Object attributes: masking view (which includes the host name, port group and storage group)
].

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 host device can access storage objects if:

- *The masking view includes the host name associated with the host device attempting to access storage*
- *The host name is associated with a valid initiator for the host device attempting to access storage*
- *The masking view includes the storage group associated with the storage object being accessed by the host device*
- *The host device is connected (directly or through a SAN) to a port that is part of the port group included in the storage masking view*

].

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*].

6.2.2.3 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*the storage array*].

6.2.2.4 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*parity data for RAID 5 and RAID 6*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*reconstruct the user data and send a notification*].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 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 **administrative** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.2 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 in the form of asterisks*] to the user while the authentication is in progress.

6.2.3.3 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 **administrative** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 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 [*Block Storage Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*masking view, including host name, port group and storage group*] to [*users in the Administrator and StorageAdmin roles*].

6.2.4.2 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 [*Block Storage 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 Administrator and StorageAdmin roles*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.3 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the operations listed in Table 11*] the [*TSF data listed in Table 11*] to [*the roles listed in Table 11*].

TSF Data Type	Operations	Roles
User account information	Create Query Modify Delete	Administrator SecurityAdmin
Roles	Create Query Modify Delete	Administrator StorageAdmin
Audit data	Query Delete	Administrator StorageAdmin SecurityAdmin Auditor

Table 11 – Security Management of TSF Data

6.2.4.4 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: [*manage storage access, manage users and roles, view audit records*].

6.2.4.5 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 [*Administrator, SecurityAdmin, StorageAdmin, Auditor*].

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

6.2.5 Protection of the TSF (FPT)

6.2.5.1 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.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.IDAUTH	O.INTEGRITY	O.PROTECT	O.TIME
FAU_GEN.1			X				
FAU_SAR.1			X				
FAU_SAR.3			X				
FDP_ACC.1	X						
FDP_ACF.1	X						
FDP_RIP.1						X	
FDP_SDI.2					X		
FIA_UAU.2				X			
FIA_UAU.7		X		X			
FIA_UID.2				X			
FMT_MSA.1		X					
FMT_MSA.3		X					
FMT_MTD.1		X					
FMT_SMF.1		X					
FMT_SMR.1		X					
FPT_STM.1			X				X

Table 12 – Mapping of SFRs to Security Objectives

6.3.1 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 protect the data that it has been entrusted to store from unauthorized access.	
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 identifying the rules and attributes of the Block Storage Access Control SFP, which are used to control host device access to data stored on the TOE.	

Objective: **O.ADMIN**	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	
Security Functional Requirements:	FIA_UAU.7	Protected authentication feedback
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FIA_UAU.7 supports this objective by preventing the inadvertent viewing of passwords, thereby reducing the risk of unauthorized users accessing TOE security functions. FMT_MSA.1 and FMT_MSA.3 support this objective by providing restrictions on access to the attributes that configure the Block Storage Access Control SFP. FMT_MTD.1 supports this objective by providing controls on the access to TSF data that is used to enforce security functions. FMT_SMF.1 meets this objective by providing the management functions to securely manage the TOE. FMT_SMR.1 supports this objective by ensuring that specific roles are defined to govern management of the TOE.	

Objective: **O.AUDIT**	The TOE must provide a means of logging security related events. The audit records must be viewable, and users must be able to filter the records by date and user.	
Security Functional	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review

Requirements:	FAU_SAR.3	Selectable audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 provides the means to review audit records. FAU_SAR.3 provides the ability to filter the records by date or user. FPT_STM.1 provides reliable time stamps in support of audit records.	

Objective: **O.IDAUTH**	The TOE must be able to ensure that administrative users are identified and authenticated prior to allowing access to administrative functions and TSF data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Rationale:	FIA_UAU.2 meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. FIA_UAU.7 supports this objective by protecting the passwords used to gain administrative access from accidental disclosure, thereby reducing the risk of an unauthorized user gaining access to administrative functions and TSF data. FIA_UID.2 supports this objective by ensuring that the identity of each TOE Administrator is known before allowing access to TOE functions and data.	

Objective: **O.INTEGRITY**	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.	
Security Functional Requirements:	FDP_SDI.2	Stored data integrity monitoring and action
Rationale:	FDP_SDI.2 meets this objective by providing the RAID functionality that protects against integrity errors due to a hardware fault.	

Objective: **O.PROTECT**	The TOE must protect against inadvertent access to data. The TOE must ensure that data is removed prior to reallocation of the resource.

Security Functional Requirements:	FDP_RIP.1	Subset residual information protection
Rationale:	FDP_RIP.1 supports this objective by ensuring that the content of the storage array is cleared on deallocation of the resource.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 satisfies this objective by providing reliable time stamps.	

6.4 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_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_RIP.1	None	N/A	
FDP_SDI.2	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.7	FIA_UAU.1	✓	
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.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	

Table 13 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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.

The assurance requirements are summarized in Table 14.

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_CMC.2	Use of a CM system

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

Table 14 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section describes how the TOE security functions meet the security requirements.

7.1 SECURITY AUDIT

The TOE generates audit records for administrative actions performed on Unisphere for PowerMax or Solutions Enabler. These actions include the modification of user role information, and changes to masking view information that impacts access by host devices. Audit records include the information shown in Table 15.

Property	Description
Record Number	Unique identifier for the audit entry. The record number is incremented by one as each new record is generated.
Text	Summary of the operation being performed
Time	Date and time that the audit entry was made
Application ID	This is the specific application on the storage system that triggered the entry
Username	Name of the user who issued the command that resulted in the creation of the audit record
Function Class	Generic audit category for the operation on the storage system
Action Code	Specific audit code for the operation on the storage system. Action codes indicate details such as successful or failed connections, loss of connection, reboot, file transfer, or configuration change.
Host	Host operating on the storage system. This is the name given to the host

Table 15 – Audit Record Details

The audit functionality is stopped or started with the Unisphere for PowerMax and Solutions Enabler applications. A specific audit record is not generated for shutdown; however, the cessation of auditing can be viewed in the logs. An audit record is generated to indicate startup.

Audit records may be viewed using the Unisphere for PowerMax or Solutions Enabler CLI. The audit records may be filtered by date or username. This is done in the Solutions Enabler CLI by using the options available for the symaudit command. This is done in the Unisphere for PowerMax GUI by opening the Auto Log Filter dialog and selecting the options on which to filter. Although other options are available, only the date and username filtering capabilities are included in the evaluation.

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

7.2 USER DATA PROTECTION

The TOE enforces a Block Storage Access Control SFP on host devices attempting to write to or read from storage objects within the TOE.

Host devices are identified by their respective initiators. Within the TOE, a masking view is created. The masking view includes:

- The host or host group, using a host name or host group name created by the TOE administrator. The host or host group may be assigned any convenient name; however, the initiator associated with that name must be valid for the host that is allowed access
- The port group which provides a list of all of the fibre channel ports on which the host device may access the TOE
- The storage group within the TOE to which the host device or devices are granted access

A host device is able to access storage objects if:

- The masking view includes the host name associated with the host device attempting to access storage
- The host name is associated with a valid initiator for the host device attempting to access storage
- The masking view includes the storage group associated with the storage object being accessed by the host device
- The host device is connected (directly or through a SAN) to a port that is part of the port group included in the storage masking view

When a resource is deallocated from the storage array, the data is erased by being overwritten by zeros. The TOE performs a background destage operation to overwrite the disk. Other hosts reusing the logical space will see only zeros.

Storage objects are protected from corruption through the use of RAID groups. RAID 5 or RAID 6 configurations provide parity data, which is distributed over multiple drives. If the data on a drive becomes unavailable, the data can be rebuilt from the parity data on the other drives. Unisphere can be configured to display an alert on the Unisphere for PowerMax GUI when a data integrity error is detected.

VMAX 250F hardware supports RAID 5 (3+1), RAID 5 (7+1) and RAID 6 (6+2). The 950F model supports RAID 5 (7+1) and RAID 6 (14+2). The PowerMax 2000 model supports RAID 5 (3+1), RAID 5 (7+1) and RAID 6 (6+2). The PowerMax 8000 model supports RAID 5 (7+1) and RAID 6 (6+2).

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_RIP.1, FDP_SDI.2.

7.3 IDENTIFICATION AND AUTHENTICATION

Users must be identified and authenticated prior to being granted access to security management functionality within the Solutions Enabler CLI or the Unisphere for PowerMax GUI. In the evaluated configuration, administrative users login directly to Unisphere for PowerMax using a username and password. Identification and authentication is performed by Unisphere for PowerMax. Solutions Enabler ensures that users are identified and authenticated prior to being granted access, but does not perform the authentication of users. Administrative users must be authenticated by Unisphere for PowerMax or the Windows operating system. The authenticated identity is then passed to Solutions Enabler and the user is granted access. Although any user with credentials on the Administrative host machine may be able to access Solutions Enabler, unless the user has been assigned one or more roles, the user will not be able to view any system information or perform any administrative functions.

When entering the user password, Unisphere for PowerMax obscures the data being entered with asterisks.

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

7.4 SECURITY MANAGEMENT

Two management interfaces are provided to perform security management for the TOE: the Unisphere for PowerMax GUI and the Solutions Enabler CLI. The Unisphere for PowerMax GUI is accessed through a web browser on the administrative host. The Solutions Enabler application is also installed on the administrative host and provides a set of commands that may be used to perform security management functions.

Both interfaces provide functionality to create, query, modify and delete the security attributes that make up the masking view. The default values for these attributes are considered to be restrictive in that they do not exist until the masking view is created by a user in the Administrator or StorageAdmin role. Security management functionality is also provided to:

- manage user accounts, including associating users with roles
- view audit data

The roles and associated permissions shown in Table 16 are included in the evaluated configuration. Other default roles exist; however, only the roles required to perform the claimed security functions are included here for simplicity. Users may be assigned up to four roles.

Function	Roles with required permissions			
	Administrator	StorageAdmin	SecurityAdmin	Auditor
Manage user account	✓		✓	

Function	Roles with required permissions			
	Administrator	StorageAdmin	SecurityAdmin	Auditor
information				
Assign roles	✓		✓	
View audit data	✓	✓	✓	✓
Set storage access controls	✓	✓		

Table 16 – Security Management Roles and Functions

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

7.5 PROTECTION OF THE TSF

The TOE provides reliable time stamps for inclusion in audit records.

TOE Security Functional Requirements addressed: FPT_STM.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrative host	The term 'Administrative host' refers to the computer that supports the Unisphere for PowerMax and Solutions Enabler TOE components.
Host Device	A host device is the device that accesses storage objects on behalf of an application or user.
Masking view	A masking view is made up of host information, port group information and storage group information.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DAE	Disk Array Enclosure
EAL	Evaluation Assurance Level
FCoE	Fibre Channel over Ethernet
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
PBe	petabytes of effective capacity

Acronym	Definition
PDF	Portable Document Format
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SFP	Security Function Policy
SFR	Security Functional Requirement
SP	Special Publication
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

Table 18 – Acronyms