EMC Corporation

EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2

Security Target

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

Prepared for:

EMC Corporation
171 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 (508) 435-1000
Email: info@emc.com
http://www.emc.com

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2, and will hereafter be referred to as the TOE throughout this document. The TOE consists of hardware and software that provide data availability, storage, and management capabilities for mid- to high-end data storage systems. The TOE can operate within a Storage Area Network[1] (SAN) or connected directly to a device[2].

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC Corporation EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2 Security Target
ST Version	Version 2.1
ST Author	Corsec Security, Inc.

[1] Please refer to Section 9.2 for a definition of the term "SAN".
[2] The term "device" refers to any type of computing device that can attach to or access storage on a VMAX system. Typical usage refers to application servers (e.g., a web server or file server), and mainframes (i.e., computing devices used to house large databases).

ST Title	EMC Corporation EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2 Security Target
ST Publication Date	2015-07-27
TOE Reference	EMC® HYPERMAX™ OS 5977.596.583, EMC Solutions Enabler 8.0.2.0 EMC Unisphere for VMAX™ 8.0.2.6 EMC VMAX 100K System Bay: • P/N 900-887-024 • P/N 900-887-025 • P/N 900-887-026 EMC VMAX 200K System Bay: • P/N 900-887-021 • P/N 900-887-022 • P/N 900-887-023 EMC VMAX 400K System Bay: • P/N 900-887-028 • P/N 900-887-029 • P/N 900-887-030 EMC VMAX Storage Bay: • P/N 100-887-053-02 • P/N 100-887-055-02 • P/N 100-887-057-02 EMC VMAX Disk Array Enclosure (P/N 100-887-010-03) EMC VMAX Engine (P/N 100-887-011-02) EMC VMAX MMCS (P/N 100-887-103-00) EMC VMAX Front End I//O Modules: • Fibre Channel (P/N 303-092-102B) • FCoE (P/N 303-142-100A) EMC VMAX Back End I/O Module: • Serially Attached SCSI (P/N 303-161-101B-04)
FIPS 140-2 Status	N/A

1.3 Product Overview

The VMAX Series storage solution offers a physical storage array combined with operating and management software to fulfill an organization's data storage and availability needs. Application servers can use the storage array to store mission-critical data and facilitate the sharing of important files. Storage arrays can range in size from hundreds of terabytes to petabytes of raw[3] data storage capacity, and can be composed of a combination of high-capacity magnetic platter disk drives, or high-speed Enterprise Flash[4] drives. Disks in the storage array can be further grouped into a collection of Redundant Array of Independent Disks (RAID[5]) groups to ensure reliability and mitigate data loss.

[3] The term "raw" refers to the total storage capacity offered by the VMAX disks. After users apply RAID and the VMAX array claims a small portion of the space for its own use, the drives offer less total storage capacity.
[4] Please refer to "Flash" in Section 9.2 Terminology for a definition of the term "flash".
[5] Please refer to "RAID" in Section 9.2 Terminology for a definition of the term "RAID".

VMAX arrays offer storage to direct-attached and SAN-attached devices. The SAN is composed of a series of controller cards and fabric[6] connections that provide redundant access to the storage array. The SAN architecture allows many different types of devices to share the services that a single VMAX array can provide, and allows organizations to manage storage across all devices from a single interface. Simplified management of storage for devices allows users greater control over storage allocation, improved fault tolerance, and simplified backups versus directly attaching storage to individual devices.

Several racks filled with VMAX components, called bays, organize the VMAX hardware into serviceable units. There are two types of bays: System Bays, which contain the components necessary for controlling and servicing the VMAX array; and Storage Bays, which hold disks (up to 240 per bay) and Link Control Cards (LCCs). LCCs provide several services for disk drives, including data connectivity, environmental monitoring, failover[7] control, drive detection, and other functions related to drive control and reliability. Depending on solution level, the VMAX array can include one System Bay and one to ten Storage Bays. The VMAX SE[8] alternative offers an integrated system bay with up to 120 disks and an optional Storage Bay.

Each Storage Bay connects (directly or daisy-chained) to the System Bay, which connects to devices that use the VMAX array. The System Bay mediates access between devices and the data stored on the VMAX array.

[6] Please refer to “Fabric” in Section 9.2 Terminology for a definition of the term “fabric”.
[7] Please refer to “Failover” in Section 9.2 Terminology for a definition of the term “failover”.
[8] SE – Single Engine

Table 2 below explains the differences between the VMAX 100K, 200K, and 400K models.

Table 2 VMAX 100K, 200K, and 400K

Model	Engine Support	Drive Support	Front End Ports	Internal Networking
100K	1-2 Engines • 24 2.1 GHz[9] Ivy Bridge cores • 128GB[10], 256GB, 512GB RAM[11]	Up to 1440 2.5" drives Up to 720 3.5" drives	Up to 64	56 Gb/s[12] 12-port InfiniBand switch
200K	1-4 Engines • 32 2.6 GHz Ivy Bridge cores • 128GB, 256GB, 512GB RAM	Up to 2880 2.5" drives Up to 1440 3.5" drives	Up to 128	56 Gb/s 12-port InfiniBand switch
400K	1-8 Engines • 48 2.7 GHz Ivy Bridge cores • 128GB, 256GB, 512GB RAM	Up to 5760 2.5" drives Up to 2880 3.5" drives	Up to 256	56 Gb/s 18-port InfiniBand switch

1.4 TOE Overview

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

The TOE is a combination of the software and hardware portions of the VMAX Series storage solution. EMC® develops VMAX arrays to provide enterprise-class data availability, storage, and management to a user's Information Technology (IT) infrastructure. The TOE components of the VMAX Series storage solution consists of:

- VMAX 100K, 200K, and 400K Hardware
  - VMAX System Bay
  - VMAX Storage Bay and Disk Array Enclosures (DAEs)
  - VMAX Engine hardware
  - VMAX MMCS[13]
  - Fibre Channel and FCoE[14] front end I/O modules
  - Serially Attached SCSI[15] (SAS) back end I/O modules

[9] GHz – Gigahertz
[10] GB – Gigabyte
[11] RAM – Random Access Memory
[12] Gb/s – Gigabit per second
[13] MMCS – Management Module Control Station
[14] FCoE – Fibre Channel over Ethernet
[15] SCSI – Small Computer System Interface

- VMAX Software
  - HYPERMAX OS[16] 5977, the VMAX operating environment,
  - Solutions Enabler 8.0.2, a Command Line Interface (CLI) that allows management and configuration of VMAX arrays, and
  - Unisphere for VMAX (Unisphere), a web-based Graphical User Interface (GUI) that allows management and configuration of VMAX arrays.

The VMAX 100K, 200K, and 400K Architecture provides a highly scalable storage subsystem with consolidation and efficiency technologies for enterprise consumers. A standard configuration can include one to eight system bays and up to 10 standard Storage Bays for expansion. System Bays house the VMAX Engines, the MMCS (including KVM[17]), DAEs, and other additional components. Storage Bays provide additional expansion for DAEs for storage of multiple Flash, Fibre Channel, and SAS drives.

Each VMAX Engine provides support for a Front End (FE) Adapter housing front end and back end I/O modules, cards that plug into the Engine that provide front end Fibre Channel and FCoE ports and back end SAS ports. Management and storage data flowing to and from the TOE is processed by the HYPERMAX operating environment executing on the VMAX Engines.

The HYPERMAX OS efficiently services devices' read and write (Input/Output (I/O)) requests. HYPERMAX is designed to work with the VMAX architecture to manage I/O operations while minimizing the delays typically associated with such operations. Techniques that increase efficiency include caching of data in a large area of global memory[18], intelligent prefetching[19], and asynchronous writes to disk[20].

The MMCS is an administrative server delivered with the TOE. On-site EMC engineers use a KVM connection to the MMCS to deploy the VMAX system into its evaluated configuration. Access to the MMCS is restricted by contract to EMC engineers only with credentials obtained from a secure website that are specific to each user and activity and valid for a limited duration. Its use (after system deployment) is not part of the evaluated configuration. Via Ethernet port connections, it maintains remote connectivity to EMC monitoring centers, provides remote support notification, and allows local and remote support connectivity to the TOE. For redundancy, every VMAX array contains a second MMCS in case the primary MMCS should fail. Any use of the MMCS by EMC engineers during deployment of the TOE requires bringing the TOE out of the evaluated configuration. In the evaluated configuration of the TOE, neither KVM or Ethernet connections to the MMCS are permitted.

Solutions Enabler includes the VMAX Command Line Interface (SYMCLI). Unisphere is a web-based GUI. These two interfaces provide the management and configuration framework for VMAX arrays. Solutions Enabler administrators[21] can enter commands manually or write scripts to manage and configure the TOE through SYMCLI. Both interfaces require that administrators identify themselves before the TOE performs any actions on their behalf. Unisphere also requires administrators' identities to be authenticated.

Solutions Enabler also includes the VMAX Application Programming Interface (SYMAPI). SYMAPI consists of a set of libraries and support services that provide several interfaces designed to be called by SYMCLI, Unisphere, and third party SYMAPI-consuming applications which reside outside of the TOE boundary and whose use is excluded from the evaluated configuration of the TOE.

[16] OS – Operating System
[17] KVM – Keyboard, Video, and Mouse
[18] Please refer to "Global Memory" in Section 9.2 Terminology for a definition of the term "Global Memory".
[19] Intelligent prefetching is a technique used to predict what data will be accessed next, based on what data has been recently accessed.
[20] Asynchronous writes occur because devices write data to global memory, rather than directly to the disk. HYPERMAX performs the disk write as a separate operation.
[21] Unless explicitly noted, the term "administrator" is used in this document to refer to an individual who manages the TOE and not the "administrator" role.

The TOE does not present physical disks to users; instead, administrators define logical disks. Logical disks typically include segments from multiple physical disks, rather than occupying physically adjacent areas on a single disk. When creating a logical disk, administrators can define the capacity of the disk. Administrators configure one or more logical disks into pools— groups of logical disks—and give users access to the pools.

The TOE offers administrators the ability to provide tiered storage for users with differing speed requirements. The storage array must contain multiple types of disks, such as high speed Enterprise Flash drives and high capacity magnetic drives, for this feature to function. Administrators can select the type of physical disks that will contain a logical disk, and thereby provide tiered storage based on the disk type selected. Users of such logical disks benefit from the shortened access times that faster physical disks provide whenever the TOE must retrieve data into global memory.

The TOE offers a secure erase feature that allows administrators to destroy the data on a physical disk before the physical disk is removed from the storage array. Administrators can select one of several algorithms to use, and can set the number of passes to make. After the secure erase function has completed, no residual information exists on the erased disk.

The TOE offers an Instantaneous Volume Table Of Contents (iVTOC) function. iVTOC is a method of formatting disks or partitions on disks with 0's while still allowing the TOE to access the disk. If the area of the disk accessed is the portion being formatted or scheduled to be formatted, then the TOE returns all 0's in place of actual data, until the formatting operation is complete and data is stored in those portions of the disk.

The TOE is capable of grouping disks into RAID groups. The supported RAID types are:

- RAID 1, RAID 5 (3+1) and RAID 5 (7+1),
- RAID 6 (6+2) and RAID 6 (14+2).

The RAID configurations allow the TOE to preserve data stored within a RAID group when a disk in the RAID group fails. When a disk in a RAID group fails and is replaced, the TOE automatically rebuilds the data from the other drives and populates the new disk.

The TOE provides access control functions that restrict the ability of administrators to manage pools of logical disks. From an administrative workstation, administrators can use Solutions Enabler and Unisphere to assign management rights to other administrative workstations based on each workstation's unique identifier (typically the hostname). Such workstations are henceforth referred to as administrative hosts or Solutions Enabler Hosts.

The TOE can provide the following services:

- Monitor the integrity of stored user data against unintentional corruption,
- Control access to stored user data and storage space,
- Control access to the ability to manage user data storage.

1.4.1 TOE Environment

The evaluated deployment configuration of the TOE requires the following environmental components in order to function properly:

- a SAN to allow devices to connect to the TOE,
- devices on the network that use the storage that the TOE provides,
- cables and connectors that allow the devices to connect to the SAN,

- an administrative host with an operating system that supports Solutions Enabler, Unisphere, and a web browser. Supported web browsers include Internet Explorer and Mozilla Firefox.

The TOE is intended to be deployed in a physically secure cabinet room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is intended to provide storage to devices on a SAN or directly attached to the VMAX array. For the TOE to operate correctly, all devices must be connected to the TOE directly or through the SAN. The TOE environment is required to provide for this configuration.

The TOE is managed through a CLI and web-based GUI. Administrators must access these interfaces from a trusted administrative host that supports the Solutions Enabler software and a graphical web browser. The CLI and web GUI are part of the TOE. Administrators access the CLI via the Solutions Enabler product, and the web GUI through a web browser.

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all the components of the TOE and the TOE Environment.

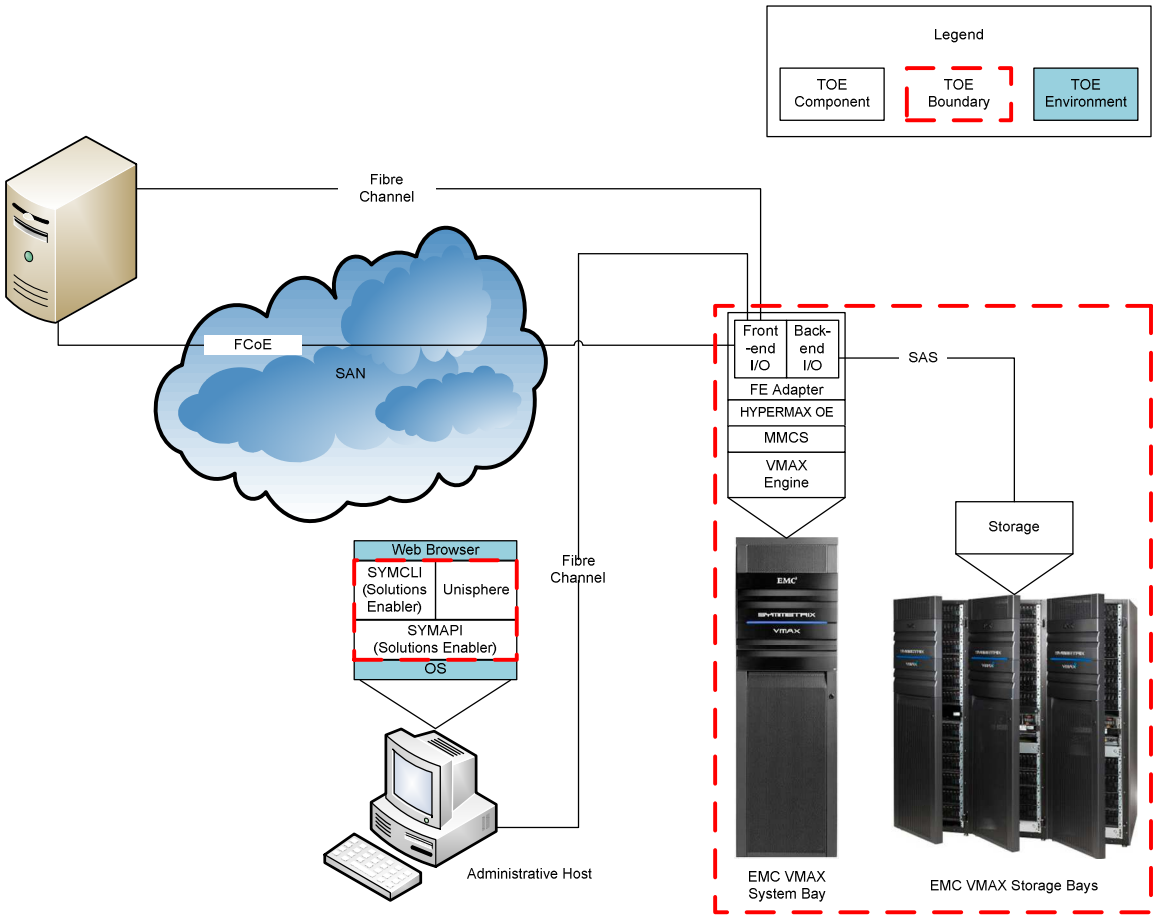

Figure 1 TOE Boundary

The TOE is a hardware and software storage solution which includes the custom VMAX 100K, 200K, and 400K hardware components. The TOE software components are installed on the VMAX hardware and a separate administrative host as depicted in Figure 1 above.

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

- *TOE environment:*
  1. an administrative host with Windows Server 2012 R2 and Internet Explorer 11 installed on general purpose hardware
  2. a server with a HBA[22] connected to the SAN, running Windows Server 2012 R2 installed on general purpose hardware

- *TOE components:*
  1. the VMAX 100K, 200K, and 400K in a "Single Engine System Bay Rack" configuration, which includes one Engine and two DAEs
  2. the HYPERMAX OS installed on the VMAX hardware
  3. front end Fibre Channel or FCoE I/O modules
  4. Solutions Enabler 8.0.2 and Unisphere for VMAX 8.0.2 installed on the administrative host

1.5.1.1 Guidance Documentation

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

- *Admin Guides:*
  - EMC® VMAX Family with HYPERMAX OS Product Guide
  - EMC® VMAX Family 100K, 200K, and 400K Planning Guide
  - EMC® VMAX Family Security Configuration Guide
  - EMC® VMAX3 Family with HPERMAX OS 5977 Release Level HYPERMAX OS 5977.596.583 Release Notes
  - EMC® Solutions Enabler Array Management CLI User Guide Version 8.0.2
  - EMC® Solutions Enabler SRM Version 8.0.2 CLI User Guide
  - EMC® Solutions Enabler CLI Version 8.0.2 Command Reference[23]
  - EMC® Solutions Enabler, VSS Provider, and SMI-S Provider Version 8.0.2 Release Notes
  - EMC® Unisphere for VMAX Version 8.0.2 Online Help
  - EMC® Unisphere for VMAX Version 8.0.2 Release Notes

- *Installation Guides:*
  - EMC® Solutions Enabler Version 8.0.2 Installation Guide
  - EMC® Unisphere for VMAX Version 8.0.2 Installation Guide

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF, and
- TOE Access.

[22] HBA – Host Bus Adapter
[23] The 8.0.2 version of this guide is included to address errata discovered in the TOE release version.

1.5.2.1 Security Audit

The TOE is capable of generating audit messages that administrators can review. Audit review is provided through Solutions Enabler and Unisphere. Audits show the history of administrator commands and the identity of the user that performed the command.

1.5.2.2 User Data Protection

The TOE controls access to the storage that it provides to users. Users can use and manage the storage only if an administrator has configured the TOE's Block Storage Access Control Policy to allow access to an area of storage. If administrators have not assigned permissions to a user for a storage area, then the user cannot access or manage that storage.

The TOE protects stored user data from unintentional corruption through the use of RAID groups.

The TOE can erase all data from a physical disk that is to be removed from the storage array. Several algorithms provide the TOE with the ability to ensure that no residual information remains on an erased disk.

The TOE can apply iVTOC functionality to logical disks, which results in the TOE formatting the disks. Any information previously on the disk or partition that was formatted is replaced with 0's upon initiation of the iVTOC process.

1.5.2.3 Identification and Authentication

Each Unisphere administrator is provided with a username, password, and from one to four roles. The TOE ensures that Unisphere administrators must identify themselves and authenticate their identities before accessing any of the functionality available in Unisphere. Administrators that use Solutions Enabler must identify their identities before performing any actions through Solutions Enabler. TOE administrators can give each user of the TOE access to specific storage arrays based on their identity, role, and allowed content types.

1.5.2.4 Security Management

The TOE provides administrators with the ability to manage the behavior of security functions and security attributes. Administrators are assigned management rights from seven roles: Administrator, SecurityAdmin, StorageAdmin, Auditor, Monitor, PerfMonitor, and None. Administrators are assigned from one to four roles. The TOE allows administrators to manage the attributes associated with the Storage Access Control Policy. Only authorized administrators are allowed to manage users.

1.5.2.5 Protection of the TSF

The TOE's internal clock provides timestamps in the audit log, which are used to provide a chronological order of events during audit review.

1.5.2.6 TOE Access

Access banners are presented to any TOE administrator attempting to log into Unisphere. TOE Administrators create and customize the access banner to provide a notice and consent warning regarding the use of the TOE.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

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

- VMAX MMCS functionality, which provides remote support notification and local and remote support connectivity to the TOE,
- use of supported operating systems other than Windows Server 2012 R2,
- use of Solutions Enabler in client/server mode,
- use of third party SYMAPI-consuming applications,
- use of SATA[24] II drives,
- use of Solutions Enabler Host access types other than ADMIN and ALL,
- use of the Unisphere REST[25] API[26],
- iSCSI[27] support,
- TimeFinder,
- Database Storage Analyzer[28] (DSA) and its associated "DSA Admin" and "DSA read only" roles,
- VMAX Remote Data Facility (SRDF),
- Virtual Appliance Manager (vApp Manager) for Solutions Enabler,
- priority controls,
- ControlCenter, and
- use of crypto-generated numbers for identification of devices or hosts.

[24] SATA – Serial Advanced Technology Attachment
[25] REST – Representational State Transfer
[26] API – Application Programming Interface
[27] iSCSI – Internet SCSI
[28] A standalone Oracle database troubleshooting application included with Unisphere.

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM as of 2014-05-01 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with ALC_FLR.2 Flaw Reporting Procedures

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[29] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Natural threats: These are threats to the TOE Security Function (TSF) that are a natural byproduct of the systems that compose the TOE, such as electromagnetic interference on a line during transmission of user data.

The following threats are applicable:

Table 4 Threats

Name	Description
T.DATA_CORRUPTION	User data and configuration data could become corrupted due to hardware failure, unsafe environmental conditions, or incorrect system operations caused by malicious users outside of the controlled access facility where the TOE is housed.
T.IMPROPER_SERVER	A user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE, thus exposing configuration and user data to harm or to unauthorized access.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for them.

3.2 Organizational Security Policies

There are no Organizational Security Policies (OSPs) defined for this ST.

[29] IT – Information Technology

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 Assumptions

Name	Description
A.CONNECTIVITY	It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.
A.FIREWALL	It is assumed that the IT Environment must block all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE.
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.
A.MANAGE	It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.MMCS_PROTECT	it is assumed that no KVM or Ethernet connections will be made to the MMCS after deployment of the TOE, so that the MMCS cannot be used for local or remote access to the TOE.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 Security Objectives for the TOE

Name	Description
O.PROTECT	The TOE must protect configuration and user data that it has been entrusted to protect.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and provide the means to store and review that data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 IT Security Objectives

Name	Description
OE.PROPER_NAME_ASSIGNMENT	The TOE Environment must provide accurate unique server identifiers for each system that communicates with the TOE.
OE.SECURE_COMMUNICATIONS	The TOE Environment must provide untampered communications between systems connected to the SAN.
OE.SECURE_SERVERS	The TOE Environment must ensure that application servers communicating with the TOE do not allow unauthorized users or attackers access to the TOE.
OE.FIREWALL	The TOE Environment must ensure that the port designated for use by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.
OE.CONNECT	The TOE administrators will configure the IT Environment so that

Name	Description
	users can access data through a direct connection to the TOE, or so that zones are configured on the SAN that allow users to access data stored on the TOE.
OE.MMCS	The TOE Environment must ensure that no connections, either KVM or Ethernet, are made to the MMCS after system deployment, thereby preventing local or remote access to the MMCS.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
OE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

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

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_RIP.1a	Subset residual information protection	✓	✓		✓
FDP_RIP.1b	Subset residual information protection	✓	✓	✓	✓
FDP_SDI.2	Stored data integrity monitoring and action		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UAU.7	Protected authentication feedback		✓	✓	
FIA_UID.2	User identification before any action			✓	
FMT_MSA.1	Management of security attributes	✓	✓		

Name	Description	S	A	R	I
FMT_MSA.3	Static attribute initialization	✓	✓	✓	
FMT_MTD.1	Management of TSF Data (for general TSF data)	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable Time Stamps			✓	
FTA_TAB.1	TOE access banner			✓	

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

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 and authorization levels,
addition or removal of masking views,
addition or removal of storage groups, port groups, and/or initiator groups].

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 information*].

Application Note: The TOE's audit function cannot be stopped other than by the shutdown of the TOE. No "shutdown" audit record is generated, but auditing ends upon shutdown. When the TOE starts up again, an audit record is generated. An administrator can tell that the TOE previously shutdown by looking at the start up audit record and the audit record immediately preceding the start up audit record.

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.

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 [*the roles in Table 10*] with the capability to read [*the audit information defined in FAU_GEN.1.1, as specified in Table 10*] from the audit records.

Table 10 Audit Information Viewable by Role

Role	Audit Information Viewable
Administrator	All
SecurityAdmin	All
StorageAdmin	All
Auditor	All. This is the minimum role required to view the audit log.
Monitor	None
PerfMonitor	None
None	None

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.2 Class FDP: User Data Protection

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 Policy*] on [
Subjects: device accessing storage controlled by the TOE,
Objects: storage space,
Operations: read/write from storage.
].

Application Note: To simplify provisioning, TOE administrators perform masking operations, which associate the following three auto-provisioning groups (one of each type) with each other in a masking view: initiator group, port group (front-end ports), storage group (logical disks), and device *WWN*[30] . Administrators can modify these groups and masking views as provisioning needs change.

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1

The TSF shall enforce the [*Block Storage Access Control Policy*] on objects based on the following: [
Subject (device accessing storage controlled by the TOE) attributes:

- *initiator group*
- *port group*
- *masking view*

Object (storage space) attributes:

- *storage group*
- *device WWN*

].
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 device can access storage space on a logical disk if:

- *the device's initiator group is part of a masking view for the storage space,*
- *the device is connected (directly or through a SAN) to a port contained in that view's port group, and*
- *that view's storage group contains the logical disk.*
- *that view contains the device WWN for the storage*

].
FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on ~~the following~~ **no** additional rules.
FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on ~~the following~~ **no** additional rules.

[30] WWN – World Wide Name

Application Note: The subject and object attributes of the Block Storage Access Control Policy are managed by authorized TOE administrators according to FMT_MSA.1 through the TOE's administrative interfaces.

FDP_RIP.1a Subset residual information protection
Hierarchical to: No other components.
Dependencies: No dependencies
FDP_RIP.1.1a

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

FDP_RIP.1b Subset residual information protection
Hierarchical to: No other components.
Dependencies: No dependencies
FDP_RIP.1.1b

The TSF shall ensure that any previous information content of a ~~resource~~ **logical disk** is ~~made unavailable~~ **zeroized** upon the [allocation of the disk to] the following objects: [*the list of disks to be formatted using iVTOC functionality*].

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 [*unintentional integrity errors*] on all ~~objects~~ **user data**, based on the following attributes: [*mirroring for RAID 1; parity data for RAID 5 (3+1) and (7+1); and parity data for RAID 6 (6+2) and (14+2)*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data and notify the authorized administrator*].

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: None
Dependencies: None
FIA_ATD.1.1

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

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

FIA_UAU.7 Protected authentication feedback
Hierarchical to: None
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1

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

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 **by Unisphere or Solutions Enabler** before allowing any other TSF-mediated actions through **Unisphere or Solutions Enabler** on behalf of that user.

6.2.4 Class FMT: Security Management

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_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Block Storage Access Control Policy*] to restrict the ability to [*perform the actions listed in Table 11 on*] the security attributes [*listed in Table 11*] to [*the roles listed in Table 11*].

Table 11 Management of Security Attributes

Role	Actions	Security Attributes
Administrator	• Create • Query • Modify • Delete	• Group name, devices included in the group, and access control entries of device accessing storage controlled by the TOE • Initiator group, storage group, port group, and masking view of storage space
SecurityAdmin	• Query • Modify	• Access control entries of device accessing storage controlled by the TOE
StorageAdmin	• Create • Query • Modify • Delete	• Access control entries of device accessing storage controlled by the TOE • Initiator group, storage group, port group, and masking view of storage space
Auditor	• Query	• Group name, devices included in the group, and access control entries of device accessing storage controlled by the TOE • Initiator group, storage group, port group, and masking view of storage space

Application Note: The Block Storage Access Control Policy does not actually control access to the security attributes; rather these attributes are used in the enforcement of the Block Storage Access Control Policy and are restricted by role-based access control.

FMT_MSA.3 Static attribute initialization
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 Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Administrator and SecurityAdmin roles*] to specify alternative initial values to override the default values when an object ~~or information~~ is created.

FMT_MTD.1 Management of TSF Data (for general 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 [*manage*] the [*items in Table 12*] to the [*roles in Table 12*].

Table 12 Management of TSF Data

Role	Actions	TSF Data
Administrator	• Create • Modify	• Account passwords • Alerts and thresholds to monitor performance • Replication and reservation settings
Administrator SecurityAdmin	• Assign	• Roles
Administrator	• Query • Add	• License keys
SecurityAdmin	• Create • Modify	• Account passwords • Replication and reservation settings
StorageAdmin	• Modify	• Alerts and thresholds to monitor performance • Replication and reservation settings
StorageAdmin	• Query • Add	• License keys
PerfMonitor	• Modify	• Alerts and thresholds to monitor performance

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: [*listed in Table 13*].

Table 13 TSF Management Capabilities

Function
Assign permissions to users
Change account passwords
Create and delete accounts
Discover arrays
Manage arrays
Release array locks
Set access controls
Set alerts and thresholds to monitor performance
Set replication and reservation preferences
Show and add license keys

Function
View audit log
View settings (e.g., audit log and access control definitions)

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, Monitor, PerfMonitor, None*[31]].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.

[31] The "None" role has no permissions and can be used to effectively place an account on hold without deleting the account entirely. The account can later be reactivated by assigning a role having permissions.

6.2.5 Class FPT: Protection of the TSF

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 timestamps **for its own use**.

6.2.6 Class FTA: TOE Access

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 **Authorized Administrator-specified** advisory **notice and consent** warning message regarding ~~unauthorized~~ use of the TOE.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 14 summarizes the requirements.

Table 14 Assurance Requirements

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

7 TOE Security Specification

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

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each TSF is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the TSFs and their associated SFRs.

Table 15 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1a	Subset residual information protection
	FDP_RIP.1b	Subset residual information protection
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps
TOE Access	FTA_TAB.1	TOE access banner

7.1.1 Security Audit

The TOE generates an audit log for administrative control operations performed via Unisphere and Solutions Enabler, including:

- Modifying user roles and authorization levels
- Adding/removing masking views
- Adding/removing storage groups, port groups, and/or initiator groups

The TOE audit records contain the following information:

Table 16 Audit Record Contents

Field	Content
Record Number	An integer that starts at 1 and is incremented by 1 for each new audit log record generated.
Time	Time the audit record was created in MM/DD/YY HH:MM:SS format.
Vendor ID	The vendor ID (e.g., "EMC Corp.")
Application ID	Which application triggered the log entry.
Host Name	The network name of the host generating the record. This name is unique for each host and thus allows host identification.
Client Host	If the hostname is a server acting on behalf of a client system, then the name of the client system is placed in this field. Values for this field are generated as are the hostname values.
Function Class	Class, or major functional area, of action being performed.
Action Code	Subordinate action in a Function Class being performed. The kinds of actions include: • Successful connection • Failed connection • Loss of connection • Reboot • File transfer • Configuration change • Installation • Uninstallation of tokens
Text	Free-form text description of action being performed.
Username	The name of the logged-in user responsible for issuing the command that triggered the record.
Activity ID	A randomly generated label used to identify each user session.

Audit events caused by a user of the TOE will be recorded with the associated username. Audit records can be viewed through Unisphere or through the Solutions Enabler CLI. In Unisphere, administrators can select the audit log page through a tab menu along the top of the screen.

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

7.1.2 User Data Protection

The TOE enforces a Block Storage Access Control Policy on devices trying to read to or write from the storage that the TOE provides. Access via the Block Storage Access Control Policy is based on an initiator group, port group, storage group, device WWN, and masking view:

- Initiator groups uniquely identify the devices that connect to logical disks on a SAN via the specified ports.
- Port groups specify physical ports to which the TOE connects directly to devices or to a SAN.
- Storage groups specify logical disks within the TOE to which a device may be assigned.
- Device WWNs uniquely identify the storage device

Masking views are constructs created when an initiator group, port group, and storage group are associated with one another. A masking operation creates this association. Masking views allow a set of devices access to a group of logical disks via front-end ports.

The TOE allows administrators to erase data on physical drives within the storage array. Administrators specify the erasure algorithm to use and the number of times to execute the algorithm, which destroys all residual information on the specified disk after it is deallocated from the storage array at the request of the administrator.

The TOE performs iVTOC functionality on logical disks and partitions within the storage array. Administrators specify which logical disks and partitions should be formatted. The formatting process replaces all of the data on the disk or partition with zeroes, removing any residual data that previously resided on the disk.

Note that the data erasure functions for both physical and logical disks are not run automatically. Administrators must execute these features prior to a physical or logical disk being removed or deallocated from a storage pool/array.

The TOE protects stored user data from unintentional corruption through the use of RAID groups. RAID groups provide mirroring and striping of data. Mirroring creates an exact copy of all of the data on a disk, so that in the event that some of the data becomes corrupted or becomes inaccessible (e.g., because of a disk failure), the RAID can discover the error and replace it with the correct data. Parity calculates a code from the actual data present on the disks, then distributes the parity data so that it exists on a separate drives than the drives containing the information it was calculated from. If an error occurs in a parity-based RAID group, the data can be rebuilt from the parity information stored on the other disks.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_RIP.1a, FDP_RIP.1b, FDP_SDI.2.

7.1.3 Identification and Authentication

TOE user accounts can be created during the installation and setup of Unisphere and during regular operation by an authorized TOE user with the Administrator or SecurityAdmin role. When creating a TOE user, the administrator provides the user with an identity, a password, and from one to four roles. User accounts can also be deleted by a TOE user with the Administrator or SecurityAdmin role.

Unisphere requires users to identify themselves and to be authenticated before the TOE performs any actions on their behalf. Unisphere users enter a username and password pair at the Unisphere login screen and invoke the Login button. Password feedback is obscured while entering the username and password pair.

SYMCLI identifies users against a mapping of roles to user and Solutions Enabler Host identities of the underlying operating system. Solutions Enabler stores and maintains this mapping as a table on the VMAX array. Users must successfully identify themselves before SYMCLI allows them to view any TOE data or perform any actions on the TOE. Access controls and user authorization must be enabled (as required by the evaluated configuration) for user and host authorization to occur via the CLI. Access controls and user authorization do not provide any kind of authentication of users and hosts, only identification.

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

7.1.4 Security Management

The TOE provides two management interfaces for administrators: Solutions Enabler as a CLI and Unisphere as a web GUI. Unisphere is accessed through a web browser on an administrative host and presents commands to users in the form of Hypertext Markup Language (HTML) elements (such as text boxes, hyperlinks, and drop-down lists). Solutions Enabler is customer software that must be installed on an administrative host. The Solutions Enabler interface uses well-defined text conventions to pass commands to the TOE.

The TOE provides seven user roles: Administrator, SecurityAdmin, StorageAdmin, Auditor, Monitor, PerfMonitor, and None. The None role is used to specifically deny management access to a user without deleting the account. Other roles have a predefined set of permissions to view or configure different parts of the TOE. Only the Administrator role has unlimited access to manage the TOE. Table 17 below details the permissions associated with each role in the TOE.

Table 17 Permissions by Role

Permission	Role						
	Administrator	Storage Admin	Perf Monitor	Monitor	Security Admin	Auditor	None
Create/delete user accounts	✓				✓		
Reset user password	✓				✓		
Assign roles	✓				✓ (self excluded)		
Change own password	✓	✓	✓	✓	✓	✓	✓
Manage storage systems	✓	✓					
Discover storage systems	✓				✓		
Add/show license keys	✓	✓					
Set alerts and Optimizer monitoring options	✓	✓					
Release storage system locks	✓	✓					

Permission	Role						
	Administrator	Storage Admin	Perf Monitor	Monitor	Security Admin	Auditor	None
Set Access Controls	✓	✓					
View Access Controls	✓	✓			✓	✓	
Set replication and reservation preferences	✓	✓					
View replication and reservation preferences	✓	✓			✓	✓	
View audit log	✓	✓			✓	✓	
Access performance data	✓	✓	✓	✓	✓	✓	
Start data traces	✓	✓	✓	✓	✓	✓	
Set performance thresholds/alerts	✓	✓	✓				
Create and manage performance dashboards	✓	✓	✓	✓	✓	✓	

TOE users are assigned from one to four roles. Only TOE users with the Administrator and StorageAdmin roles have the ability to manage the VMAX arrays. The Administrator and SecurityAdmin roles have the ability to assign roles to TOE users. Only the Administrator and SecurityAdmin roles have the ability to create and delete user accounts and reset user passwords. TOE users with the Monitor, Auditor, PerfMonitor, and None roles do not have the ability to manage TOE data.

Administrators can also manage security attributes associated with the Block Storage Access Control Policy. All administrative roles, except for the None role, have access rights to query, modify, and manage these attributes. The Block Storage Access Control Policy, by default, does not permit any devices to use the storage provided by the TOE.

An Administrator, StorageAdmin, or SecurityAdmin can set and modify access controls on specific logical disks within an array, which assigns those disks to a specific device. Once set, only that device can see those disks. Other devices connected to that array will not be able to see those disks. The same roles can set and modify preferences for replication monitoring, which provides visual tracking of replication operations, and for reservations, which allow devices to reserve logical disks for their use only. The Auditor role users can view these settings and access control settings but are unable to change them.

Audit logs are viewable by users with Administrator, StorageAdmin, SecurityAdmin, and Auditor status. Audit logs are not modifiable by any user.

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

7.1.5 Protection of the TSF

The performance of an auditable event requires that the specific time for the event be logged. This ensures accurate tracking of events that can occur milliseconds between one another. The generation of a timestamp associated with an auditable event is provided by internal TOE clocks.

TOE Security Functional Requirements Satisfied: FPT_STM.1

7.1.6 TOE Access

TOE Administrators can create and customize the access banner seen by all TOE users. An Administrator must create a login message following the instructions provided in the Unisphere documentation. When active, the access banner will be seen by all TOE users accessing the TOE via the Unisphere web GUI prior to being presented with the login screen.

TOE Security Functional Requirements Satisfied: FTA_TAB.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4. There are no extended SFRs or SARs contained within this ST.

There are no protection profile claims for this ST.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 18 below provides a mapping of the objects to the threats they counter.

Table 18 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION User data and configuration data could become corrupted due to hardware failure, unsafe environmental conditions, or incorrect system operations caused by malicious users outside of the controlled access facility where the TOE is housed.	O.PROTECT The TOE must protect configuration and user data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the configuration and user data that has been entrusted to the TOE.
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.	O.TOE_ADMINISTRATION counters this threat by allowing administrators to properly configure the mechanisms of the TOE that prevent data corruption and restrict access to authorized individuals.
	OE.FIREWALL The TOE Environment must ensure that the port designated for use by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.	OE.FIREWALL counters this threat by preventing unauthenticated use of Solutions Enabler by subjects outside of the controlled access facility where the TOE is housed.
	OE.MMCS The TOE Environment must ensure that no connections, either KVM or Ethernet, are made to the MMCS after system deployment, thereby preventing local or remote access to the	OE.MMCS counters this threat by ensuring no physical access to the MMCS. OE.MMCS ensures that no KVM or Ethernet connections are made to the MMCS after system deployment.

Threats	Objectives	Rationale
	MMCS.	
T.IMPROPER_SERVER A user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE, thus exposing configuration and user data to harm or to unauthorized access.	O.PROTECT The TOE must protect configuration and user data that it has been entrusted to protect.	O.PROTECT counters this threat by providing adequate mechanisms to give only authorized servers access to the appropriately authorized configuration data. O.PROTECT allows administrators to destroy residual user or configuration data that is contained within hard drives before they are removed from the storage array.
	OE.PROPER_NAME_ASSIGNMENT The TOE Environment must provide accurate unique server identifiers for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT counters this threat by ensuring that the unique server identifiers provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide untampered communications between systems connected to the SAN.	OE.SECURE COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are untampered for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.	O.TOE_ADMINISTRATION counters this threat by allowing administrators to properly configure the mechanisms of the TOE designed to control the Discretionary Access Control Policy and the Storage Access Control Policy.
	OE.SECURE_SERVERS The TOE Environment must ensure that application servers communicating with the TOE do not allow unauthorized users or attackers access to the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that only authorized users can access the TOE through servers connected to the TOE.
T.NO_AUDIT An attacker may perform security-relevant operations on the TOE without being held accountable for them.	O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and provide the means to store and review that data.	O.SYSTEM_MONITORING counters this threat by ensuring that an audit trail of management events and alerts on the TOE is preserved.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 19 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 19 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.CONNECTIVITY It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.	OE.CONNECT The TOE administrators will configure the IT Environment so that users can access data through a direct connection to the TOE, or so that zones are configured on the SAN that allow users to access data stored on the TOE.	OE.CONNECT upholds this assumption by ensuring that the IT Environment is configured appropriately to allow users to access information stored on the TOE.
A.FIREWALL It is assumed that the IT Environment must block all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE.	OE.FIREWALL The TOE Environment must ensure that the port designated for use by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.	OE.FIREWALL upholds this assumption by ensuring the necessary ports will be blocked from traffic coming from outside the controlled access facility.
A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	OE.PHYSICAL upholds this assumption by ensuring that physical security is provided for the TOE.
A.MANAGE It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	OE.MANAGE upholds this assumption by ensuring that those responsible for the TOE provide competent individuals to perform management of the security of the environment. These individuals restrict these functions and facilities from unauthorized use.
A.NOEVIL It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	OE.NOEVIL upholds this assumption by ensuring that administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.MMCS_PROTECT	OE.MMCS	OE.MMCS upholds this

Assumptions	Objectives	Rationale
it is assumed that no KVM or Ethernet connections will be made to the MMCS after deployment of the TOE, so that the MMCS cannot be used for local or remote access to the TOE.	The TOE Environment must ensure that no connections, either KVM or Ethernet, are made to the MMCS after system deployment, thereby preventing local or remote access to the MMCS.	assumption by ensuring that no KVM or Ethernet connections exist to the MMCS after system deployment.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 20 below shows a mapping of the objectives and the SFRs that support them.

Table 20 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.PROTECT The TOE must protect configuration and user data that it has been entrusted to protect.	FDP_ACC.1 Subset access control	This requirement supports O.PROTECT by enforcing an access control policy that ensures that only authorized devices gain access to user data within the TOE.
	FDP_ACF.1 Security attribute based access control	This requirement supports O.PROTECT by providing access control functionality to manage access to user data within the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FDP_RIP.1a Subset residual information protection	This requirement supports O.PROTECT by ensuring that residual data on the disks in the storage array is destroyed before they are removed from the storage array.
	FDP_RIP.1b Subset residual information protection	This requirement supports O.PROTECT by ensuring that residual data on the disks in the storage array is destroyed before they are reallocated for use after formatting.
	FDP_SDI.2 Stored data integrity monitoring and action	This requirement supports O.PROTECT by providing data integrity against unintentional corruption via the RAID options the TOE implements.
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and provide the means to store and review that data.	FAU_GEN.1 Audit Data Generation	This requirement supports O.SYSTEM_MONITORING by requiring the TOE to produce audit records for the system security events.
	FAU_GEN.2 User Identity Association	This requirement supports O.SYSTEM_MONITORING by requiring the TOE to associate a username with the auditable event.
	FAU_SAR.1 Audit review	This requirement supports O.SYSTEM_MONITORING by requiring the TOE to make the recorded audit records available for review.
	FPT_STM.1 Reliable Time Stamps	This requirement meets O.SYSTEM_MONITORING by producing a time stamp with each auditable event.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.	FIA_ATD.1 User attribute definition	This requirement supports O.TOE_ADMINISTRATION by ensuring each user is assigned a role.
	FIA_UAU.2 User authentication before any action	This requirement supports O.TOE_ADMINISTRATION by requiring Unisphere administrators to authenticate their claimed identities before the TOE will perform any actions on

Objective	Requirements Addressing the Objective	Rationale
		their behalf via Unisphere.
	FIA_UAU.7 Protected authentication feedback	This requirement supports O.TOE_ADMINISTRATION by ensuring a password cannot be seen by an unauthorized user. This prevents an unauthorized user from accessing the TOE.
	FIA_UID.2 User identification before any action	This requirement supports O.TOE_ADMINISTRATION by requiring administrators to identify themselves before the TOE will perform any actions on their behalf.
	FMT_MSA.1 Management of security attributes	This requirement supports O.TOE_ADMINISTRATION by specifying the security attributes of the TOE that can be modified and which administrators can modify them.
	FMT_MSA.3 Static attribute initialization	This requirement supports O.TOE_ADMINISTRATION by specifying that restrictive default values are used by the Block Storage Access Control Policy, and specifying which administrative roles can specify alternative values.
	FMT_MTD.1 Management of TSF Data (for general TSF data)	This requirement supports O.TOE_ADMINISTRATION by ensuring only authorized Administrators are able to manage and configure the TOE.
	FMT_SMF.1 Specification of management functions	This requirement supports O.TOE_ADMINISTRATION by specifying each of the management functions that are used to securely manage the TOE. These functions are provided by Solutions Enabler and Unisphere.
	FMT_SMR.1 Security roles	This requirement supports O.TOE_ADMINISTRATION by specifying the roles defined to govern management of the TOE.
	FTA_TAB.1 TOE access banner	This requirement meets O.TOE_ADMINISTRATION by warning the user that only

Objective	Requirements Addressing the Objective	Rationale
		authorized TOE Administrators are allowed to login to the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System has incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 21 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 21 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_RIP.1a	None	Not applicable	
FDP_RIP.1b	None	Not applicable	
FDP_SDI.2	None	Not applicable	
FIA_ATD.1	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is included and is hierarchical to FIA_UID.1.

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is included and is hierarchical to FIA_UAU.1.
FIA_UID.2	None	Not applicable	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is included and is hierarchical to FIA_UID.1.
FPT_STM.1	None	Not applicable	
FTA_TAB.1	None	Not applicable	

9 Acronyms and Terms

This section defines the acronyms and terms used throughout this document.

9.1 Acronyms

Table 22 Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DSA	Database Storage Analyzer
EAL	Evaluation Assurance Level
FE	Front End
Gb/s	Gigabit per second
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTML	Hypertext Markup Language
I/O	Input/Output
IT	Information Technology
KVM	Keyboard, Video, and Mouse
LCC	Link Control Card
MMCS	Management Module Control Station
NAS	Network Attached Storage
OS	Operating System
PP	Protection Profile
QOS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
REST	Representational State Transfer
SAN	Storage Area Network
SAR	Security Assurance Requirement

Acronym	Definition
SATA	Serial Advanced Technology Attachment
SE	Single Engine
SFP	Security Functional Policy
SFR	Security Functional Requirement
SRDF	VMAX Remote Data Facility
ST	Security Target
SYMAPI	VMAX Application Programming Interface
SYMCLI	VMAX Command Line Interface
TOE	Target of Evaluation
TSF	TOE Security Functionality
WWN	World Wide Name

9.2 Terminology

Administrator – an individual who manages and configures the TOE. Also can be used as the "Administrator role" where indicated.

Data striping - The technique of segmenting logically sequential data, such as a file, so that consecutive segments are stored on different physical storage devices.

Device – The term "device" refers to any type of computing device that can attach to or access storage on a VMAX. Typical usage refers to application servers (e.g., a web server or file server), and mainframes (i.e., computing devices used to house large databases).

Fabric – The hardware that connects devices to storage arrays in a SAN.

Failover – Failover is an operation that automatically switches data from a failed system to an operational system in the event that a system fails. In this case, "system" refers to the disks in the storage array.

Flash – Flash is a technology that uses a special type of transistor to isolate and hold an electrical charge long-term, thereby allowing non-volatile storage of electronic data without requiring moving parts.

Global Memory – Global memory is volatile memory that is shared by all of the components of the VMAX system (analogous to random access memory in a desktop computer).

LCC – LCCs provide several services for disk drives, including data connectivity, environmental monitoring, failover control, drive detection, and other functions related to drive control and reliability.

NAS – A system that provides storage to devices on a network.

Pool – A group of one or more logical disks.

RAID – A technology that copies redundant data across an array of disks. This technique preserves data stored in a RAID in case one or more (depending on RAID type) of the drives in a RAID fails.

Raw – The term "raw" refers to the total storage capacity offered by the disks within VMAX. After users apply RAID and the VMAX claims a small portion of the space for its own use, the drives will offer less total storage capacity.

SAN – A network architecture that allows remote storage to appear local to devices accessing that storage.

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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