

EMC® Corporation

EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™

Security Target

Evaluation Assurance Level (EAL): EAL3+
Document Version: 0.8



Prepared for:



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

Phone: +1 508 435 1000
<http://www.emc.com>

Prepared by:



Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 703 267 6050
<http://www.corsec.com>

Table of Contents

1	INTRODUCTION	4
1.1	PURPOSE	4
1.2	SECURITY TARGET AND TOE REFERENCES	4
1.3	PRODUCT OVERVIEW	5
1.4	TOE OVERVIEW	7
1.4.1	<i>Brief Description of the Components of the TOE</i>	10
1.4.2	<i>TOE Environment</i>	11
1.5	TOE DESCRIPTION.....	11
1.5.1	<i>Physical Scope</i>	11
1.5.2	<i>Logical Scope</i>	13
1.5.3	<i>Product Physical/Logical Features and Functionality not included in the TOE</i>	14
2	CONFORMANCE CLAIMS	15
3	SECURITY PROBLEM	16
3.1	THREATS TO SECURITY.....	16
3.2	ORGANIZATIONAL SECURITY POLICIES	17
3.3	ASSUMPTIONS.....	17
4	SECURITY OBJECTIVES.....	18
4.1	SECURITY OBJECTIVES FOR THE TOE.....	18
4.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT.....	18
4.2.1	<i>IT Security Objectives</i>	18
4.2.2	<i>Non-IT Security Objectives</i>	19
5	EXTENDED COMPONENTS	20
6	SECURITY REQUIREMENTS	21
6.1.1	<i>Conventions</i>	21
6.2	SECURITY FUNCTIONAL REQUIREMENTS	21
6.2.1	<i>Class FAU: Security Audit</i>	23
6.2.2	<i>Class FDP: User Data Protection</i>	24
6.2.3	<i>Class FIA: Identification and Authentication</i>	27
6.2.4	<i>Class FMT: Security Management</i>	28
6.3	SECURITY ASSURANCE REQUIREMENTS.....	31
7	TOE SPECIFICATION.....	32
7.1	TOE SECURITY FUNCTIONS.....	32
7.1.1	<i>Security Audit</i>	33
7.1.2	<i>User Data Protection</i>	33
7.1.3	<i>Identification and Authentication</i>	34
7.1.4	<i>Security Management</i>	35
8	RATIONALE.....	36
8.1	CONFORMANCE CLAIMS RATIONALE	36
8.2	SECURITY OBJECTIVES RATIONALE	36
8.2.1	<i>Security Objectives Rationale Relating to Threats</i>	36
8.2.2	<i>Security Objectives Rationale Relating to Policies</i>	39
8.2.3	<i>Security Objectives Rationale Relating to Assumptions</i>	39
8.3	RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS	41
8.4	RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS.....	41
8.5	SECURITY REQUIREMENTS RATIONALE	41
8.5.1	<i>Rationale for Security Functional Requirements of the TOE Objectives</i>	41
8.5.2	<i>Security Assurance Requirements Rationale</i>	43

8.5.3	Rationale for Refinements of Security Functional Requirements.....	44
8.5.4	Dependency Rationale.....	44
9	ACRONYMS AND TERMS.....	47
9.1	ACRONYMS.....	47

Table of Figures

FIGURE 1 – DEPLOYMENT CONFIGURATION OF THE TOE.....	9
FIGURE 2 – PHYSICAL TOE BOUNDARY.....	12

List of Tables

TABLE 1 – ST AND TOE REFERENCES.....	4
TABLE 2 – CC AND PP CONFORMANCE.....	15
TABLE 3 – THREATS.....	16
TABLE 4 – ASSUMPTIONS.....	17
TABLE 5 – SECURITY OBJECTIVES FOR THE TOE.....	18
TABLE 6 – IT SECURITY OBJECTIVES.....	18
TABLE 7 – NON-IT SECURITY OBJECTIVES.....	19
TABLE 8 – TOE SECURITY FUNCTIONAL REQUIREMENTS.....	21
TABLE 9 – AUTHORIZED ROLES.....	29
TABLE 10 – ASSURANCE REQUIREMENTS.....	31
TABLE 11 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS.....	32
TABLE 12 – THREATS:OBJECTIVES MAPPING.....	36
TABLE 13 – ASSUMPTIONS:OBJECTIVES MAPPING.....	39
TABLE 14 – OBJECTIVES:SFRs MAPPING.....	41
TABLE 15 – FUNCTIONAL REQUIREMENTS DEPENDENCIES.....	44
TABLE 16 – ACRONYMS AND TERMS.....	47



Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™, and will hereafter be referred to as the TOE, or VNX OE/Unisphere. The TOE is a combination File (NAS¹) and Block (SAN²) operating environment with Unified Management (Unisphere). The TOE provides access controls for internal storage provided by the TOE hardware. Internal storage is accessed via NAS on a Local Area Network³ and traditional SAN based protocols.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST 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 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 – ST and TOE References

ST Title	
	EMC® Corporation EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ Security Target

¹ NAS – Network Attached Storage

² SAN – Storage Attached Network. A SAN is a network where the main feature is to provide dedicated or shared storage to devices connected to the SAN.

³ LAN – Local Area Network

ST Title	EMC® Corporation EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ Security Target
ST Version	Version 0.8
ST Author	Corsec Security, Inc.
ST Publication Date	2011-05-27
TOE Reference	EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ VNX OE for Block v05.31.000.5.006 and VNX OE for File v7.0.12.0 Unisphere v7.0.12.0 and Control Station v05.31.000.5.006
Keywords	VNX, Storage Area Network, SAN, storage array, data storage, Unisphere, Network Attached Storage, NAS

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ can be divided into three main components. VNX OE is the software portion of the product responsible for access controls and management of storage. Unisphere is the management software that allows administrators to maintain and configure the product. VNX is the hardware portion of the product. Together, these components provide Block and File access to internal storage for external entities:

1. Block: controls access to internal storage for devices on a SAN. These access controls allow administrators to determine which devices on a SAN have access to VNX storage, and also which areas of storage (disks or portions of disks) are available to each device. Storage is provided over Fiber Channel (FC) and Internet Small Computer Systems Interface (iSCSI).
2. File: controls access to internal storage for devices on a LAN. While Block mode requires devices to access storage from a SAN using SAN-specific communications, VNX also provides NAS that allows traditional IP⁴-based devices to access internal storage over a LAN. NAS storage is provided over Network File System (NFS⁵), Common Internet File System (CIFS⁶), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP).

⁴ IP – Internet Protocol

⁵ NFS is a platform-independent file sharing system commonly used by UNIX and UNIX variants for file sharing. NFS versions 2, 3, and 4.

⁶ CIFS is a platform-independent file sharing system commonly used by Microsoft Windows network file sharing.

Unisphere is a unified management suite presented through a Graphical User Interface (GUI) that allows administrators to configure the majority of VNX functionality from a single management console. In addition to Unisphere, VNX provides a CLI called Navisecli and a second CLI available on the Control Station. Navisecli provides a subset of the functionality available via the Unisphere GUI, while Control Station provides necessary functionality to configure File mode properties. Administrators can create shell scripts and batch files for CLI commands to automate management tasks. The Control Station CLI provides a Secure Shell (SSH) interface that administrators can use for File-specific configuration management activities. The product includes an SSH server to provide this functionality.

VNX OE/Unisphere administrators can provision (make available) internal storage to devices on a LAN and devices on a SAN. Once storage has been provisioned to LAN users, it is no longer available to SAN users, and storage provisioned to SAN users is no longer available to LAN users. Storage can be re-provisioned as needed to suit the needs of users.

In File mode, VNX presents itself as one or more standard network-based file servers to client machines on a LAN. In Block mode, VNX presents itself as a series of block storage devices to client machines on a SAN. Administrators manage VNX and control the policies that govern access to storage with the Unisphere GUI and Navisecli. Administrators may also have to use the Control Station CLI to manage the File portion of VNX.

The product can run in Block mode, File mode, or Unified Block and File mode of operation. Block mode allows the product to provide only traditional SAN-based access and access controls to internal storage for devices on the SAN. File mode allows the product to control only LAN access to internal storage. Unified Block and File mode is a combination of the above two modes, allowing the product to provide and control access to internal storage from both typical SAN and LAN devices. Unisphere runs on the VNX hardware in the Unified Block and File mode of operation⁷.

VNX/Unisphere allows an organization to manage its storage needs separately from its application and file servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers. In a typical deployment scenario for VNX/Unisphere, individual client machines are attached to a SAN through a Fibre Channel⁸ or iSCSI switch. Client machines also connect to VNX/Unisphere over an IP-based LAN through standard networking equipment (IP routers and switches as needed). These client machines are then configured to use storage on VNX—in the form of Logical Units or file servers—for their applications.

VNX OE implements a Storage Operating Environment (SOE), which provides RAID⁹ and storage provisioning capabilities. The product provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to stored data. The product is designed to allow customers to scale both system performance and storage capacity.

Hardware/software components called Data Movers¹⁰ implement the NAS functionality. Data Movers are the VNX file-side components that perform the actual transfer of data between the internal storage and LAN clients. Each Data Mover provided by VNX can host one or more file servers that present shared services to client machines on a LAN.

⁷ Unified Block and File mode is the evaluated configuration.

⁸ Fibre Channel is a serial data transfer interface that operates over copper wire and/or optical fiber at connection speeds currently supported up to 4 GB/s or 8 GB/s.

⁹ RAID – Redundant Array of Independent Disks

¹⁰ Data Movers are also called X-Blades and the two terms are used interchangeably throughout the product's documentation.

Administrators can configure the type of server and protocols that are supported by that server per Data Mover. Client machines on the LAN, with the appropriate access privileges, can then use file-side VNX to store and access data as they would any other network-based file server. Additionally, shared file systems can be configured for FTP or TFTP access.

VNX is responsible for enforcing all access permissions for user data. In File mode, each file server on VNX can be configured to interface with a Microsoft Active Directory server or utilize local user authentication files. When a request for data access is made from an IP-based client machine, VNX utilizes the appropriate authentication mechanism, checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the Data Mover User. User data can be stored directly on storage provided by VNX.

The VNX hardware includes internal storage (disk arrays). This internal storage is configured to provide a storage system where VNX users can store data. The block storage portion of VNX's SOE allows this storage system to store and retrieve block units of data for VNX users on a SAN. Each of these block units is associated with a Logical Unit, which is in turn associated with a Logical Unit Number (LUN). Individual elements of the storage system are presented to VNX as Logical Units. Each Logical Unit is a useable storage system volume that VNX can use to store user data.

EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ runs on the C-125, C-250, C-500, and C-1000 series of hardware appliances. The Unisphere and Navisecli software contain utilities for installing and configuring VNX, maintaining the system, and monitoring system performance. Unisphere uses a Java-capable web browser as its platform, navisecli runs on an administrator's management workstation, and Control Station hardware hosts CLI management software. The Data Mover operating system is referred to as DART (Data Access in Real Time). VNX can have from 1 to 8 Data Movers. There are several different models of Data Movers; however, use and management of all Data Movers is identical. VNX/Unisphere can be monitored by an EMC ControlCenter Agent Server to collect information on the health or status of the product.

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 software-only TOE is the EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™. The TOE is a combination File (NAS) and Block (SAN) operating environment with Unified Management (Unisphere). It includes an SOE, which provides RAID and storage provisioning capabilities, one or more NAS servers that allow LAN clients to connect and use internal storage, and a set of interfaces administrators can use to manage the TOE and access controls for internal storage.

The TOE is managed by authorized users through the Unisphere Manager, Navisecli, and Control Station CLI interfaces. Unisphere Manager is a Java-based applet that runs within a web browser. To access the functions available via Unisphere Manager, an authorized user must open a web browser and enter the IP address or hostname of the desired storage system Storage Processor (SP) or corresponding Control Station. Navisecli is a command line interface that provides access to common functions for monitoring and managing the TOE. The Secure CLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions.

In Block mode, the TOE software includes an SOE optimized for implementation of RAID storage architectures, providing fault detection, isolation, and diagnosis capabilities. It enables the use of logical storage elements (LUNs) to improve performance and capacity utilization. The TOE also implements a technology called Access Logix. Access Logix lets multiple hosts share a storage system by using Storage Groups. A Storage Group is one or more Logical Units within a storage system that are reserved for one or more hosts and is inaccessible to other hosts. Access Logix enforces the host-to-Storage Group permissions.

The TOE also performs event monitoring of system status and host registration of client machines. This is done through the TOE's SP Agent. The SP Agent collects information about the state of the system, including the operating environment, hardware components associated with the TOE, and the TOE's Logical Units, and reports this information to authorized TOE users. The SP Agents also communicate host registration information between the SP Agents and the client machines. These agents periodically retrieve volume-mapping information from the client machines and forward it to Unisphere Manager for display.

The TOE also provides NAS Services that allow hosts on a LAN to access file systems via one of the supported file-based protocols (CIFS, NFS, FTP, and TFTP). The TOE presents this storage as one or more file servers on the customer's network. Client systems that attempt to access the file systems must pass VNX access controls before the TOE allows the access to occur.

Figure 1 shows the details of the deployment configuration of the TOE:

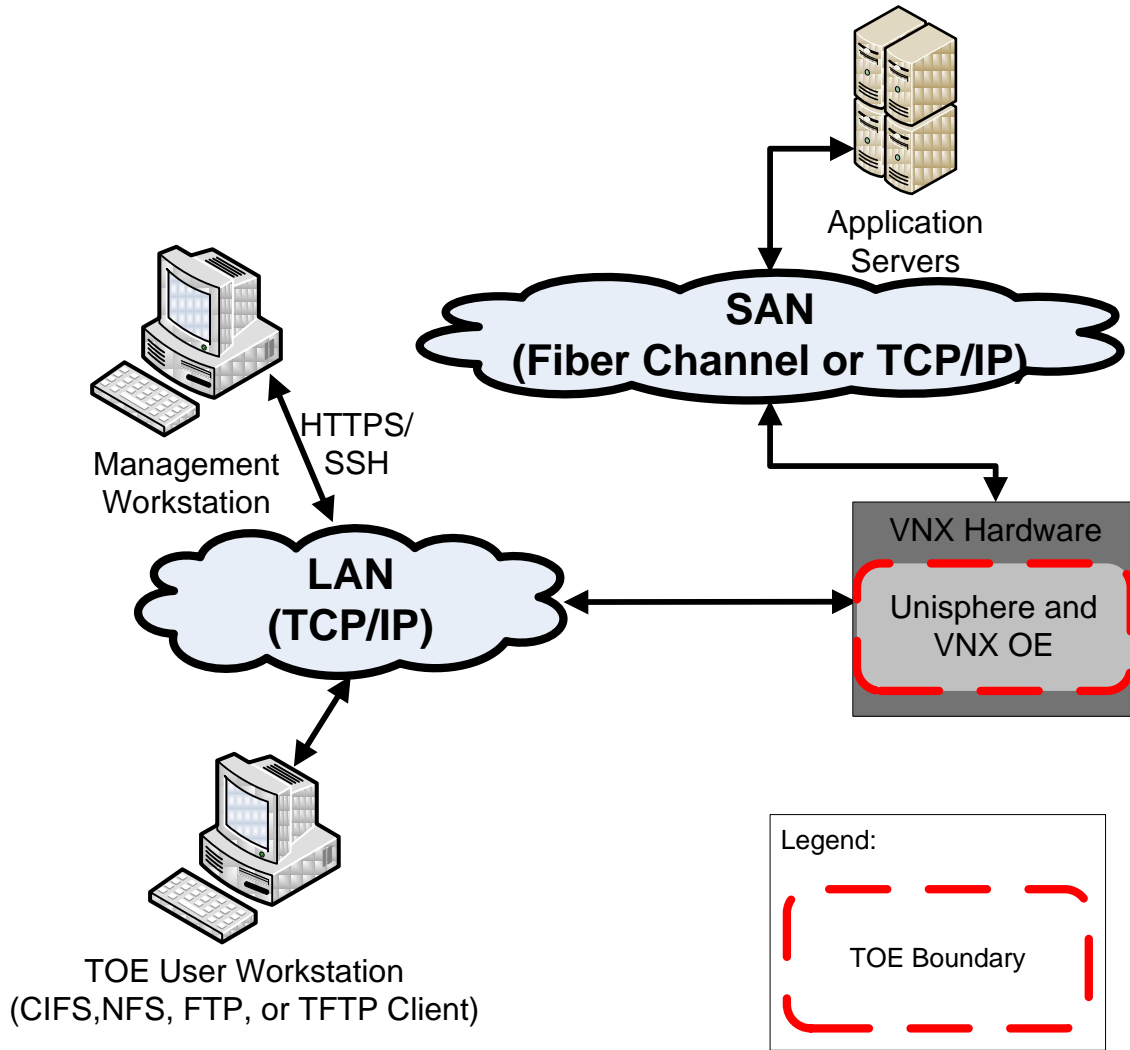


Figure 1 – Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The following sections describe the technologies and concepts related to the TOE.

1.4.1.1 Logical Units

The TOE works with storage entities called Logical Units. In Block mode, the TOE presents storage to client machines on the SAN in the form of Logical Units, and the TOE software provides for the management of Logical Units. Each Logical Unit represents a unit of storage to a client machine, analogous to a local disk drive. However, the Logical Unit provided by the TOE is not constrained to be a single individual disk. In fact, a typical deployment would have Logical Units that span multiple individual disks that are grouped into a RAID Group. Since IP-based client machines are presented storage as one or more file servers, Logical Units are not presented to IP-based clients.

1.4.1.2 File Servers

In File mode, the TOE presents storage to end users on a LAN through file server representations of that storage. File servers are hosted by the data movers. Each file server presents a portion of the internal storage to TOE users. TOE users access this storage as they would any NAS storage.

1.4.1.3 Storage Processors

The central component of the TOE in Block mode is the SP. The SP is responsible for interfacing with the SAN and with each of the individual disks within the VNX. There are two SPs in each TOE which logically operate as a single entity to provide increased performance and fault tolerance. The SP provides administrators with the ability to manage the TOE and establish Logical Units and RAID Groups.

1.4.1.4 RAID Groups

A RAID Group is a collection of individual disks. The TOE supports a variety of disk types and capacities (chosen by the customer when the product is purchased). In a RAID Group, disks of a similar type are typically grouped together. This RAID Group can then be configured by an administrator with various attributes, such as which RAID level to provide. In this manner, an administrator can manage the TOE through successive levels of abstraction.

1.4.1.5 Storage Groups

The TOE manages access to Logical Units through a component of the SP called Access Logix. Access Logix allows an administrator to group Logical Units together in a Storage Group. Each Storage Group can then be mapped to one or more client machines, identified by their Fibre Channel World Wide Name¹¹ (WWN) or iSCSI Qualified Name¹² (IQN). When this mechanism is used, a client machine can only access Logical Units that are present in a Storage Group that the client machine has been permitted to access.

It is also possible that multiple client machines are given access to the same Storage Group. This is used in cases where the client machine has been deployed in such a way as to manage multiple servers accessing the same Logical Unit, for example, in a clustered environment.

1.4.1.6 Management Software

Unisphere is the Java GUI used to manage the TOE. Administrators log into Unisphere in order to manage the TOE or the policies that control user access to storage. Management functionality is presented in the form of multiple screens that contain graphical elements, such as fields, buttons, and boxes. Unisphere also provides utilities to maintain and install the TOE. In addition to Unisphere, the TOE provides two CLIs

¹¹ A World Wide Name is a unique identifier in a Fibre Channel.

¹² An iSCSI Qualified Name is a unique identifier in a Serial Attached SCSI storage network.

that administrators can use to manage the TOE. Naviseccli contains a subset of the Unisphere functionality, while Control Station CLI provides management functionality specific to File mode operations.

1.4.1.7 Data Movers

Hardware/software components called Data Movers implement NAS functionality. Data Movers transfer data between the internal storage and LAN clients. Each Data Mover can host one or more file servers that present shared services to client machines on a LAN.

1.4.2 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a SAN with the constituent servers managed by administrators operating under a consistent security policy with the administrators that manage the TOE.

The TOE provides access control to individual Logical Units through its Access Logix component. For this to operate correctly, the WWN that is provided to the TOE must be accurate and must not be spoofed. The TOE Environment is required to provide this.

The TOE relies on secure access provided by the LAN and SAN to which it is attached. The purpose of the TOE is to mediate access to user data for client machines connected to an IP network or SAN. This functionality requires that the communications paths to the LAN and SAN be managed properly.

In a deployment where NFS is used, the NFSv2 and v3 servers are responsible for authenticating users. CIFS, NFSv4, and FTP provide for authentication to be carried out by the file server against the data store configured by TOE administrators, which may be an external Active Directory server.

The TOE must be run on custom-built VNX hardware to perform its intended function as a storage appliance.

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

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

- Unisphere and Control Station management software,
- Data Mover software, and
- Storage Operating Environment software.

The essential components of the TOE Environment are:

- VNX, Data Mover, and storage hardware in the environment,
- Management workstation,
- .Application servers and LAN users to use the storage services provided by the TOE,
- cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other

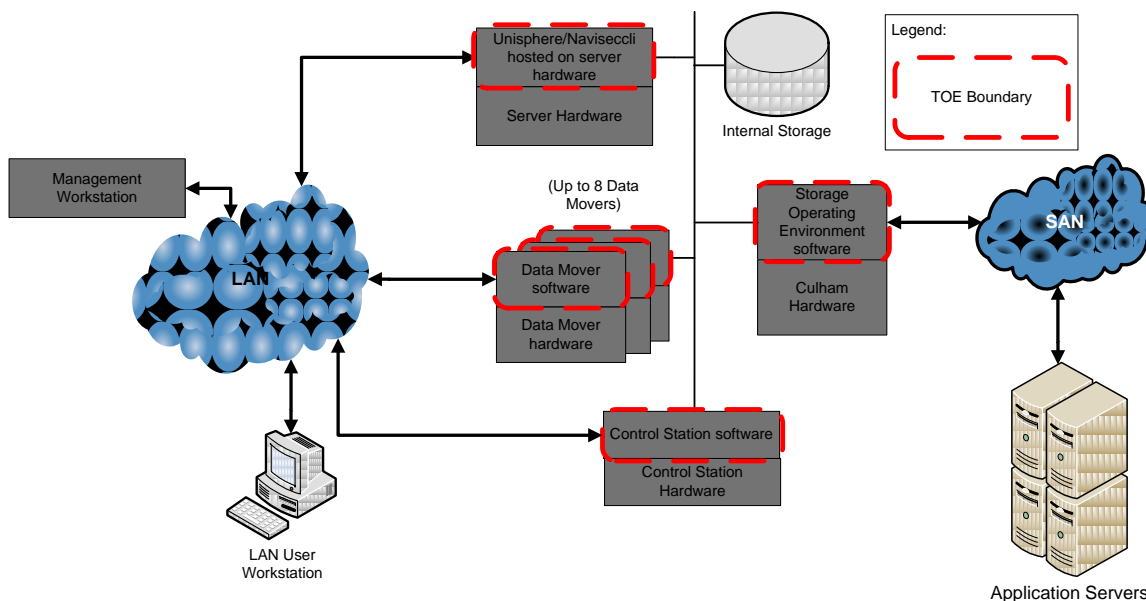


Figure 2 – Physical TOE Boundary

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

1.5.1.1 TOE Software

The TOE is a software-only TOE meant to be used with custom hardware. EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ runs on the VNX5100, VNX5300, VNX5500, VNX5700, and VNX7500 series of hardware appliances. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Unisphere/Navisecli/Control Station – unified management software used to manage the TOE
- Data Mover software – 1 to 8 Data Movers are present in the TOE to facilitate File access to internal storage
- Storage Operating Environment software – used to control and optimize access to storage

Each Data Mover is used to mediate access to storage provided by a SAN to client machines that are connected via an IP network.

1.5.1.2 Guidance Documentation

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

- EMC Setting up a Unisphere Management Station for the VNX Series P/N 300-011-796 Rev. A01
- EMC VNX Getting Started with VNX Installation Assistant for File/Unified P/N 300-011-839 Rev. A01
- EMC VNX for Block Command Line Interface Reference P/N 300-011-815 Rev. A01
- EMC VNX Series Command Line Interface Reference for File P/N 300-011-841 Rev. A01
- EMC VNX Security Configuration Guide on VNX for File P/N 300-011-803 Rev. A01
- EMC VNX Unisphere Online Help.html

1.5.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

1.5.2.1 Security Audit

The TOE generates audit records for all administrator actions that result in a configuration change and all login attempts. Authorized administrators can view, sort, and filter the audit records.

1.5.2.2 User Data Protection

The User Data Protection function implements functionality necessary to protect user data which is entrusted to the TOE. In File mode, this functionality is primarily enforced by each of the Data Movers in the TOE. Users of the TOE are identified and authenticated, either by the TOE or the TOE Environment. These Data Mover users are then granted access to files and directories managed by the TOE. Each file and directory has an Access Control List (ACL) that contains the access privileges for Data Mover users of the TOE to that object.

In Block mode, Storage Processors govern access to storage by using Storage Groups. Individual devices on the SAN are assigned to storage groups, which allows them to access storage provided by the TOE. If a device is not a member of a storage group that grants access to a particular set of storage, then that device is not able to access that storage.

The TOE protects user data primarily in two additional ways. First, it ensures that only the client machines that have been granted access to a LUN have access to that LUN. Second, it ensures the integrity of the data entrusted to it through its use of RAID levels.

1.5.2.3 Identification and Authentication

This function of the TOE is used to identify and authenticate each operator of the TOE. In the case of Unisphere Administrators, the TOE provides username and password verification functionality. Data Mover Users of the TOE can be authenticated directly by the TOE or can be authenticated by a separate, external Active Directory, Kerberos, or NFS¹³ server in the TOE environment (Active Directory, Kerberos, and NFS authentication are not being evaluated). Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage. This functionality is configured by an Administrator.

1.5.2.4 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Function (TSF). Proper management of the TSF is required to properly mediate access to user data.

The TOE is managed by authorized users through the Unisphere Manager, Navisecli, and Control Station CLI. Unisphere Manager is a Java applet that runs within a web browser. Navisecli is a command line interface that provides access to common functions for monitoring and managing the TOE. The Control Station CLI contains management functionality specific to the File-side features of the TOE.

¹³ Kerberos and NFS authentication are only available for File-side clients.

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store user data. Administrators are assigned a role that governs what aspects of the TOE they are authorized to manage. Configuration of RAID settings, Storage Group membership, and administrator access is all supported through this security function.

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:

- VNX storage appliance hardware
- Remotely Anywhere
- Unisphere Analyzer
- Unisphere SnapView
- Unisphere MirrorView/Asynchronous
- Unisphere MirrorView/Synchronous
- Unisphere SAN Copy
- Unisphere Quality of Service Manager (UQM)
- iSCSI functionality
- Access Control Levels for Unisphere Administrators
- Multi-Path File System
- Replication Technologies
- VNX FileMover

The TOE supports several File System Access Policies. For the purposes of this evaluation, only the “MIXED” Access Policy is to be evaluated. The “NATIVE”, “NT”, “UNIX”, “SECURE”, and “MIXED_COMPAT” Policies are excluded from the evaluation.



Conformance Claims

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

Table 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2010/08/27 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3+ augmented with Flaw Remediation (ALC_FLR.2)



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 IT¹⁴ assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two 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.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF¹⁵ and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 3 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.
T.IMPROPER_SERVER	A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.
T.IMPROPER_CONFIG	The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.
T.MEDIATE_ACCESS	Access to user data could be improperly granted by an administrator to users who should not have access to it.
T.UNAUTH	An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.

¹⁴ IT – Information Technology

¹⁵ TSF – TOE Security Functionality

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

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

Table 4 – Assumptions

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	Physical security will be provided for the TOE and its environment.
A.PROTECT	The IT Environment shall provide a secure place to store user data of which access to that data will be mediated by the TOE.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.I&A	The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of those users.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_REVIEW	The TOE must provide authorized administrators with the ability to review the audit trail.
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.
O.BYPASS	The TOE must ensure that the TSF cannot be bypassed.
O.I&A	The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

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

Table 6 – IT Security Objectives

Name	Description
OE.I&A	The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.
OE.SECURE_COMMUNICATIONS	The TOE Environment must provide secure communications between systems connected to the Storage Area Network.
OE.SECURE_SERVERS	The TOE Environment must provide properly configured

Name	Description
	authentication servers and client machines to communicate with the TOE.
OE.TIME	The TOE environment must provide reliable time stamps to the TOE.
OE.PROPER_NAME_ASSIGNMENT	The TOE Environment must provide accurate World Wide Names for each system that communicates with the TOE.

4.2.2 Non-IT Security Objectives

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

Table 7 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.
NOE.PROTECT	The TOE Environment must protect the data it has been entrusted to protect.



Extended Components

There are no extended SFRs and extended SARs for this evaluation of the TOE.



Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 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: ~~TSE Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using “EXT_” at the beginning of the short name.
- Iterations are identified by appending a letter 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 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_ACC.1a	Subset access control		✓		✓
FDP_ACC.1b	Subset access control		✓		✓
FDP_ACF.1a	Security attribute based access control		✓	✓	✓
FDP_ACF.1b	Security attribute based access control		✓		✓
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MSA.1a	Management of security attributes	✓	✓		✓
FMT_MSA.1b	Management of security attributes	✓	✓		✓

Name	Description	S	A	R	I
FMT_MSA.3a	Static attribute initialisation	✓	✓		✓
FMT_MSA.3b	Static attribute initialisation	✓	✓		✓
FMT_MTD.1a	Management of TSF data	✓	✓		✓
FMT_MTD.1b	Management of TSF data	✓	✓		✓
FMT_MTD.1c	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

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.

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) *[all administrator actions that result in a configuration change to the storage array, all administrator login attempts].*

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].*

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide *[authorised administrators]* with the capability to read *[all audit information]* from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FDP: User Data Protection

FDP_ACC.1a Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*¹⁶] on
 [
 a) *Subjects: Application servers*
 b) *Objects: LUNs*
 c) *Operations: Read and write*
].

Application note: the Subjects are client machines connected to the SAN acting on behalf of an authorized user.

Dependencies: FDP_ACF.1a Security attribute based access control

FDP_ACF.1a Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*] to objects based on the following:
 [
 Subject attributes:
 1. *World Wide Name*
 2. *Storage Group Membership*
 Object Attributes:
 1. *Lun ID*¹⁷
 2. *Storage Group Membership*
].

FDP_ACF.1.2a

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
 [
 A valid subject of the TOE is allowed to read and write to a LUN if the subject and the LUN are members of the same storage group
].

FDP_ACF.1.3a

The TSF shall explicitly authorise access of subjects to objects based on ~~the following no~~ additional rules: [~~assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects~~].

FDP_ACF.1.4a

The TSF shall explicitly deny access of subjects to objects based on **no additional rules** ~~the~~ [~~assignment: rules, based on security attributes, that explicitly deny access of subjects to objects~~].

Dependencies: FDP_ACC.1a Subset access control
FMT_MSA.3a Static attribute initialization

FDP_ACC.1b Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1b

¹⁶ SFP – Security Functional Policy

¹⁷ ID – Identifier

The TSF shall enforce the [File and Directory Access SFP] on

[

- a) *Subjects: CIFS, NFS, FTP, and TFTP Users*
- b) *Objects: Files and Directories*
- c) *Operations: Create, Read, Write, Append, Execute, Delete, Change Ownership, Read Permissions, Change Permissions, Read Attributes, Write Attributes, Read Extended Attributes, and Write Extended Attributes*].

Dependencies: FDP_ACF.1b Security attribute based access control

Application Note: The CIFS naming convention has been used for operations. Equivalent operations are provided via NFS v4, but may be named slightly differently by NFS clients. FTP, NFS v2, and NFS v3 access supports a subset of these operations.

FDP_ACF.1b Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1b

The TSF shall enforce the [File and Directory Access SFP] to objects based on the following:

[

Subject attributes:

- 1. *UserID*
- 2. *GroupIDs*

Object attributes:

- 1. *UTF¹⁸-8 Filename*
- 2. *UTF-16 Filename*
- 3. *8.3 MS¹⁹-DOS²⁰ Filename*
- 4. *Access Control List*

].

FDP_ACF.1.2b

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [A valid subject of the TOE is allowed to perform an operation if the contents of the Access Control List for the object authorize the UserID or a GroupID of the Subject to perform the desired operation].

FDP_ACF.1.3b

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- 1. *For CIFS access, subjects that are members of the group Local Administrators shall be authorized to backup, restore, and take ownership of all objects*
- 2. *For NFS access, subjects that are authorized as superusers can perform all operations on all objects*

].

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the [A valid subject of the TOE is explicitly denies the ability to perform an operation if the contents of the Access Control List for the object explicitly deny the UserID or a GroupID of the Subject to perform the desired operation].

Dependencies: FDP_ACC.1b Subset access control
FMT_MSA.3b Static attribute initialization

¹⁸ UTF – Unicode Transformation Format

¹⁹ MS – Microsoft

²⁰ DOS – Disk Operating System

FDP_SDI.2 Stored data integrity monitoring and action**Hierarchical to: FDP_SDI.1 Stored data integrity monitoring****FDP_SDI.2.1**

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** objects, based on the following attributes: [*parity data for RAID 3, RAID 5, and RAID 6; mirrored data for RAID 1 and RAID 1+0*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data for RAID 3, RAID 5, and RAID 6; replace erroneous data with the mirrored data for RAID 1, and RAID 1+0; and notify an administrator*].

Dependencies: No dependencies

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:
[*UserID, one or more GroupIDs, and a password*].

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

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

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MSA.1a Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Storage Group Membership*] to [*the administrator, sanadmin, and storageadmin roles*].

Dependencies: FDP_ACC.1a Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1b Management; of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1b

The TSF shall enforce the [*File and Directory Access SFP*] to restrict the ability to [modify, delete, add] the security attributes [*UserID and GroupID assignment*] to [*authorized roles*].

Dependencies: FDP_ACC.1b Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3a Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1a

The TSF shall enforce the [*Discretionary Access control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a

The TSF shall allow the [*administrator, sanadmin, and storageadmin roles*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3b Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1b

The TSF shall enforce the [*File and Directory Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b

The TSF shall allow the [*Object Owner*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MTD.1a Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1a

The TSF shall restrict the ability to [query] the [*storage system information*] to [*all roles except securityadministrator*].

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

FMT_MTD.1b Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1b

The TSF shall restrict the ability to [query, modify, delete, [create]] the [*LUNs, RAID Groups, and Storage Groups*] to [*the administrator, sanadmin, and storageadmin roles*].

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

FMT_MTD.1c Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1c

The TSF shall restrict the ability to [query, modify, delete, [create]] the [*user accounts*] to [*the securityadministrator role*].

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

- [
- a) *Management of security functions behavior;*
- b) *Management of TSF data;*
- c) *Management of security attributes*
-].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorised roles identified in Table 9*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

Table 9 – Authorized Roles

Role	Description	GUI Name
operator	Read only for storage and domain information. No security, not even read.	Operator
networkadmin	DNS/IP settings for management path only. Routing/SNMP + Operator	Network Administrator
nasadmin	On File, NAS storage tasks only. Root role minus security. Operator on block.	NAS administrator
sanadmin	Block storage tasks only. Operator on File.	SAN administrator
storageadmin	nasadmin + sanadmin	Storage administrator
securityadministrator	Security and Domain tasks	Security administrator
administrator	Securityadministrator + storageadmin + networkadmin	Administrator

Role	Description	GUI Name
localdataprotection	Snap/Clone on Block. Checkpoints on File.	Local dataprotection
dataprotection	Localdataprotection + mirror on Block. Checkpoints on File	Dataprotection
datarecovery	On Block, localdataprotection + dataprotection. Additionally, recovery tasks, e.g. rollback. Replication Full Control and Checkpoints Full Control on File.	Datarecovery

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 EAL3 augmented with ALC_FLR.2. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – 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.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
	ATE_DPT.1 Testing basic design
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis



TOE Specification

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

7.1 TOE Security Functions

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

Table 11 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1a	Subset access control
	FDP_ACC.1b	Subset access control
	FDP_ACF.1a	Security attribute based access control
	FDP_ACF.1b	Security attribute based access control
	FDP_SDI.2	Stored data integrity
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1a	Management of security attributes
	FMT_MSA.1b	Management of security attributes
	FMT_MSA.3a	Static attribute initialisation
	FMT_MSA.3b	Static attribute initialisation
	FMT_MTD.1a	Management of TSF data
	FMT_MTD.1b	Management of TSF data
	FMT_MTD.1c	Management of TSF data
	FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles	

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit function, all administrator actions that result in a configuration change and all login attempts. Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event. Authorized administrators can view the audit records from the CLI or GUI. Audit records are presented to administrators in a clearly understandable format.

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

7.1.2 User Data Protection

This section describes the various User Data Protection SFRs claimed.

7.1.2.1 File and Directory Access SFP

The TOE enforces the File and Directory Access SFP²¹ on each Data Mover User of the TOE based on the security attributes of that user.

File and Directory Access SFP: The TOE enforces the File and Directory Access SFP on Data Mover Users by assigning access privileges to users based on their UserID and GroupIDs. The ability to perform operations on objects, which are governed by the File and Directory Access SFP, are granted to Data Mover Users by an object's owner. Thus, a Data Mover User is allowed to perform an operation on an object so long as permission is granted to the user within the object's ACL. A Data Mover User can also be denied the ability to perform an operation on an object if the contents of the object's ACL deny the desired operation based on the UserID or GroupID of the User.

Under the CIFS access protocol, Data Mover Users are allowed to backup, restore, and take ownership of all objects if they are member of the local Administrators group. For the NFS access protocol, Data Mover Users who are *superusers* can perform all operations on all objects.

The TOE is designed to mediate access to files and directories for authorized Data Mover Users. These files and directories are stored within internal storage. The TOE accesses the storage to provide Data Mover Users access to their data through several standard IP network file sharing mechanisms.

Identification and authentication of Data Mover Users is performed by the Identification and Authentication security function. Once a user has been successfully authenticated, the TOE is then in possession of the UserID and one or more GroupIDs for that User. These credentials are used to mediate access to files and directories.

Each file and directory managed by the TOE has an ACL associated with it. This ACL contains one or more Access Control Entries (ACEs). Each ACE contains a UserID or GroupID and a set of permissions that are granted or explicitly denied to that UserID or GroupID. Whenever a Data Mover User requests access to a file or directory, the TOE utilizes its File and Directory Access SFP to decide whether or not that access is permitted. The TOE uses the UserID and GroupIDs of the user and the contents of the ACL to determine if the operation should be allowed to proceed.

²¹ SFP – Security Functional Policy

7.1.2.2 Discretionary Access SFP

The TOE also provides the User Data Protection security function to manage access from client machines to configured Logical Units. The TOE provides this functionality for servers connected to the SAN.

Using the Security Management security function, Administrators of the TOE can configure Logical Units to provide storage to client machines. These Logical Units are then placed into Storage Groups, which allows an Administrator to limit access to each Logical Unit to one or more client machines. When a client machine requests a list of available Logical Units from the TOE, the TOE Environment provides a WWN. This WWN is used to identify the client machine to the TOE. The TOE then provides a list of Logical Units that the client machine has been granted access to. With each successive request to read or write information to or from a Logical Unit, the TOE ensures that only authorized client machines have access to the Logical Units to which they have been given access.

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure RAID levels 0, 1, 1+0, 3, 5, or 6. Each of these, except RAID level 0, provides fault tolerance for integrity errors or individual disk drive failure. The TOE provides mechanisms to check data integrity continuously while reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators can configure “hot spare” disk drives. These “hot spares” are used when a disk failure has been detected by the system. Once a failure has been detected, the drive that has been lost will be recreated on the “hot spare”. The Administrator can then replace the failed drive and configure it as a new “hot spare”. This process is provided while real-time access to user data continues.

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

7.1.3 Identification and Authentication

The TOE performs identification and authentication of both Administrators and Data Mover Users. The purpose of the identification and authentication function is to allow the TOE to restrict access to both administrative functions and to user data based upon the authenticated identity and associated attributes of a user.

7.1.3.1 Administrative I&A

Unisphere Administrators can access the TOE through a web browser or through a command line interface. The TOE supports internally enforced username and password-based authentication as well as authentication against an LDAP (Lightweight Directory Access Protocol) authentication server. The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE security functionality.

7.1.3.2 User I&A

Data Mover Users of the TOE are defined as those subjects that wish to use the TOE to store and mediate access to data. Data Mover Users of the TOE would typically not be Administrators (although they could be). The way identification and authentication works on the TOE for Data Mover Users is configurable by an Administrator. This security function provides the ability for the TOE to internally identify and authenticate users, and manage their attributes. The TOE can also utilize this functionality through its environment.

For CIFS and NFSv4 File user access, the TOE will identify and authenticate the username and password with each request for access. If configured for local administration of Data Mover Users, the TOE will

refer to its list of authorized users and groups. If the user can be authenticated, the function will allow the user access. Access to individual files and directories is then governed by the User Data Protection security function. If configured to use Active Directory or Kerberos (not included within the evaluation), the TOE will communicate with the respective external server in the TOE environment to authenticate the user and provide a list of groups that the user is a member of. The authentication result is then accepted by the TOE.

For NFSv2 and NFSv3 File user access, the external server from which the request is coming has already identified and authenticated each Data Mover User (although this is not part of the evaluated functionality). For this configuration, the TOE relies on its environment to perform proper identification and authentication. The TOE also relies on the environment to provide a list of GroupIDs that have been assigned to the user.

Identification and Authentication of client machines connecting to the TOE to access LUNs is provided by the TOE Environment through the proper assignment and use of WWNs.

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

7.1.4 Security Management

Unisphere Administrators are primarily responsible for managing and configuring system objects. This includes managing the use of LUNs provided by the storage system, grouping those LUNs into useful storage groups called Volumes, and creating and managing individual file systems on those Volumes. The Administrator also manages individual Data Movers, creates and manages file servers, and maps shares on those file servers to configured file systems. The Administrator is responsible for configuring the access control mechanisms to be supported by each file server.

The TOE provides mechanisms to govern which client machines can access which LUNs. The Security Management function allows Administrators to properly configure this functionality.

Administrators of the TOE are assigned one of the ten roles described in Table 9 above.

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

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 12 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.PROTECT The TOE must protect 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 data.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured	OE.SECURE_SERVERS counters this threat by ensuring that each server connected to the storage

Threats	Objectives	Rationale
	authentication servers and client machines to communicate with the TOE.	area network operates properly and does not intentionally compromise data.
	OE.PROPER_NAME_ASSIGNMENT The TOE Environment must provide accurate World Wide Names for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT counters this threat by ensuring that the World Wide Names provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
T.IMPROPER_CONFIG The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	O.BYPASS counters this threat by ensuring that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A counters this threat by ensuring that all authorized administrators are properly identified and authenticated.
T.MEDIATE_ACCESS Access to user data could be improperly granted by an administrator to users who should not have access to it.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	O.PROTECT The TOE must protect data that it	O.PROTECT counters this threat by providing mechanisms to

Threats	Objectives	Rationale
	has been entrusted to protect.	protect the data that has been entrusted to the TOE.
	<p>OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.</p>	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely.
	<p>O.BYPASS The TOE must ensure that the TSF cannot be bypassed.</p>	O.BYPASS counters this threat by ensuring that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	<p>O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.</p>	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE environment have properly identified and authenticated a user prior to providing access to user data.
<p>T.UNAUTH An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.</p>	<p>O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.</p>	O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	<p>O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.</p>	O.AUDIT_REVIEW counters this threat by ensuring that administrators can review the audited changes to the TOE configuration.
	<p>OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.</p>	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.
	<p>O.ADMIN The TOE must provide a method for administrative control of the TOE.</p>	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	<p>OE.SECURE_COMMUNICATIONS The TOE Environment must</p>	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and

Threats	Objectives	Rationale
	provide secure communications between systems connected to the Storage Area Network.	authentication performed by the TOE Environment is done over a secure communications channel.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely. Depending upon the access mechanism chosen, the TOE may depend upon these servers for identification and authentication of users.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	O.BYPASS counters this threat by ensuring that the protection mechanisms of the TOE cannot be bypassed.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.

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 OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 13 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent	NOE.MANAGE Sites deploying the TOE will	NOE.MANAGE upholds this assumption by ensuring that those

Assumptions	Objectives	Rationale
individuals assigned to manage the TOE and the security of the information it contains.	provide competent TOE administrators who will ensure the system is used securely.	responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL upholds this assumption by ensuring that administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL Physical security will be provided for the TOE and its environment.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information.
A.PROTECT The IT Environment shall provide a secure place to store user data of which access to that data will be mediated by the TOE.	NOE.PROTECT The TOE Environment must protect the data it has been entrusted to protect.	NOE.PROTECT upholds this assumption by ensuring that sites using the TOE will connect the TOE to a storage area network that provides data storage. This data storage should be configured and managed securely to allow the TOE to properly mediate access to user data.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable time stamps to the TOE.	OE.TIME upholds this assumption by ensuring that the environment provides reliable time stamps to the TOE.
A.I&A The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of those users.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	OE.I&A upholds this assumption by ensuring that the environment provides identification and authentication of client machine users.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 14 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security-related events, including relevant details about the event.
O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review the audit trail.
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UAU.2 User authentication before any action	This SFR supports O.ADMIN by ensuring that the TOE shall successfully authenticate each administrator before allowing management of the TOE.
	FIA_UID.2 User identification before any action	This SFR supports O.ADMIN by ensuring that the TOE will properly identify and authenticate all administrators.
	FMT_MSA.1a Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.1b Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of

Objective	Requirements Addressing the Objective	Rationale
		the TOE can only be changed by authorized administrators.
	FMT_MSA.3a Static attribute initialisation	This SFR supports O.ADMIN by ensuring that permissive values for data access are provided and the TOE administrator can change them when a data object is created.
	FMT_MSA.3b Static attribute initialisation	This SFR supports O.ADMIN by ensuring that restrictive values for data access are provided, and the Object Owner can change them when a data object is created.
	FMT_MTD.1a Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1b Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1c Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	This SFR supports O.ADMIN by ensuring that each of the management functions are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	This SFR supports O.ADMIN by ensuring that specific roles are defined to govern management of the TOE.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.1a Subset access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy that ensures that only authorized servers can gain access to data within the TOE.
	FDP_ACC.1b Subset access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data protected by the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1a Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data within the TOE.
	FDP_ACF.1b Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy which ensures that only authorized users gain access to data protected by the TOE.
	FDP_SDI.2 Stored data integrity	This SFR supports O.PROTECT by ensuring that the TOE protects the stored user data from integrity errors.
O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	FIA_ATD.1 User attribute definition	This SFR supports O.I&A by ensuring that the TOE, when configured for local user administration, maintains security attributes for each user.
	FIA_UAU.2 User authentication before any action	This SFR supports O.I&A by ensuring that the TOE authenticates each Administrator, and when configured for local user administration each user, prior to granting access to the TSF.
	FIA_UID.2 User identification before any action	This SFR supports O.I&A by ensuring that the TOE identifies each Administrator and when configured for local user administration, each user prior to granting access to the TSF>

8.5.2 Security Assurance Requirements Rationale

EAL3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3+, the TOE will have 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 Rationale for Refinements of Security Functional Requirements

The following refinements of SFRs from CC version 3.1 have been made to clarify the content of the SFRs, and make them easier to read:

The words “no additional rules” were added and others stricken, to FDP_ACF.1a.

The word “objects” was changed to “user data” to specify more precisely what is protected with FDP_SDI.2.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 15 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 15 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, the TOE Environment provides reliable timestamps to the TOE. An environmental objective states that the TOE will receive reliable timestamps, thereby satisfying this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1a	FDP_ACF.1a	✓	
FDP_ACC.1b	FDP_ACF.1b	✓	
FDP_ACF.1a	FDP_ACC.1a	✓	
	FMT_MSA.3a	✓	
FDP_ACF.1b	FDP_ACC.1b	✓	
	FMT_MSA.3b	✓	
FDP_SDI.2	None	Not applicable	
FIA_ATD.1	None	Not applicable	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.
FIA_UID.2	None	Not applicable	
FMT_MSA.1a	FDP_ACC.1a	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1b	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1b	✓	
FMT_MSA.3a	FMT_MSA.1a	✓	
	FMT_SMR.1	✓	
FMT_MSA.3b	FMT_MSA.1b	✓	
	FMT_SMR.1	✓	
FMT_MTD.1a	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1b	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1c	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.



Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 16 – Acronyms and Terms

Acronym	Definition
ACE	Access Control Entry
ACL	Access Control List
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
DART	Data Access in Real Time
DOS	Disk Operating System
EAL	Evaluation Assurance Level
FC	Fiber Channel
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
ID	Identifier
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit
MS	Microsoft
NAS	Network Attached Storage
NFS	Network File System
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks

Acronym	Definition
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SOE	Storage Operating Environment
SP	Storage Processor
SSH	Secure Shell
ST	Security Target
TSF	TOE Security Functionality
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UQM	Unisphere Quality of Service Manager
UTF	Unicode Transformation Format
WWN	World Wide Name

Prepared by:
Corsec Security, Inc.

The logo for Corsec, featuring the word "Corsec" in a bold, dark red serif font, centered within a white oval that has a subtle 3D effect with a grey shadow on the right side.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

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

