EMC Corporation
EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.2

Prepared for:

EMC Corporation
176 South Street
Hopkinton, MA 01748
Phone: (508) 435-1000

http://www.emc.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.2	2007-09-05	Nathan Lee	Final release.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems, and will be referred to as the TOE or the EMC CLARiiON FLARE/Navisphere throughout this document. The TOE is a storage operating environment/management software suite combination designed for CLARiiON storage arrays. CLARiiON storage arrays provide midrange Storage Area Network (SAN) storage.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish, or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE Security Functions (TSF) and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats 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.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE’s environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	EMC Corporation EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems Security Target
ST Version	Version 1.2
Author	Corsec Security, Inc. Nathan Lee and Matthew Appler
TOE Identification	EMC CLARiiON FLARE 03.24.010.5.011, FLARE 03.24.020.5.011, FLARE 03.24.040.5.011, and FLARE 03.24.080.5.011, with Navisphere v6.24.0.6.13, running on CX3 Series Storage Systems
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of 2006-06-29 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+: EAL2 Augmented with ALC_FLR.1 Basic flaw remediation

Keywords	Storage Area Network (SAN), storage array, data storage, CLARiiON, EMC, FLARE, Navisphere

1.3 Conventions

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

The Common Criteria (CC) allows for several operations to be performed on security requirements: assignment, refinement, selection, and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security functions provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The EMC CLARiiON is a storage device designed to provide managed storage on a SAN. The CLARiiON hardware runs the CLARiiON FLARE/Navisphere software suite, which is the TOE. It includes a Storage Operating Environment (SOE) providing Redundant Array of Independent Disks (RAID) and virtual storage capability, as well as an interface by which EMC CLARiiON storage appliances in a SAN environment can be administered and managed.

The purpose of a SAN is to allow many different application servers to share storage provided by centrally managed storage devices. The EMC CLARiiON allows an organization to manage its storage needs separately from its application servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application servers. In a typical deployment scenario, individual application servers are attached to a SAN through a Fibre Channel switch. These application servers are then configured to use storage on the CLARiiON, in the form of Logical Units (LUNs), as storage for their applications. CLARiiON storage can also be used through an EMC Celerra to provide Network Attached Storage (NAS) for traditional Internet Protocol (IP) based clients. Figure 1 below shows the details of the deployment configuration of the TOE.

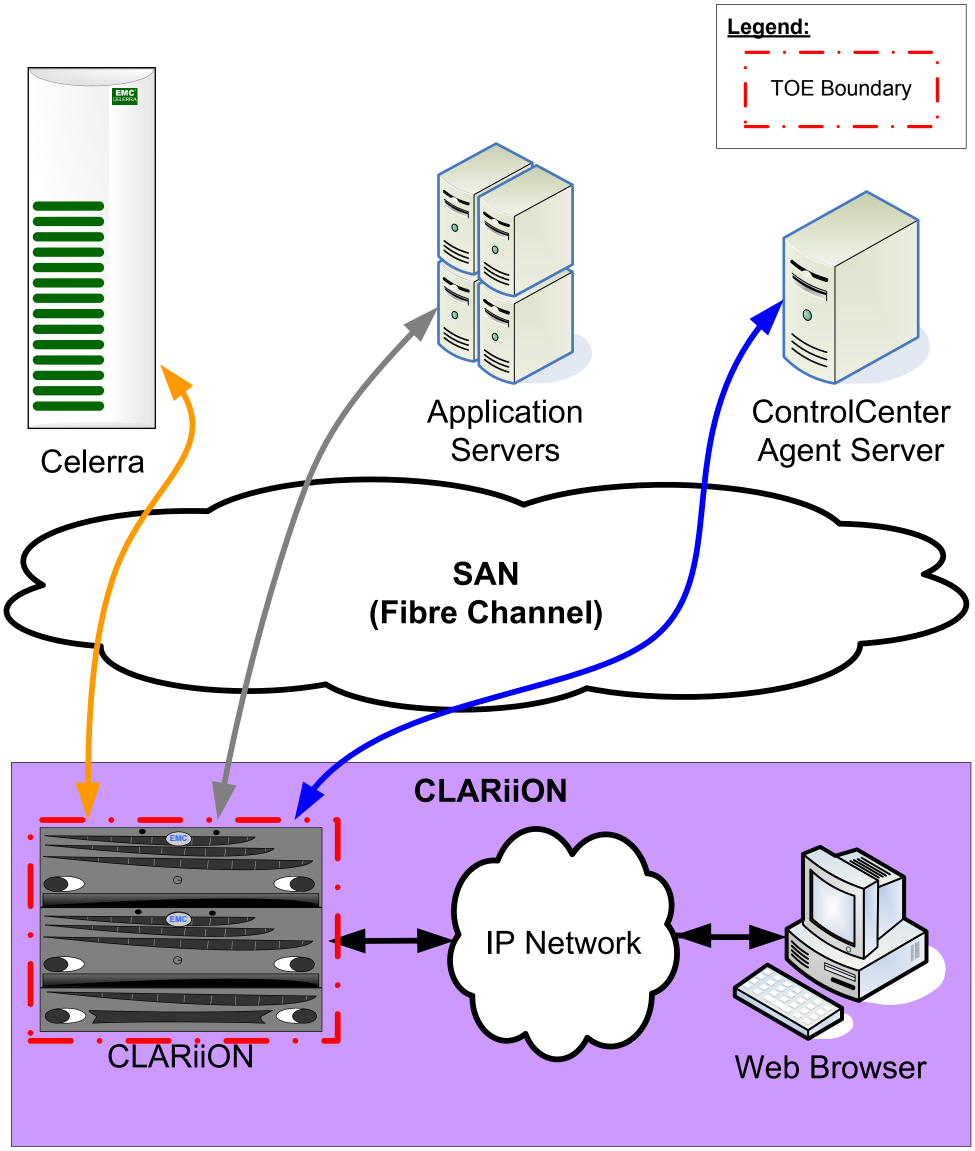

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The EMC CLARiiON running CLARiiON FLARE/Navisphere is a secure, storage management solution that provides a complete suite of management capabilities. It provides the underlying operating environment for the EMC CLARiiON, which provides SAN-attached storage to configured servers. The product provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to the data that it stores. The CLARiiON accomplishes this through purpose-built hardware and software. They are designed to allow customers to scale both system performance and storage capacity.

The EMC Navisphere software is a management application suite designed to be the central console in a CLARiiON-based Storage Area Network (SAN). The purpose of a SAN is to allow many different application servers to share storage provided by centrally managed storage devices. This architecture allows an organization to manage its storage needs separately from its application servers, allowing greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application servers.

The TOE is managed by authorized users through the Navisphere Manager and the Navisphere Secure CLI[1] interfaces. Navisphere Manager is a Java-based applet that runs within a web browser. To access the functions available via Navisphere Manager, an authorized user must open a web browser and enter the IP address or hostname of the desired storage system Storage Processor (SP). Navisphere Secure CLI 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. CLI commands can also be used to automate management functions via shell scripts and batch files.

The EMC FLARE software is a SOE optimized for implementation of RAID storage architectures, providing fault detection, isolation, and diagnosis capabilities. It enables the use of virtual storage elements (LUNs) to improve performance and capacity utilization. The FLARE software also provides a Navisphere-managed storage appliance with the flexibility to support multiple generations of CLARiiON hardware and different types of interconnects with consistent functionality. FLARE 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 LUNs within a storage system that is 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 application servers. This is done through the TOE's SP Agent. The SP Agent collects event information about the state of the system, including FLARE, the TOE's hardware components, and the TOE's LUNs and reports this information to authorized TOE users. The SP Agents also communicate host registration information between the SP Agents and the application servers. These agents periodically retrieve volume-mapping information from the storage systems and forward it to Navisphere Manager for display.

2.2.1 CLARiiON FLARE/Navisphere Concepts

2.2.1.1 LUNs

A central concept of the CLARiiON product is a virtual memory unit called a LUN. The CLARiiON storage appliance presents storage to the SAN is in the form of a LUN, and the CLARiiON FLARE/Navisphere software provides for the management of LUNs. Each LUN represents a unit of storage to an application server, analogous to a local disk drive. However, the LUN provided by the CLARiiON FLARE/Navisphere is not constrained to be a single individual disk. In fact, a typical deployment would have LUNs that span multiple individual disks that are grouped into a RAID Group.

2.2.1.2 Storage Processors

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

2.2.1.3 RAID Groups

A RAID Group is a collection of individual disks. The CLARiiON 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 CLARiiON through successive levels of abstraction.

[1] CLI – Command Line Interface

2.2.1.4 Storage Groups

The CLARiiON manages access to LUNs through a component of the SP called Access Logix. Access Logix allows an administrator to group LUNs together in a Storage Group. Each Storage Group can then be mapped to one or more application servers, identified by their Fibre Channel World Wide Name (WWN). When this mechanism is used, only the LUNs that are present in a Storage Group that a particular application server has been given access to are made accessible to that application server. These LUNs are then available for exclusive use by that application server.

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

2.3 TOE Boundaries and Scope

This section will primarily address the physical and logical components of the TOE that are included in the evaluation.

2.3.1 Physical 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. The TOE is the EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems software suite. The TOE runs on the EMC CLARiiON CX3 UltraScale Series hardware, models 10, 20, 40, and 80.

2.3.1.1 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 LUNs 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.

2.3.2 Logical Boundary

The TOE is a software-only TOE consisting of EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems. The TOE runs the Navisphere software suite, which includes Navisphere Storage-System Initialization Utility, Navisphere Host and SP Agents, Navisphere Server Utility, Navisphere Manger, Navisphere Integrator, Navisphere Storage Management Server, and Navisphere Secure CLI. The TOE also includes the following FLARE versions: FLARE 03.24.010.5.011, FLARE 03.24.020.5.011, FLARE 03.24.040.5.011, and FLARE 03.24.080.5.011.

The TOE is managed by authorized users through the Navisphere Manager and the Navisphere Secure CLI. Navisphere Manager is a Java applet that runs within a web browser. Navisphere Secure CLI is a command line interface that provides access to common functions for monitoring and managing the TOE.

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:

- Identification and Authentication
- Protection of the TSF
- Security Management
- User Data Protection

2.3.2.1 Identification and Authentication

The TOE provides the ability for administrators to manage the security functions of the TOE. The Identification and Authentication security function allows the TOE to identify and authenticate administrators of the TOE. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage.

2.3.2.2 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features, such as identification and authentication and access control mediation. The TOE maintains its own domain for execution and does not share any hardware with other applications.

2.3.2.3 Security Management

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.

2.3.2.4 User Data Protection

The User Data Protection function implements functionality necessary to protect User Data which is entrusted to the TOE. The TOE protects user data primarily in two ways. First, it ensures that only the application servers 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.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

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

- CLARiiON storage appliance hardware
- internet Small Computer System Interface (iSCSI) with Challenge-Handshake Authentication Protocol (CHAP) authentication
- EMCRemote
- Classic Command Line Interface (CLI)
- Navisphere Analyzer
- Navisphere SnapView
- Navisphere MirrorView/Asynchronous
- Navisphere MirrorView/Synchronous
- Navisphere SAN Copy
- Navisphere Quality of Service Manager (NQM)

3 Security Environment

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:

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

3.1 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.

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.

3.2 Threats to Security

This section identifies the threats to the Information Technology (IT) 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/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/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE)

The following threats are applicable:

Name	Description
T.DATA_CORRUPTION	Data could become corrupted due to hardware failure or incorrect system access
T.IMPROPER_SERVER	A system connected to the TOE could access data to which it was not intended to gain access by bypassing the protection mechanisms of the TOE

3.3 Organizational Security Policies

There are no Organizational Security Policies.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

Name	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.BYPASS	The TOE must ensure that the TSF cannot be bypassed.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Name	Description
OE.PROPER_NAME_ASSIGNMENT	The TOE environment must provide accurate World Wide Names for each system that communicates with 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 application servers to communicate 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.

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 non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Security Requirements

This section defines the SFRs and SARs met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 2 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_UAU.2(a)	User authentication before any action				✓
FIA_UID.2(a)	User identification before any action				✓
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_MTD.1(c)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				
FPT_SEP.1	TSF domain separation				

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

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.

5.1.1 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] on

[*a] Subjects: Application Servers;*

b) Objects: LUNs

c) Operations: Read and Write

].

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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*
2. *Storage Group Membership*

].

FDP_ACF.1.2

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

[

A valid 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.1.3

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.1.4

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.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

FDP_SDI.2.1

The TSF shall monitor user data stored within the TSC for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 3 and RAID 5*].

FDP_SDI.2.2

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

Dependencies: No dependencies

5.1.2 Class FIA: Identification and Authentication

FIA_UAU.2(a) User authentication before any action

Hierarchical to: FIA_UAU.1

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(a) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.3 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*membership in a Storage Group*] to [*the Administrator and Manager roles*].

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

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.3.2

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

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

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query*] the [*storage system information*] to [*the Administrator, Manager, and Monitor roles*].

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

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

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

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

FMT_MTD.1(c) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

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

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

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 security management functions:

[

a) Management of security functions behaviour;

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 [*as the authorized identified roles in Table 3*].

Table 3 - Authorized Roles

Roles	Description
Administrator	This role can access all administrative and management interfaces and data, can change a user's role, can add or delete users, and depending on the scope of the account can add or delete information from a domain.
Manager	This role can view all storage system information and perform storage-system operations (such as binding LUNs), but cannot add, modify, or delete user or domain information.
Monitor	This role can view all storage-system information, but cannot add, modify, or delete information from a domain or perform configuration operations such as binding LUNs.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirement on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.3 and hence conformant to CC Version 2.3 Part 2.

Name	Description	S	A	R	I
FIA_UAU.2(b)	User authentication before any action			✓	✓
FIA_UID.2(b)	User identification before any action			✓	✓

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

5.2.1 Class FIA: Identification and Authentication

FIA_UAU.2(b) User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user **of an Application Server** to be successfully authenticated **to the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2(b) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user **of an Application Server** to identify itself **to the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from Part 3 of the CC at EAL2+ augmented with ALC_FLR.1. Table 4 – Assurance Requirements summarizes the requirements.

Table 4 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Flaw Remediation	ALC_FLR.1 Basic flaw remediation
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_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 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 are suitable to satisfy the necessary requirements.

Table 5 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Identification and Authentication	FIA_UAU.2(a)	User authentication before any action
	FIA_UID.2(a)	User identification before any action
Protection of TOE Security Functions	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data
	FMT_MTD.1(c)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control

TOE Security Function	SFR ID	Description
	FDP_SDI.2	Stored data integrity

6.1.1 Identification and Authentication

The Identification and Authentication security function provides the TOE with the ability to govern access by Administrators. Administrators of the TOE can access the TOE in one of two methods. An Administrator can manage the TOE through the Navisphere Manager, a web-based graphical user interface. An Administrator can also manage the TOE through the Navisphere Secure CLI, a command line interface application. Prior to allowing access through these interfaces, the TOE requires an Administrator to be identified using a username and password. Before successful completion of the security function, an Administrator is unable to perform any management function.

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

6.1.2 Protection of the TSF

Protection of the TSF provides for the integrity of the mechanisms that protect the TOE. The TOE runs on a purpose-built hardware appliance. It does not share memory or processors with any other application or system. The TOE maintains its own domain for its execution. Interfacing with the TOE is only done through well-defined interfaces, each utilizing security functions to maintain the security of that interface. The TOE relies on its environment to provide protection from physical tampering.

Non-bypassability of the TSP is provided through basic configuration and enforcement of the security mechanisms. All Administrators and Users of the TOE must be authenticated prior to performing any security functionality. Once authenticated, Administrators and Users can only perform operations which they have been explicitly granted permission to perform. The TOE uses unique sessions for each operator and maintains separation between concurrent operators.

6.1.3 Security Management

The purpose of the TOE is to provide a storage system to application servers attached to a SAN. The TOE provides mechanisms to govern which application servers can access which LUNs. The Security Management function allows Administrators to properly configure this functionality.

Management of the TOE occurs through either the Navisphere Manager or the Navisphere Secure CLI. Administrators of the TOE are assigned one of three roles. These three roles are hierarchical in nature; the higher level role is a superset of the previous (lower) roles' functionality. The following description of the Security Management function is described through the capabilities of each of the roles, starting with the least privileged role.

The Monitor role allows an Administrator to query information about the TOE. The Monitor role may view information about individual disk drives, RAID Groups, LUNs, and Storage Groups. This functionality is provided through the Navisphere interfaces.

The Manager role can perform all of the functionality of the Monitor role and can configure and modify storage system objects. The Manager role can:

- add and remove individual disk drives to a RAID Group
- create and modify LUNs
- administer membership of LUNs and application servers in a Storage Group

The Administrator role can perform all of the functionality of the Monitor and Manager roles and can manage user accounts. This includes creating, deleting, and changing the role of any user account on the TOE.

6.1.4 User Data Protection

The TOE provides the User Data Protection security function to manage access from application servers to configured LUNs. The purpose of SAN attached storage is to allow high speed, scalable, fault-tolerant storage separate from individual application servers. The TOE provides this functionality for servers connected to the SAN.

Using the Security Management security function, Administrators of the TOE can configure LUNs to provide storage to application servers. These LUNs are then placed into Storage Groups, which allows an Administrator to limit access to each LUN to one or more application servers. When an application server requests a list of available LUNs from the TOE, the TOE Environment provides a WWN. This WWN is used to identify the application server to the TOE. The TOE then provides a list of LUNs that the application server has been granted access to. With each successive request to read or write information to a LUN, the TOE ensures that only authorized application servers have access to the LUNs 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, or 5. 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.

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 6 - Assurance Measures Mapping to TOE SARs

Assurance Component	Assurance Measure
ACM_CAP.2	EMC CLARiiON FLARE/Navisphere - Configuration Management: Capabilities
ADO_DEL.1	EMC CLARiiON FLARE/Navisphere - Delivery and Operation: Secure Delivery
ADO_IGS.1	[Installation and Setup Procedure]
ADV_FSP.1	EMC CLARiiON FLARE/Navisphere - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	EMC CLARiiON FLARE/Navisphere - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	EMC CLARiiON FLARE/Navisphere - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	[Administrator Guides]
AGD_USR.1	[User Guides]
ALC_FLR.1	EMC CLARiiON FLARE/Navisphere – Life Cycle Support: Flaw Remediation
ATE_COV.1	EMC CLARiiON FLARE/Navisphere – Functional Tests and Coverage
ATE_FUN.1	EMC CLARiiON FLARE/Navisphere – Functional Tests and Coverage

Assurance Component	Assurance Measure
ATE_IND.2	Provided by laboratory evaluation
AVA_SOF.1	EMC CLARiiON FLARE/Navisphere - Vulnerability Assessment
AVA_VLA.1	EMC CLARiiON FLARE/Navisphere - Vulnerability Assessment

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at EMC. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery. The Installation Documentation provided by EMC details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users(s) on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The EMC design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.5 ALC_FLR.1: Basic Flaw Remediation

The Flaw Remediation document outlines the steps taken at EMC to capture, track, and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.

6.2.6 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing, ATE_IND.2: Independent Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

6.2.7 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum Strength of Function (SOF) requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ST. The following tables demonstrate the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

8.1.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT mitigates 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 to which 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 supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT ensures that the TOE provides adequate mechanisms to give only authorized servers access to the appropriately authorized data.
	OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide	OE.PROPER_NAME_ASSIGNMENT ensures that the World Wide Names provided to the TOE are accurate.

Threats	Objectives	Rationale
	accurate World Wide Names for each system that communicates with the TOE.	This allows the mechanisms provided by O.PROTECT to properly protect data.
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURECOMMUNICATIONS ensures that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	OE.SECURE_SERVERS The TOE environment must provide properly configured application servers to communicate with the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that each server connected to the Storage Area Network operates properly and does not intentionally compromise data.

8.1.2 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security will be provided for the TOE and its environment.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	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. OE.PHYSICAL satisfies this assumption.
A.MANAGE 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.	Those 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. OE.MANAGE satisfies this assumption.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	Sites using the TOE ensure that administrators are non-hostile, appropriately trained, and follow all administrator guidance. OE.NOEVIL satisfies this assumption.

8.2 Security Functional Requirements Rationale

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

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UAU.2(a) User authentication before any action	The TOE shall successfully authenticate each administrator before allowing them to manage the TOE.
	FIA_UID.2(a) User identification before any action	The TOE will properly identify and authenticate all administrators.
	FMT_MTD.1(c) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1(b) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of the TOE.
	FMT_SMF.1 Specification of management functions	FMT_SMF specifies each of the management functions that are utilized to securely manage the TOE.
	FMT_MTD.1(a) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MSA.3 Static attribute initialisation	Permissive values for data access are provided, and the TOE administrator can change them when a data object is created.
	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators.
O.BYPASS The TOE must ensure that the	FPT_SEP.1 TSF domain separation	The TOE maintains a security domain for its execution that protects it from interference and tampering.

Objective	Requirements Addressing the Objective	Rationale
TSF cannot be bypassed.	FPT_RVM.1 Non-bypassability of the TSP	The TOE ensures that policy enforcement functions are invoked and succeed before each function is allowed to proceed
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_SDI.2 Stored data integrity	
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to data within the TOE.
	FDP_ACC.1 Subset access control	The TOE has an access control policy which ensures that only authorized servers gain access to data within the TOE.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network.	FIA_UAU.2(b) User authentication before any action	Users are not able to access the TOE until the environment has properly authenticated the user.
OE.SECURE_SERVERS The TOE environment must provide properly configured application servers to communicate with the TOE.	FIA_UAU.2(b) User authentication before any action	The TOE will not give access to a user until the environment has properly authenticated the user.
OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate World Wide Names for each system that communicates with the TOE.	FIA_UID.2(b) User identification before any action	The TOE will not give access to a user until the environment has properly identified the user.

8.3 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. At EAL2+, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.4 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

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

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

The words “to the TOE Environment” have been added to FIA_UAU.2(b) and FIA_UID.2(b).

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the CC. Table 7 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 7 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	No Dependencies	✓	
FIA_UAU.2(a)	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UAU.2(b)	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UID.2(a)	No Dependencies	✓	
FIA_UID.2(b)	No Dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(c)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No Dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FPT_RVM.1	No Dependencies	✓	
FPT_SEP.1	No Dependencies	✓	

8.6 TOE Summary Specification Rationale

8.6.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (TSS) (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. These sets of security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the

TSF to meet the security functional requirements. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 5 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

8.6.2.1 Configuration Management

The *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems - Configuration Management: Capabilities* documentation provides a description of tools used to control the configuration items and how they are used at the EMC. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.6.2.2 Delivery and Operation

The *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems - Delivery and Operation: Secure Delivery* documentation provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery. The Installation Documentation provided by EMC details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.6.2.3 Development

The *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence* design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.6.2.4 Guidance Documentation

The EMC Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. EMC provides single versions of documents which address the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.6.2.5 Life Cycle Support

The *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems – Life Cycle Support: Flaw Remediation* documentation describes the processes that EMC follows to capture, track, and correct flaws (or "bugs") that are found within the TOE. The documentation demonstrates that all discovered flaws are recorded and that the process ensures that flaws are tracked through their entire life cycle.

Corresponding CC Assurance Components:

- Basic Flaw Remediation

8.6.2.6 Tests

There are a number of components that make up the *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems – Tests; Coverage Functional Tests* documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. EMC Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.6.2.7 Vulnerability and TOE Strength of Function Analyses

The *EMC EMC CLARiiON FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems - Vulnerability Assessment: Strength of TOE Security Functions* documentation is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.7 Strength of Function

A SOF rating of SOF-basic was claimed for this TOE to meet the EAL2+ assurance requirements. This SOF is sufficient to resist the threats identified in Section 3 of the Security Target. Section 8 of the Security Target demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. Section 8.1 of the Security Target provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 of the Security Target demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense (DoD) low robustness environments processing unclassified information.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are:

- Identification and Authentication: FIA_UAU.2 - User Authentication before any action

The only mechanisms within the TOE that are probabilistic and permutational in nature are the passwords used to authenticate users to the TOE.

9 Acronyms

Table 8 - Acronyms

Acronym	Definition
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
DoD	Department of Defense
EAL	Evaluation Assurance Level
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
ISO	International Organization for Standardization
IT	Information Technology
LUN	Logical Unit
NAS	Network Attached Storage
NQM	Navisphere Quality of Service Manager
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SOE	Storage Operating Environment
SOF	Strength of Function
SP	Storage Processor
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	Toe Summary Specification
WWN	World Wide Name