EMC Corporation
Data Domain Operating System
v4.8.2.0

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.7

Prepared for:

EMC Corporation
2421 Mission College Blvd.
Santa Clara, CA 95054
Phone: (408) 980-4800

http://www.datadomain.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
0.1	2009-06-18	Nathan Lee	Initial draft.
0.2	2009-12-24	Josh McCally Justin Yu	Addressed laboratory verdicts; modified FTA_SSL.3.
0.3	2010-03-03	Justin Yu	Removed EXT_FTP class
0.4	2010-04-12	Justin Yu	Changes made per EWA comments
0.5	2010-05-18	Amy Nicewick	Updated TOE version number and Figure 1, added TOE hardware models to Section 1.4.1, and addressed lab comments dated 2010/03/15.
0.6	2010-08-31	Amy Nicewick	Updated TOE version and build numbers.
0.7	2010-10-18	Amy Nicewick	Updated company name and addressed other miscellaneous comments.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the EMC Corporation Data Domain Operating System v4.8.2.0, and will hereafter be referred to as the TOE throughout this document. The TOE is the principal software component of EMC® Data Domain® disk-based backup and recovery appliances.

1.1 Purpose

This ST provides 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 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 0) – 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 Definition (Section 2) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 3) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 4) – 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 5) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 7) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 8) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	EMC Corporation Data Domain Operating System v4.8.2.0 Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc. Nathan Lee
ST Publication Date	October 18, 2010
TOE Reference	Data Domain Operating System v4.8.2.0 Build 201150

1.3 Product Overview

EMC Data Domain disk-based de-duplication storage systems optimize data protection and disaster recovery performance. EMC Data Domain offers a comprehensive range of appliances to meet the backup and archive storage needs of enterprises of all sizes, as they seek to reduce costs and simplify data management. EMC Data Domain systems support all leading enterprise backup and archive applications for seamless integration into existing Information Technology (IT) infrastructures. An EMC Data Domain system makes backup data available with the performance and reliability of disks at a cost competitive with tape-based storage. The integrity of stored data is ensured via multiple levels of data checking and repair, including methods that utilize OpenSSL.

The primary benefit of an EMC Data Domain solution over competing technologies is EMC Data Domain's data de-duplication technology, which stores only unique "segments" of files on disk, dramatically reducing the amount of physical storage required in a typical backup environment. Data de-duplication technology can be performed on-the-fly at line-speed.

An EMC Data Domain system works seamlessly with existing backup software: to a backup server, the EMC Data Domain system appears as a file server supporting the Network File System (NFS) or Common Internet File System (CIFS) protocols over an Ethernet connection, or as a virtual tape library over a Fibre Channel connection. Multiple backup servers can share one EMC Data Domain system, and each EMC Data Domain system can handle multiple simultaneous backup and restore operations. If additional throughput and capacity are needed, multiple EMC Data Domain systems can be attached to one or more backup servers. EMC Data Domain systems can also provide replication services, whereby one EMC Data Domain system acts as a backup for another EMC Data Domain system.

EMC Data Domain systems are managed via a command line interface (CLI) at the console of the local system or via a web-based graphical user interface (GUI) hosted on the local system and accessed over a network connection from a management workstation.

1.4 TOE Overview and Description

The TOE Overview provides a context for the TOE evaluation by identifying the TOE type and defining the specific evaluated configuration.

1.4.1 TOE Type

The TOE is a software-only TOE consisting of the Data Domain Operating System (DD OS) software. The TOE runs on Data Domain appliance hardware. The Data Domain appliance hardware models are:

- DD120
- DD140
- DD410
- DD430
- DD460
- DD510
- DD530
- DD560
- DD565
- DD580
- DD610
- DD630
- DD660
- DD690
- DD880

1.4.2 Evaluated Configuration

As shown in Figure 1 below, the TOE encompasses the entire DD OS software image and excludes the hardware on which the DD OS executes. All functionality (except functionality called out in Section 1.4.6 below) of the DD OS is included within the TOE boundary, but no security claims are made about the use of OpenSSL.

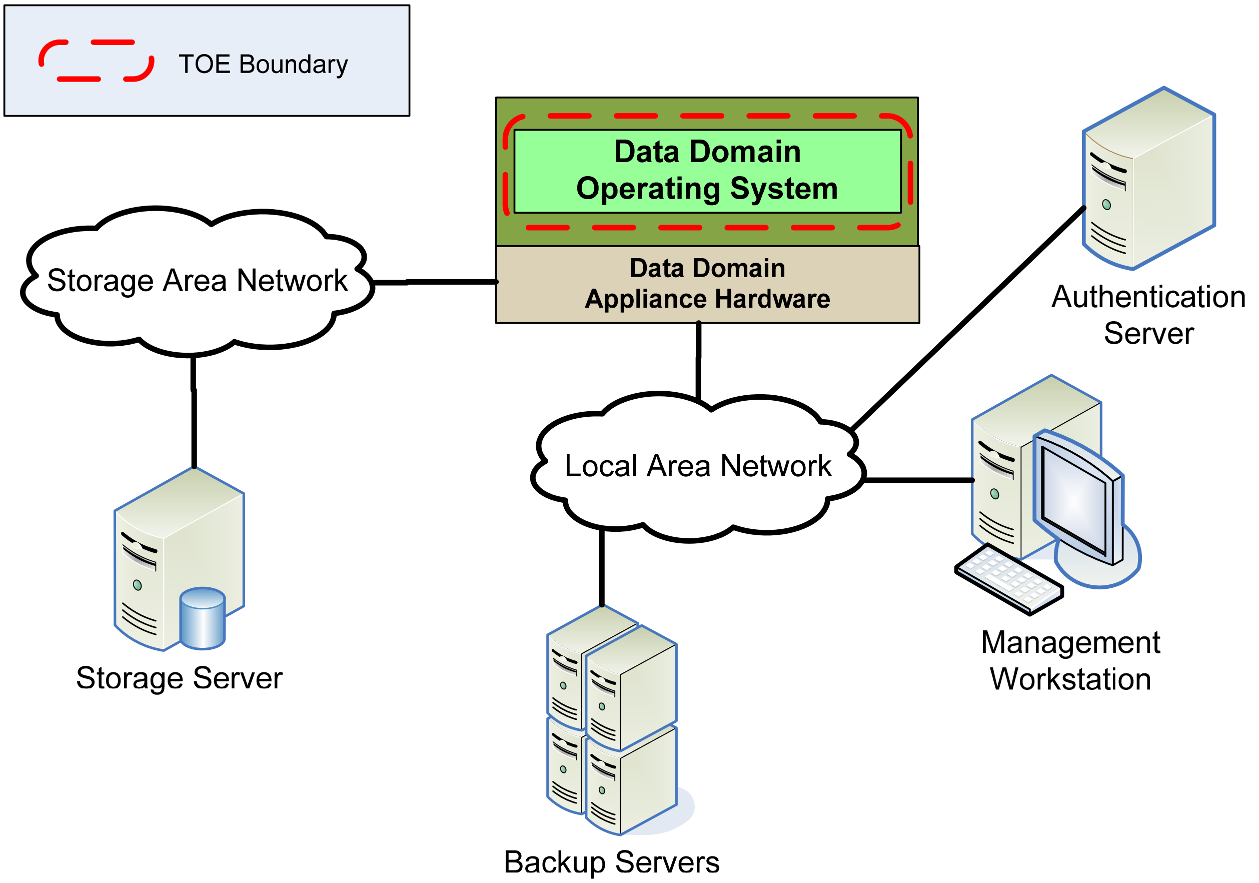

Figure 1 – TOE and TOE Environment

1.4.3 TOE Environment

The TOE requires the following components to be properly configured and available in the operational environment:

- Data Domain appliance hardware, on which the TOE runs, including local storage for de-duplicated backup data.
- Management Workstation, used to administer the TOE.
- Backup Server(s), which use the TOE for storage and retrieval of backup data.
- Optional external authentication server
- Optional Storage Area Network (SAN), in which the TOE can store and retrieve de-duplicated backup data.

1.4.4 TOE Physical and Logical Scope

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

Figure 1 above illustrates the physical and logical 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 Boundary includes the entire DD OS software image, but excludes the underlying hardware. It also excludes the management workstation, backup servers, optional authentication server, and optional SAN.

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Audit
- User Data Storage
- Identification and Authentication
- Management

1.4.4.1 Audit

The TOE audits all logins, logouts, and administrative actions (whether they succeed or fail) on the TOE's GUI and CLI. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, user identity, and a message indicating the outcome (success or failure) of the event. The TOE also audits the startup and shutdown of the audit function. The TOE can provide audit review functions to all users of the TOE. However, in CC-configuration mode, only the users with *Admin* or *SE*[1] role can review the audit records. The users with *user* role cannot access the audit records. Disabling of the audit review functions for the users with *user* role is achieved by an *SE* user resetting a registry key using the following command from the command line interface: *reg set config.user.longvisible=false.* Hence, the TOE provides audit review functions, and it restricts audit review to users with the appropriate permissions.

1.4.4.2 User Data Storage

The TOE optimizes the storage of user data by scanning all user data that is to be stored for segments of data that have already been stored (as part of a different set of user data). If a duplicate segment is found, the TOE will replace the duplicate segment with a pointer to the already-stored segment, and will store the rest of the unique user data.

Information Flow Control permissions for stored user data flowing between the TOE and external servers are implemented through the User Data Information Flow Control Security Functional Policy (SFP).

The TOE provides methods by which administrators can ensure that deleted user data is thoroughly destroyed.

If a disk error (resulting in the loss of or inability to read user data) is encountered, the TOE is able to reconstruct the user data.

The TOE has the ability to enforce minimum and maximum retention lock periods for the protection of stored user data from modification and deletion.

1.4.4.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting an authenticated service has provided a valid username and password and is authorized to access that service. For each user, the TOE stores the following security attributes: username, password (if the user is a local user), role, logon status, date and time password was most recently set, date and time password expires, and GUI session key (if the user is currently logged into the GUI).

[1] SE – Systems Engineer

1.4.4.4 Management

Access Control permissions for TOE users managing the TOE are implemented by the Management Access Control SFP. The TOE implements three user roles: *User*, *Admin*, and *SE*, each with defined permissions. Inactive administrative sessions on the TOE's GUI are automatically terminated after thirty minutes of inactivity.

1.4.5 Guidance Documentation

The following product guides are part of the TOE:

- Data Domain Operating System Release Notes Version 4.8
- Data Domain Operating System User Guide Software Version 4.8

1.4.6 Product Features and Functionality not included in the TOE

Features and functionality that are not part of the evaluated configuration of the TOE are:

- Telnet access to the management CLI
- Diffie-Hellman Crypto
- OpenSSL

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 7.1.

Table 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 extended; CC Part 3 conformant; PP claim (none).
PP Identification	None
Evaluation Assurance Level	EAL2+ (Augmented with Flaw Reporting Procedures (ALC_FLR.2))

2 Security Problem Definition

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

2.1 Threats to Security

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

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings and 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 and 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 backup data saved on or being transmitted to or from the TOE. Removal, diminution and mitigation of the threats are through the objectives identified in Section 3 - Security Objectives.

The following threats are applicable:

Table 3 – Threats

Name	Description
T.DATA_STORAGE	Data could become corrupted due to incorrect system access by TOE users or non-TOE users, or could be stored inefficiently.
T.IMPROPER_SERVER	A system (under the control of a TOE user or a non-TOE user) connected to the TOE could access data to which it was not intended to gain access by bypassing the protection mechanisms of the TOE.

2.2 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 Organizational Security Policies.

2.3 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.PHYSICAL	Physical security will be provided for the TOE and its environment.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
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.

3 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 2). 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.

3.1 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.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.AUDIT	The TOE must provide a means of detecting and logging security-relevant events, and must provide administrators with a means of reviewing the audit log.
O.DATA_OPTIMIZATION	The TOE must disallow the duplication of stored data by identifying and removing previously-stored segments.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.

3.2 Security Objectives for the Operational Environment

3.2.1 IT Security Objectives

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

Table 6 – IT Security Objectives

Name	Description
OE.SECURE_COMMUNICATIONS	The TOE environment must provide secure communications between systems connected to the TOE.
OE.SECURE_SERVERS	The TOE environment must provide servers configured per current corporate security policy guidelines to communicate with the TOE.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

3.2.2 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 or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 – Non-IT Security Objectives

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

4 Extended Components Definition

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 5.1.1.

4.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 – Extended TOE Security Functional Requirements

Name	Description
EXT_FDD_DDR.1	Duplicate data removal
EXT_FRU_RLP.1	Minimum and maximum retention lock periods

4.1.1 Class EXT_FDD: User Data De-Duplication

User Data De-Duplication functions involve optimizing the storage of user data by identifying segments of data that have already been stored, and ensuring that redundancy is not caused by storing those segments multiple times for different sets of user data. The EXT_FDD: User Data De-Duplication class was modeled after the CC FDP: User Data Protection class. The extended family and related components for EXT_FDD_DDR: Duplicate data removal was modeled after the CC family FDP_RIP: Subset residual information protection.

4.1.1.1 Duplicate data removal (EXT_FDD_DDR)

Family Behaviour

This family defines the requirements for data de-duplication functionality.

Component Leveling

EXT_FDD_DDR.1: Duplicate data removal
1

Figure 2 – EXT_FDD_DDR Duplicate data removal family decomposition

EXT_FDD_DDR.1 Duplicate data removal, provides the capability to remove redundant data from the stored user data.

Management: EXT_FDD_DDR.1

The following actions could be considered for the management functions in FMT:

- Maintenance (deletion, modification, addition) of the group of users and file servers with access rights to the stored user data.

EXT_FDD_DDR.1 Duplicate data removal

Hierarchical to: No other components

Dependencies: No dependencies

This component will ensure that the TOE identifies and removes segments of data that have been previously stored, before storing user data.

EXT_FDD_DDR.1.1 The TSF[2] shall ensure that any previously stored data segments in incoming user data are identified and removed from the user data before the user data is stored.

[2] TSF – TOE Security Functionality

4.1.2 Class FRU: Resource Utilization

Resource Utilization functions involve optimizing the storage of user data by identifying segments of data that have already been stored, and ensuring that redundancy is not caused by storing those segments multiple times for different sets of user data. The extended family and related components for EXT_FRU_RLP: Minimum and maximum retention lock periods was modeled after the CC family FRU_RSA: Resource allocation.

4.1.2.1 Minimum and maximum retention lock periods (EXT_FRU_RLP)

Family Behaviour

The requirements of this family allow the TSF to control the use of retention lock periods.

Component Leveling

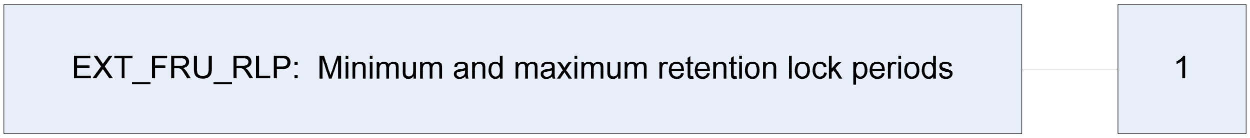

Figure 3 – EXT_FRU_RLP Minimum and maximum retention lock periods family decomposition

EXT_FRU_RLP.1 Minimum and maximum retention lock periods, provides the capability to institute retention lock periods for the purpose of protecting a file from being modified or deleted during the specified retention period.

Management: EXT_FRU_RLP.1

The following actions could be considered for the management functions in FMT:

- Specifying minimum and maximum limits for retention lock periods for specified files.

Audit: EXT_FRU_RLP.1

The following actions could be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Rejection of file modification or deletion attempt due to active retention lock period.
- Basic: All attempted file modifications or deletions for files that are under control of the TSF.

EXT_FRU_RLP.1 Minimum and maximum retention lock periods

Hierarchical to: No other components

Dependencies: No dependencies

EXT_FRU_RLP.1.1 The TSF shall enforce maximum retention lock periods of files of stored user data that are retained on disk in a non-rewriteable and non-eraseable format.

EXT_FRU_RLP.1.2 The TSF shall ensure the provision of minimum retention lock periods of files of stored user data that are retained on disk in a non-rewriteable and non-eraseable format.

4.2 Extended TOE Security Assurance Components

There are no extended assurance components.

5 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 5.1.1.

5.1.1 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 Parts 2 and 3 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 italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses 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.

5.2 Security Functional Requirements

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

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
EXT_FDD_DDR.1	Duplicate data removal				
FDP_ACC.2	Complete access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_IFC.2	Complete information flow control		✓		

Name	Description	S	A	R	I
FDP_IFF.1	Simple security attributes		✓		
FDP_RIP.1	Subset residual information protection	✓	✓		
FDP_SDI.2	Stored data integrity monitoring and action		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
EXT_FRU_RLP.1	Minimum and maximum retention lock periods				
FTA_SSL.3	TSF-initiated termination		✓	✓	

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

5.2.1 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:

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*login and logout on the CLI and GUI;*
- *all administrative actions performed on the CLI and GUI*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- 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_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

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

Dependencies: FAU_SAR.1 Audit review

5.2.2 Class EXT_FDD: User Data De-Duplication

EXT_FDD_DDR.1 Duplicate data removal

Hierarchical to: No other components.

EXT_FDD_DDR.1.1

The TSF shall ensure that any previously stored data segments in incoming user data are identified and removed from the user data before the user data is stored.

Dependencies: No dependencies

5.2.3 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1

The TSF shall enforce the [*Management Access Control SFP*[3]] on [*subjects: TOE users, and objects: audit data and TOE configuration data*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

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 [*Management Access Control SFP*] to objects based on the following: [

- *Subjects: TOE users*
  - *Security Attributes:*
    - *Username*
    - *Role*
- *Objects: audit data and TOE configuration data*
  - *Security Attributes:*
    - *Permissions*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an authorized user can manipulate audit data and/or the TOE configuration if the user’s role has the appropriate permissions*].

FDP_ACF.1.3

[3] SFP – Security Functional Policy

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

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

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

FDP_IFC.2.1

The TSF shall enforce the [*User Data Information Flow Control SFP*] on [*subjects: external servers, and information: stored user data*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*User Data Information Flow Control SFP*] based on the following types of subject and information security attributes: [

- *Subjects: External servers*
  - *Security Attributes:*
    - *Identity*
- *Information: stored user data*
  - *Security Attributes:*
    - *Permissions*

].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*an authorized external server can access stored user data if the external server has the appropriate permissions*].

FDP_IFF.1.3

The TSF shall enforce [*no additional information flow control SFP rules*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1

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

Dependencies: No dependencies

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*[4] *6*].

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

[4] RAID – Redundant Array of Inexpensive Disks

5.2.4 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: [*username, password (if the user is a local user), role, logon status, date and time password was most recently set, date and time password expires, GUI session key (if the user is currently logged into the GUI)*].

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

5.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [*all management functions*] to [*administrators with the appropriate role*].

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Management Access Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*all security attributes*] to [*administrators with the appropriate role*].

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Management 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 [*administrators with the appropriate role*] 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 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*change_default, query, modify, delete,*] the [*TSF data*] to [*administrators with the appropriate 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: [*security attribute management, TSF data management, and security function management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*user, admin, SE*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2.6 Class FRU: Resource Utilization

EXT_FRU_RLP.1 Minimum and maximum retention lock periods

Hierarchical to: No other components

EXT_FRU_RLP.1.1

The TSF shall enforce maximum retention lock periods of files of stored user data that are retained on disk in a non-rewriteable and non-eraseable format.

EXT_FRU_RLP.1.2

The TSF shall ensure the provision of minimum retention lock periods of files of stored user data that are retained on disk in a non-rewriteable and non-eraseable format.

Dependencies: No dependencies

5.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive **GUI** session after a [*thirty minute interval of user inactivity*].

Dependencies: No dependencies

5.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ALC : Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional 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 satisfy the necessary requirements.

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

TOE Security Function	SFR ID[5]	Description
Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
User Data Storage	EXT_FDD_DDR.1	Duplicate data removal
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_RIP.1	Subset residual information protection
	FDP_SDI.2	Stored data integrity monitoring and action
	EXT_FRU_RLP.1	Minimum and maximum retention lock periods
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
Management	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes

[5] ID - Identifier

TOE Security Function	SFR ID[5]	Description
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination

6.1.1 Audit

The TOE audits all logins, logouts, and administrative actions (whether they succeed or fail) on the TOE's GUI and CLI. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, user identity, and a message indicating the outcome (success or failure) of the event. The TOE also audits the startup and shutdown of the audit function. The TOE can provide audit review functions to all users of the TOE. However, in CC-configuration mode, only the users with *Admin* or *SE* role can review the audit records. The users with *user* role cannot access the audit records. Disabling of the audit review functions for the users with *user* role is achieved by an *SE* user resetting a registry key using the following command from the command line interface: *reg set config.user.longvisible=false.* Hence, the TOE provides audit review functions, and it restricts audit review to users with the appropriate permissions.

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

6.1.2 User Data Storage

The TOE optimizes the storage of user data by scanning all user data that is to be stored for segments of data that have already been stored (as part of a different set of user data). If a duplicate segment is found, the TOE will replace the duplicate segment with a pointer to the already-stored segment, and will store the rest of the unique user data.

Information Flow Control permissions are implemented in a hierarchical manner. The "subjects" of the Policy are the external servers. Each external server has an identity. The "objects" of the Information Flow Control Policy are the stored user data. Each unit of stored user data has associated permissions.

The TOE provides two methods by which administrators can ensure that deleted user data is thoroughly destroyed. These methods are called "Sanitization" and "Destroy and Zero", and can be manually executed at any time by authorized administrators. The Sanitization method zeroizes the disk locations where deleted user data was stored, but retains all non-deleted data. The Destroy and Zero method zeroizes all user data in the entire filesystem, whether it was marked as deleted or not.

The TOE uses RAID 6 to store user data. RAID 6 provides redundancy and data loss recovery capability in the event of up to two concurrent disk failures. If a disk error (resulting in the loss of or inability to read user data) is encountered, the TOE is able to reconstruct the user data.

The TOE has the ability to enforce retention lock periods for the protection of stored user data from modification and deletion. The retention period that can be specified for a given file is subject to a minimum and a maximum time period. During this period, no user or process may modify or delete the locked file. (Files that are not (or no longer) subject to a retention lock period may be modified or deleted, but are not automatically deleted.)

TOE Security Functional Requirements Satisfied: EXT_FDD_DDR.1, FDP_IFC.2, FDP_IFF.1, FDP_RIP.1, FDP_SDI.2, EXT_FRU_RLP.1.

6.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting an authenticated service has provided a valid username and password and is authorized to access that service. For each user, the TOE stores the following security attributes: username, password (if the user is a local user), role, logon status, date and time password was most recently set, date and time password expires, and GUI session key (if the user is currently logged into the GUI).

The TOE can be configured to use a local user database, or to use remote authentication databases (such as Active Directory or Network Information Service (NIS) servers). When a TOE user enters his username and password at a management interface, the information is checked against the local database or sent to the configured remote authentication server. If the provided username and password are valid then the TOE allows the user to access the TOE with the permissions associated with that username; if not, then the user is allowed to attempt to re-authenticate. Before identification and authentication, the TOE user is only able to identify and authenticate himself.

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

6.1.4 Management

Management Access Control permissions are implemented in hierarchical manner. The “subjects” of the Policy are the users. Each user has a username, role, and inherited role permissions. The “objects” of the Management Access Control Policy are the audit data and TOE configuration data.

The TOE implements three user roles: *User*, *Admin*, and *SE*. The User role is the least-privileged role, and the Admin role is the most-fully-privileged role that an end-user of the TOE can hold. The SE role is a special role that can be assumed by EMC Data Domain engineers in order to perform debugging and maintenance tasks that are not available to end-users. Table 12 below provides a list of the commands that are available to each of these roles. (Note: Commands regarding Telnet are included in Table 12 below for completeness, but Telnet access to the management CLI is excluded from this evaluation.)

Inactive administrative sessions on the TOE’s GUI are automatically terminated after thirty minutes of inactivity.

Table 12 – Commands Available to Each User Role

User	Admin	SE	Command
	✓	✓	adminaccess add ftp <host-list>
	✓	✓	adminaccess add http <host-list>
	✓	✓	adminaccess add ssh <host-list>
	✓	✓	adminaccess add ssh-keys
	✓	✓	adminaccess add telnet <host-list>
	✓	✓	adminaccess authentication add {cifs}
	✓	✓	adminaccess authentication del {cifs}

User	Admin	SE	Command
	✓	✓	adminaccess authentication reset {cifs}
	✓	✓	adminaccess authentication show
		✓	adminaccess certificate generate
✓	✓	✓	adminaccess certificate show { ca | host}
	✓	✓	adminaccess del ftp <host-list>
	✓	✓	adminaccess del http <host-list>
	✓	✓	adminaccess del ssh <host-list>
	✓	✓	adminaccess del ssh-keys <lineno>
	✓	✓	adminaccess del telnet <host-list>
	✓	✓	adminaccess disable {http | https | ftp | telnet | ssh | all}
	✓	✓	adminaccess enable {http | https | ftp | telnet | ssh | all}
	✓	✓	adminaccess reset {ftp | telnet | ssh | http | all}
	✓	✓	adminaccess reset ssh-keys
	✓	✓	adminaccess show
	✓	✓	adminaccess show ssh-keys
	✓	✓	adminaccess trust add host <hostname> [type mutual]
	✓	✓	adminaccess trust copy { source | destination } <hostname>
	✓	✓	adminaccess trust del host <hostname> [type mutual]
✓	✓	✓	adminaccess trust show [hostname]
	✓	✓	adminaccess web option reset [http-port | https-port | session-timeout]
	✓	✓	adminaccess web option set http-port <port-number>
	✓	✓	adminaccess web option set https-port <port-number>
	✓	✓	adminaccess web option set session-timeout <timeout-in-secs>
	✓	✓	adminaccess web option show
	✓	✓	alerts add <email-list>
	✓	✓	alerts clear alert-id <alert-id-list>
	✓	✓	alerts del <email-list>
	✓	✓	alerts reset
✓	✓	✓	alerts show alerts-list
✓	✓	✓	alerts show all
✓	✓	✓	alerts show current
✓	✓	✓	alerts show daily
✓	✓	✓	alerts show history
✓	✓	✓	alerts test [<email-addr>]
✓	✓	✓	alias add <alias-name> "<command>"

User	Admin	SE	Command
✓	✓	✓	alias del <alias-name>
	✓	✓	alias reset
✓	✓	✓	alias show
	✓	✓	authentication nis disable
	✓	✓	authentication nis domain reset
	✓	✓	authentication nis domain set <domain> [servers <server-list>]
✓	✓	✓	authentication nis domain show
	✓	✓	authentication nis enable
	✓	✓	authentication nis groups add <group-list> priv {user | admin}
	✓	✓	authentication nis groups del <group-list> priv {user | admin}
	✓	✓	authentication nis groups reset
✓	✓	✓	authentication nis groups show
	✓	✓	authentication nis reset
	✓	✓	authentication nis servers add <server-list>
	✓	✓	authentication nis servers del <server-list>
	✓	✓	authentication nis servers reset
✓	✓	✓	authentication nis servers show
✓	✓	✓	authentication nis show
	✓	✓	authentication nis status
	✓	✓	autosupport add <email-list>
	✓	✓	autosupport del <email-list>
	✓	✓	autosupport reset all
	✓	✓	autosupport reset schedule
	✓	✓	autosupport reset support-list
✓	✓	✓	autosupport send [<email-addr>] [cmd "<cmd>"]
	✓	✓	autosupport set schedule [daily | never | <day(s)>] <time>
✓	✓	✓	autosupport show all
✓	✓	✓	autosupport show history
✓	✓	✓	autosupport show report
✓	✓	✓	autosupport show schedule
✓	✓	✓	autosupport show support-list
✓	✓	✓	autosupport test [<email-addr>]
	✓	✓	cifs add /backup <client-list>
	✓	✓	cifs add /ddvar <client-list>
	✓	✓	cifs del /backup <client-list>

User	Admin	SE	Command
	✓	✓	cifs del /ddvar <client-list>
	✓	✓	cifs disable
	✓	✓	cifs enable
	✓	✓	cifs hosts add <ipaddr> <host-list>
	✓	✓	cifs hosts del <ipaddr>
	✓	✓	cifs hosts reset
	✓	✓	cifs hosts show
✓	✓	✓	cifs nb-lookup <netbios-name>
	✓	✓	cifs option reset <name>
	✓	✓	cifs option set <name> <value>
✓	✓	✓	cifs option show
	✓	✓	cifs reset authentication
	✓	✓	cifs reset clients
	✓	✓	cifs reset nb-hostname
	✓	✓	cifs reset wins-server
	✓	✓	cifs set authentication active-directory <realm> { [<pdc> [<bdc>]] | * }
	✓	✓	cifs set authentication domain <domain> [[<pdc> [<bdc>]] | *]
	✓	✓	cifs set authentication workgroup <workgroup>
	✓	✓	cifs set nb-hostname <nb-hostname>
	✓	✓	cifs set wins-server <ipaddr>
	✓	✓	cifs share create <share> path <path> { max-connections <max connections> | clients <clients> | browsing <enabled|disabled> | writeable <enabled|disabled>| users <users> | comment <comment>}
	✓	✓	cifs share destroy <share>
	✓	✓	cifs share disable <share>
	✓	✓	cifs share enable <share>
	✓	✓	cifs share modify <share> { max-connections <max connections> | clients <clients> | browsing <enabled|disabled> | writeable <enabled|disabled>| users <users> | comment <comment>}
✓	✓	✓	cifs share show [<share>]
✓	✓	✓	cifs show active
✓	✓	✓	cifs show clients
✓	✓	✓	cifs show config
✓	✓	✓	cifs show detailed-stats
✓	✓	✓	cifs show stats
✓	✓	✓	cifs status
	✓	✓	cifs troubleshooting group <groupname> | <gid> | <SID>
	✓	✓	cifs troubleshooting list-groups

User	Admin	SE	Command
	✓	✓	cifs troubleshooting list-users
	✓	✓	cifs troubleshooting performance
	✓	✓	cifs troubleshooting user <username> | <uid> | <SID>
✓	✓	✓	config dump
	✓	✓	config reset location
	✓	✓	config reset mailserver
	✓	✓	config reset timezone
	✓	✓	config set admin-email <email-addr>
	✓	✓	config set admin-host <host>
	✓	✓	config set location "<location>"
	✓	✓	config set mailserver <host>
	✓	✓	config set timezone <zonename>
	✓	✓	config setup
✓	✓	✓	config show admin-email
✓	✓	✓	config show admin-host
✓	✓	✓	config show all
✓	✓	✓	config show location
✓	✓	✓	config show mailserver
✓	✓	✓	config show timezone
	✓	✓	disk add dev<disk-id> | enclosure <enclosure-id> [spindle-group <1-16>]
	✓	✓	disk beacon <enclosure-id>.<disk-id>
	✓	✓	disk expand
	✓	✓	disk fail <enclosure-id>.<disk-id>
	✓	✓	disk multipath failback
	✓	✓	disk multipath option reset {monitor | auto-failback}
	✓	✓	disk multipath option set auto-failback {enabled | disabled}
	✓	✓	disk multipath option set monitor {enabled | disabled}
✓	✓	✓	disk multipath option show
	✓	✓	disk multipath reset stats
	✓	✓	disk multipath resume port <port>
✓	✓	✓	disk multipath show history
✓	✓	✓	disk multipath show stats [enclosure <enc-id>]
✓	✓	✓	disk multipath status [<port-id>]
	✓	✓	disk multipath suspend port <port>
✓	✓	✓	disk port show {stats | summary}

User	Admin	SE	Command
	✓	✓	disk rescan
	✓	✓	disk reset performance
	✓	✓	disk set dev<disk-id> spindle-group <1-16>
✓	✓	✓	disk show detailed-raid-info
✓	✓	✓	disk show failure-history
✓	✓	✓	disk show hardware
✓	✓	✓	disk show performance
✓	✓	✓	disk show raid-info
✓	✓	✓	disk show reliability-data
		✓	disk show reservation
✓	✓	✓	disk status
	✓	✓	disk unfail <enclosure-id>.<disk-id>
	✓	✓	enclosure beacon <enclosure>
✓	✓	✓	enclosure show all [<enclosure>]
✓	✓	✓	enclosure show fans [<enclosure>]
✓	✓	✓	enclosure show powersupply [<enclosure>]
✓	✓	✓	enclosure show summary
✓	✓	✓	enclosure show temperature-sensors [<enclosure>]
✓	✓	✓	enclosure show topology
	✓	✓	enclosure test topology <port> duration <minutes>
	✓	✓	filesys clean reset {schedule | throttle | all}
	✓	✓	filesys clean set schedule [daily | monthly | never] <day(s)> <time>
	✓	✓	filesys clean set throttle <percent>
✓	✓	✓	filesys clean show config
✓	✓	✓	filesys clean show schedule
✓	✓	✓	filesys clean show throttle
	✓	✓	filesys clean start
✓	✓	✓	filesys clean status
	✓	✓	filesys clean stop
	✓	✓	filesys clean watch
	✓		filesys destroy [and-zero][and-shrink]
	✓	✓	filesys disable
	✓	✓	filesys enable
✓	✓	✓	filesys fastcopy source <src> destination <dest>
		✓	filesys index merge

User	Admin	SE	Command
	✓	✓	filesys option disable report-replica-as-writable
	✓	✓	filesys option enable report-replica-as-writable
	✓	✓	filesys option reset {local-compression-type | low-bw-optim | marker-type | report-replica-as-writable | global-compression-type | staging-reserve | staging-clean | staging-delete-suspend}
	✓	✓	filesys option set global-compression-type {1 | 9}
	✓	✓	filesys option set local-compression-type {none | lz | gzfast | gz}
		✓	filesys option set low-bw-optim {enabled | auto}
	✓	✓	filesys option set marker-type {auto | nw1 | cv1 | tsm1 | tsm2 | eti1 | hpdp1 | besr1 | ssrt1 | ism1 | none}
		✓	filesys option set staging-clean <percent>
		✓	filesys option set staging-delete-suspend <percent>
	✓	✓	filesys option set staging-reserve <percent>
✓	✓	✓	filesys option show {local-compression-type | low-bw-optim | marker-type | report-replica-as-writable | global-compression-type | staging-reserve | staging-clean | staging-delete-suspend}
		✓	filesys reset stats
	✓	✓	filesys restart
	✓	✓	filesys retention-lock disable
	✓	✓	filesys retention-lock enable
	✓	✓	filesys retention-lock option reset {min-retention-period | max-retention-period}
	✓	✓	filesys retention-lock option set {min-retention-period | max-retention-period} <period>
✓	✓	✓	filesys retention-lock option show {min-retention-period | max-retention-period}
	✓	✓	filesys retention-lock reset <path>
✓	✓	✓	filesys retention-lock status
✓	✓	✓	filesys show compression [<filename>] [last <n> { hours | days }] [no-sync]
✓	✓	✓	filesys show compression [summary | daily | daily-detailed] {[last <n> { hours | days | weeks | months }] | [start <date> [end <date>]]}
		✓	filesys show detailed-stats
✓	✓	✓	filesys show space
		✓	filesys show stats
✓	✓	✓	filesys show uptime
✓	✓	✓	filesys status
✓	✓	✓	filesys sync
	✓	✓	license add <license-code> [<license-code> ...]
	✓	✓	license del <license-feature> | <license-code>
	✓	✓	license reset
	✓	✓	license show [local]
	✓	✓	log host add <host>

User	Admin	SE	Command
	✓	✓	log host del <host>
	✓	✓	log host disable
	✓	✓	log host enable
	✓	✓	log host reset
✓	✓	✓	log host show
✓	✓	✓	log list [<debug>]
✓	✓	✓	log view [<filename>]
✓	✓	✓	log watch [<filename>]
	✓	✓	migration abort
	✓	✓	migration commit
	✓	✓	migration receive source-host <src-hostname>
	✓	✓	migration send {<obj-spec-list> | all} destination-host <dst-hostname>
	✓	✓	migration show stats
	✓	✓	migration status
	✓	✓	migration watch
	✓	✓	ndmp add <filer> user <username> [password <password>]
	✓	✓	ndmp del <filer>
	✓	✓	ndmp get [incremental <level>] <filer>:<src-tree> <dest-file>
	✓	✓	ndmp put [partial <subtree>] <src-file> <filer>:<dest-tree>
	✓	✓	ndmp reset filers
	✓	✓	ndmp show filers
	✓	✓	ndmp status
	✓	✓	ndmp stop <process-number>
	✓	✓	ndmp stop all
	✓	✓	ndmp test <filer>
	✓	✓	net aggregate add <virtual-ifname> mode {roundrobin | xor-L2 | xor-L3L4} interfaces <physical-ifname-list>
	✓	✓	net aggregate del <virtual-ifname> interfaces <physical-ifname-list>
	✓	✓	net aggregate reset <virtual-ifname>
✓	✓	✓	net aggregate show
	✓	✓	net config <ifname> [<ipaddr>] [netmask <mask>] [dhcp {yes | no}] [up | down] [mtu {<size> | default}] [autoneg] [duplex {full | half} speed {10 | 100 | 1000}]
	✓	✓	net config <ifname> type {none | management | data | replication | cluster | "data,replication" }]
	✓	✓	net ddns add <ifname-list | all>
	✓	✓	net ddns del <ifname-list | all>
	✓	✓	net ddns disable

User	Admin	SE	Command
	✓	✓	net ddns enable
	✓	✓	net ddns register
	✓	✓	net ddns reset
✓	✓	✓	net ddns show
✓	✓	✓	net ddns status
	✓	✓	net disable <ifname>
	✓	✓	net enable <ifname>
	✓	✓	net failover add <virtual-ifname> interfaces <physical-ifname-list> [primary <physical-ifname>]
	✓	✓	net failover del <virtual-ifname> interfaces <physical-ifname-list>
	✓	✓	net failover modify <virtual-ifname> primary {<physical-ifname> | "none"}
	✓	✓	net failover reset <virtual-ifname>
✓	✓	✓	net failover show
	✓	✓	net hosts add <ipaddr> <host-list>
	✓	✓	net hosts del <ipaddr>
	✓	✓	net hosts reset
	✓	✓	net hosts show
	✓	✓	net iperf client <server-host> [port <port>] [window-size <bytes>] [data {random|default}] [interval <secs>] [{transmit-size <bytes> | duration <secs>}]
	✓	✓	net iperf server [port <port>] [window-size <bytes>]
	✓	✓	net lookup {<ipaddr> | <hostname>}
		✓	net option reset <name>
		✓	net option set <name> <value>
		✓	net option show
✓	✓	✓	net ping <host> [broadcast] [count <n>] [interface <ifname>]
	✓	✓	net reset dns
	✓	✓	net reset domainname
	✓	✓	net reset hostname
		✓	net rpcinfo [-p hostname]
	✓	✓	net set dns <ipaddr-list>
	✓	✓	net set domainname <name>
	✓	✓	net set hostname <host>
✓	✓	✓	net show all
✓	✓	✓	net show config [<ifname>]
✓	✓	✓	net show dns
✓	✓	✓	net show domainname

User	Admin	SE	Command
✓	✓	✓	net show hardware
✓	✓	✓	net show hostname
✓	✓	✓	net show settings
✓	✓	✓	net show stats [all | interfaces | listening | route | statistics]
	✓	✓	net tcpdump capture <filename> [interface <iface>] [{host <host> | net <net> [mask <mask>]}] [port <port>] [snaplen <bytes>]
	✓	✓	net tcpdump del {<filename> | all}
	✓	✓	nfs add <path> <client-list> [(<option-list>)]
	✓	✓	nfs del <path> <client-list>
	✓	✓	nfs disable
	✓	✓	nfs enable
	✓	✓	nfs reset clients
		✓	nfs reset mountd-port
		✓	nfs reset server-port
	✓	✓	nfs reset stats
		✓	nfs set mountd-port <port>
		✓	nfs set server-port <port>
✓	✓	✓	nfs show active
✓	✓	✓	nfs show clients
✓	✓	✓	nfs show detailed-stats
	✓	✓	nfs show histogram [<op>]
		✓	nfs show port
✓	✓	✓	nfs show stats
✓	✓	✓	nfs status
	✓	✓	ntp add timeserver <time server list>
	✓	✓	ntp del timeserver <time server list>
	✓	✓	ntp disable
	✓	✓	ntp enable
	✓	✓	ntp reset
	✓	✓	ntp reset timeservers
✓	✓	✓	ntp show config
✓	✓	✓	ntp status
	✓	✓	ost destroy
	✓	✓	ost disable
	✓	✓	ost enable

User	Admin	SE	Command
	✓	✓	ost lsu create <lsu-name>
	✓	✓	ost lsu delete <lsu-name>
✓	✓	✓	ost lsu show [compression] [<lsu-name>]
	✓	✓	ost opt-dup option reset low-bw-optim
	✓	✓	ost opt-dup option set low-bw-optim {enabled | disabled}
✓	✓	✓	ost opt-dup option show [low-bw-optim]
✓	✓	✓	ost opt-dup show active
✓	✓	✓	ost opt-dup show history duration <duration>{day | hr} interval <interval>{hr}
✓	✓	✓	ost opt-dup show image-history duration <duration>{day | hr}
	✓	✓	ost reset stats
	✓	✓	ost reset user-name
	✓	✓	ost set user-name <user-name>
✓	✓	✓	ost show connections
✓	✓	✓	ost show histogram [<op>]
✓	✓	✓	ost show image-duplication active
✓	✓	✓	ost show image-duplication history duration <duration>{day | hr} interval <interval>{hr}
✓	✓	✓	ost show image-duplication image-history duration <duration>{day | hr}
✓	✓	✓	ost show stats [interval <seconds>]
✓	✓	✓	ost show user-name
✓	✓	✓	ost status
	✓	✓	perf disable trace <event-regexp>
	✓	✓	perf enable trace <event-regexp>
	✓	✓	perf start stats
	✓	✓	perf start trace [allow-wrap]
	✓	✓	perf status trace <event-regexp>
	✓	✓	perf stop stats
	✓	✓	perf stop trace <trace_filename>
		✓	reg check [<namespace-list>]
		✓	reg removekey <key>
	✓	✓	reg set <key> = <value>
		✓	reg set reg-default <key>
		✓	reg set unset-defaults
		✓	reg setraw <key> = <value>
✓	✓	✓	reg show [nokey] <key>
		✓	reg show defaults

User	Admin	SE	Command
		✓	reg show obsolete
	✓	✓	reg show stats
		✓	reg showraw [nokey]
	✓	✓	replication abort recover <destination>
	✓	✓	replication abort resync <destination>
	✓	✓	replication add source <source> destination <destination> [low-bw-optim {enabled | disabled}]
	✓	✓	replication break {<destination> | all}
	✓	✓	replication disable {<destination> | all}
		✓	replication dump
	✓	✓	replication enable {<destination> | all}
	✓	✓	replication initialize <destination>
	✓	✓	replication modify <destination> {source-host | destination-host} <new-host-name>
	✓	✓	replication modify <destination> connection-host <new-host-name> [port <port>]
	✓	✓	replication modify <destination> low-bw-optim {enabled | disabled}
	✓	✓	replication option reset {bandwidth | delay | listen-port}
	✓	✓	replication option set bandwidth <rate>
	✓	✓	replication option set delay <value>
	✓	✓	replication option set listen-port <value>
	✓	✓	replication option show
	✓	✓	replication reauth <destination>
	✓	✓	replication recover <destination>
	✓	✓	replication resync <destination>
✓	✓	✓	replication show config [<destination> | all]
✓	✓	✓	replication show detailed-history {<obj-spec-list> | all} [duration <duration>{hr | min}] [interval <interval>{hr | min}]
✓	✓	✓	replication show detailed-stats [<destination> | all]
✓	✓	✓	replication show history {<obj-spec-list> | all} [duration <duration>{hr | min}] [interval <interval>{hr | min}]
✓	✓	✓	replication show performance {<obj-spec-list> | all} [interval <sec>] [count <count>]
✓	✓	✓	replication show stats [<destination> | all]
✓	✓	✓	replication status [<destination> | all]
✓	✓	✓	replication sync [<destination>]
	✓	✓	replication throttle add <sched-spec> <rate>
	✓	✓	replication throttle del <sched-spec>
	✓	✓	replication throttle reset {current | override | schedule | all}
	✓	✓	replication throttle set current <rate>

User	Admin	SE	Command
	✓	✓	replication throttle set override <rate>
✓	✓	✓	replication throttle show [KiB]
	✓	✓	replication watch <destination>
	✓	✓	route add <route spec>
	✓	✓	route del <ipaddr>
	✓	✓	route reset gateway
	✓	✓	route set gateway <ipaddr>
✓	✓	✓	route show config
✓	✓	✓	route show gateway
✓	✓	✓	route show table
✓	✓	✓	route trace <host>
		✓	session delete key <session id> <session key>
		✓	session reset data <session id>
		✓	session restart
		✓	session show all
		✓	session show data <session id>
	✓	✓	snapshot add schedule <name> [days <days>] time <time> [,<time>...] [retention <period>]
✓	✓	✓	snapshot add schedule <name> [days <days>] time <time> every <mins> [retention <period>]
✓	✓	✓	snapshot add schedule <name> [days <days>] time <time>-<time> [every <hrs | mins>
	✓	✓	snapshot create <snapshot> [retention {<date> | <period>]
	✓	✓	snapshot del schedule [<name> | all]
	✓	✓	snapshot expire <snapshot> [retention {<date> | <period> | forever}]
✓	✓	✓	snapshot list
	✓	✓	snapshot modify schedule <name> {[days <days>] | time <time> [,<time>...] | [retention <period>]}
✓	✓	✓	snapshot modify schedule <name> {[days <days>] | time <time> every <mins> | [retention <period>]}
✓	✓	✓	snapshot modify schedule <name> {[days <days>] | time <time>-<ti
	✓	✓	snapshot rename <snapshot> <new-name>
	✓	✓	snapshot reset schedule
✓	✓	✓	snapshot show schedule <name>
	✓	✓	snmp add ro-community <community-string>
	✓	✓	snmp add rw-community <community-string>
	✓	✓	snmp add trap-host <host-name>[:port]
	✓	✓	snmp del ro-community <community-string>
	✓	✓	snmp del rw-community <community-string>
	✓	✓	snmp del trap-host <host-name>

User	Admin	SE	Command
	✓	✓	snmp disable
	✓	✓	snmp enable
	✓	✓	snmp reset
	✓	✓	snmp reset ro-communities
	✓	✓	snmp reset rw-communities
	✓	✓	snmp reset sysContact
	✓	✓	snmp reset sysLocation
	✓	✓	snmp reset trap-hosts
	✓	✓	snmp set sysContact <sysContact>
	✓	✓	snmp set sysLocation <sysLocation>
✓	✓	✓	snmp show config
	✓	✓	snmp show ro-communities
	✓	✓	snmp show rw-communities
✓	✓	✓	snmp show sysContact
✓	✓	✓	snmp show sysLocation
✓	✓	✓	snmp show trap-hosts
✓	✓	✓	snmp status
	✓	✓	support upload {bundle [<file-list>] | traces | <file-list>}
	✓	✓	system fw_upgrade <file>
	✓	✓	system headswap
	✓	✓	system ipmi config {bmc0 | bmc1} ipaddr <ipaddr> netmask <mask> gateway <gateway>
✓	✓	✓	system ipmi show {bmc0 | bmc1}
		✓	system ipmi status [local | remote <address> <user> <password>]
	✓	✓	system option reset {login-banner}
	✓	✓	system option set {login-banner <file>}
	✓	✓	system option show
	✓	✓	system poweroff
	✓	✓	system reboot
	✓	✓	system sanitize abort
	✓	✓	system sanitize start
	✓	✓	system sanitize status
	✓	✓	system sanitize watch
	✓	✓	system set date <MMDDhhmm[[CC]YY]>
✓	✓	✓	system show all
✓	✓	✓	system show burn [duration <duration> {wk | day | hr}] [interval <interval> {wk | day | hr}]

User	Admin	SE	Command
✓	✓	✓	system show date
✓	✓	✓	system show detailed-stats [local] [stop | start | ([interval <nsecs>] [count] <count>)]
✓	✓	✓	system show detailed-version
✓	✓	✓	system show hardware
✓	✓	✓	system show meminfo
✓	✓	✓	system show modelno
✓	✓	✓	system show nvram
✓	✓	✓	system show performance [local] [raw | fsop] [<duration> {hr | min | sec} [<interval> {hr | min | sec}]]
✓	✓	✓	system show ports
✓	✓	✓	system show serialno
✓	✓	✓	system show stats [local] [stop | start | ([interval] <nsecs> [count] <count>)]
✓	✓	✓	system show uptime
✓	✓	✓	system show version
✓	✓	✓	system status
	✓	✓	system upgrade <file>
	✓	✓	user add <user> [password <password>] [priv {admin | user}] [min-days-between-change <days>] [max-days-between-change <days>] [warn-days-before-expire <days>] [disable-days-after-expire <days>] [disable-date <date>]
✓	✓	✓	user change password [<user>]
	✓	✓	user change priv <user> {admin | user}
	✓	✓	user del <user>
	✓	✓	user disable <user>
	✓	✓	user enable <user> [disable-date <date>]
✓	✓	✓	user password aging option reset { all | [min-days-between-change] [max-days-between-cha
	✓	✓	user password aging option set [min-days-between-change <days>] [max-days-between-change <days>] [warn-days-before-expire <days>] [disable-days-after-expire <days>]
✓	✓	✓	user password aging show [<user>]
	✓	✓	user password strength set {[min-length <length>] [min-char-classes <num_classes>]}
	✓	✓	user password strength show
	✓	✓	user reset
✓	✓	✓	user show active
	✓	✓	user show detailed [<user>]
	✓	✓	user show list
	✓	✓	vtl add <vtl> [model <model>] [slots <num slots>] [caps <num caps>]
	✓	✓	vtl cap add <vtl> [count <number of caps>]
	✓	✓	vtl cap del <vtl> [count <num to del>]

User	Admin	SE	Command
		✓	vtl debug disable
		✓	vtl debug enable [persistent]
	✓	✓	vtl del <vtl>
	✓	✓	vtl disable
	✓	✓	vtl drive add <vtl> [count <num drives>] [model <model>]
	✓	✓	vtl drive del <vtl> drive <drive number> [count <num to del>]
	✓	✓	vtl enable
	✓	✓	vtl export <vtl> {slot | drive | cap} <address> [count <count>]
	✓	✓	vtl group add <group name> initiator <initiator alias or WWPN>
	✓	✓	vtl group add <group name> vtl <vtl name> {all | changer | drive <drive list>} [lun <lun>] [primary-port {all | none | <port list>}] [secondary-port {all | none | <port list>}]
	✓	✓	vtl group create <group_name>
	✓	✓	vtl group del <group name> initiator <initiator alias or WWPN>
	✓	✓	vtl group del <group name> vtl <vtl name> {all | changer | drive <drive list>}
	✓	✓	vtl group destroy <group_name>
	✓	✓	vtl group modify <group name> vtl <vtl name> {all | changer [lun <lun>] | drive <drive> [lun <lun>]} [primary-port {all | none | <port list>}] [secondary-port {all | none | <port list>}]
	✓	✓	vtl group rename <src_group_name> <dst_group_name>
	✓	✓	vtl group show [all | vtl <vtl> | <group_name>]
	✓	✓	vtl group use <group name> [vtl <vtl name> {all | changer | drive <drive list>}] {primary | secondary}
	✓	✓	vtl import <vtl> barcode <barcode> [count <count>] [pool <pool name>] [element <drive | cap | slot>] [address <addr>]
	✓	✓	vtl initiator reset address-method initiator <initiator alias or wwpn>
	✓	✓	vtl initiator reset alias <alias name>
	✓	✓	vtl initiator set address-method { auto | vsa } initiator <initiator alias or wwpn>
	✓	✓	vtl initiator set alias <alias name> wwpn <wwpn>
	✓	✓	vtl initiator show [initiator <initiator> | port <port>]
	✓	✓	vtl option disable <option name>
	✓	✓	vtl option enable <option name>
	✓	✓	vtl option reset <option name>
	✓	✓	vtl option set option-name <value>
	✓	✓	vtl option show <option name> | all
	✓	✓	vtl pool add <pool name>
	✓	✓	vtl pool del <pool name>
	✓	✓	vtl pool show {all | <pool name>}
	✓	✓	vtl port disable {all | <port list>}

User	Admin	SE	Command
	✓	✓	vtl port enable {all | <port list>}
	✓	✓	vtl port option {enable | disable | reset} fcp2-retry [port {<port-list> | all}]
	✓	✓	vtl port option show [fcp2-retry [port {<port-list> | all}]]
	✓	✓	vtl port show detailed-stats
	✓	✓	vtl port show hardware
	✓	✓	vtl port show stats [port {<port-list> | all}] [interval <secs>] [count <count>]
	✓	✓	vtl port show summary
	✓	✓	vtl reset hba
	✓	✓	vtl show config [<vtl>]
	✓	✓	vtl show element-address [<vtl>]
	✓	✓	vtl show stats <vtl> [drive {<drive-list> | all}] [port {<port-list> | all}] [interval <secs>] [count <count>]
	✓	✓	vtl slot add <vtl> [count <numer of slots>]
	✓	✓	vtl slot del <vtl> [count <num to del>]
	✓	✓	vtl status
	✓	✓	vtl tape add <barcode> [capacity <capacity>] [count <count>] [pool <poolname>]
	✓	✓	vtl tape del <barcode> [count <count>] [pool <poolname>]
	✓	✓	vtl tape modify <barcode> [count <count>] [pool <poolname>] writeprotect {on | off}
	✓	✓	vtl tape move <vtl> source {slot | drive | cap} <src-address> destination {slot | drive | cap} <dest-address>
	✓	✓	vtl tape move barcode <barcode> [count <count>] source <src-pool> destination <dest-pool>
	✓	✓	vtl tape show {all | pool <pool> | vault | <vtl>} [summary] [count <count>] [barcode <barcode>] [sort-by {barcode | pool | location | state | capacity | usage | percentfull | compression | modtime} [{ascending | descending}]]

TOE Security Functional Requirements Satisfied: FDP_ACC.2, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3.

7 Rationale

7.1 Conformance Claims Rationale

There are no Protection Profile conformance claims associated with this Security Target.

7.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 7.2.1, 7.2.2, and 7.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

7.2.1 Security Objectives Rationale Relating to Threats

Table 13 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_STORAGE Data could become corrupted due to incorrect system access by TOE users or non-TOE users, or could be stored inefficiently.	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.DATA_OPTIMIZATION The TOE must disallow the duplication of stored data by identifying and removing previously-stored segments.	O.DATA_OPTIMIZATION mitigates this threat by disallowing the duplication of data to be stored which would inhibit TOE efficiency.
	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 (under the control of a TOE user or a non-TOE user) 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.AUDIT The TOE must provide a means of detecting and logging security-relevant events, and must provide administrators with a means of reviewing the audit log.	O.AUDIT ensures that administrators can determine that improper data access or configuration change attempts are being performed.

Threats	Objectives	Rationale
	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.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the TOE.	OE.SECURE_COMMUNICATIONS 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 TOE environment must provide servers configured per current corporate security policy guidelines to communicate with the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that each server connected to the TOE operates securely and does not intentionally compromise 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.

7.2.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

7.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 – Assumptions:Objectives Mapping

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.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.MANAGE	OE.MANAGE	Those responsible for the TOE will provide competent individuals to

Assumptions	Objectives	Rationale
There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	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.

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.

7.3 Rationale for Extended Security Functional Requirements

A family of EXT_FDD: User Data De-Duplication requirements was created to specifically address the data de-duplication functionality of the TOE. The FDP_RIP.1 (Subset residual information protection) SFR was used as a model for creating this class. These requirements have no dependencies since the stated requirements embody all of the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

An extended SFR called EXT_FRU_RLP.1: Minimum and maximum retention lock periods was created to address the retention lock functionality of the TOE. The FRU_RSA.2 SFR (Minimum and maximum quotas) was used as a model for creating this SFR. This requirement has no dependencies since the stated requirement embodies all of the necessary functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

7.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

7.5 Security Requirements Rationale

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

7.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method	FIA_ATD.1 User attribute definition	The TOE stores administrative credentials for each user.

Objective	Requirements Addressing the Objective	Rationale
for administrative control of the TOE.	FIA_UAU.2 User authentication before any action	The TOE shall successfully authenticate each administrator before allowing her to manage the TOE.
	FIA_UID.2 User identification before any action	The TOE will properly identify and authenticate all administrators.
	FMT_MOF.1 Management of security functions behaviour	The ability to modify the behaviour of the TOE security functions is granted only to certain roles managed by the TOE.
	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.3 Static attribute initialisation	Permissive values for data access are provided, and the TOE administrator can changed them when a data object is created.
	FMT_MTD.1 Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 specifies each of the management functions that are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of the TOE.
	FTA_SSL.3 TSF-initiated termination	The TOE terminates inactive administrative sessions after thirty minutes.
O.AUDIT The TOE must provide a means of detecting and logging security-relevant events, and must provide administrators with a means of reviewing the audit log.	FAU_GEN.1 Audit data generation	The TOE generates audit records of all administrative commands.
	FAU_GEN.2 User identity association	The TOE associates each audit record with the identity of the user that caused the event that was logged.
	FAU_SAR.1 Audit review	The TOE allows authorized administrators to review the audit log.
	FAU_SAR.2 Restricted audit review	
	FDP_ACC.2 Complete access control	The TOE enforces an access control policy that restricts the viewing of audit data to only authorized

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1 Security attribute based access control	administrators.
O.DATA_OPTIMIZATION The TOE must disallow the duplication of stored data by identifying and removing previously-stored segments.	EXT_FDD_DDR.1 Duplicate data removal	The TOE identifies and removes segments of data sent to it for storage if those segments are already present in the datastore.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.2 Complete access control	The TOE has an access control policy that ensures that only authorized servers can gain access to and manage the TOE.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to the TOE.
	FDP_IFC.2 Complete information flow control	The TOE has an information flow control policy that ensures that only authorized servers can gain access to stored user data.
	FDP_IFF.1 Simple security attributes	The TOE provides information flow control functionality to manage access to the stored data managed by the TOE.
	FDP_RIP.1 Subset residual information protection	The TOE ensures that the content of deleted user data is not re-used when the storage space previously occupied by that data is re-allocated for storage of different user data.
	FDP_SDI.2 Stored data integrity monitoring and action	The TOE protects the stored user data from integrity errors.
	EXT_FRU_RLP.1 Minimum and maximum retention lock periods	The TOE protects locked files from modification or deletion during the period for which a retention lock has been defined.

7.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE controls access to backup data for devices which might be deployed in a hostile environment, the TOE itself is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the system 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.

7.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 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 16 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included since the TOE environment (the underlying hardware) provides the timestamps that are used by the TOE. Environmental Objective OE.TIME satisfies this requirement.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
EXT_FDD_DDR.1	None	✓	
FDP_ACC.2	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	FDP_ACC.2 is hierarchical to FDP_ACC.1.
	FMT_MSA.3	✓	
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	FDP_IFC.2 is hierarchical to FDP_IFC.1.
	FMT_MSA.3	✓	
FDP_RIP.1	None	✓	
FDP_SDI.2	None	✓	
FIA_ATD.1	None	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1.

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UID.2	None	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	FDP_ACC.2, which is hierarchical to FDP_ACF.1, deals with the management of the TOE.
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1.
EXT_FRU_RLP.1	None	✓	
FTA_SSL.3	None	✓	

8 Acronyms

Table 17 – Acronyms

Acronym	Definition
CC	Common Criteria
CIFS	Common Internet Filesystem
CLI	Command Line Interface
DD OS	Data Domain Operating System
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
NFS	Network File System
NIS	Network Information Service
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Inexpensive Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SE	Systems Engineer
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality