EMC® Data Domain® 5.5

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1937-000-D102
Version: 1.0
30 June 2016

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, Ltd.
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the TOE (Target of Evaluation), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional and assurance requirements.

Section 8, Acronyms, defines the acronyms used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title: EMC® Data Domain® 5.5 Security Target

ST Version: 1.0

ST Date: 30 June 2016

1.3 TOE REFERENCE

TOE Identification: EMC® Data Domain® version 5.5.4.0-525810

TOE Developer: EMC Corporation

TOE Type: Disaster recovery (operating system)

The TOE consists of both hardware and software. The hardware models identified in Table 1 below are uniquely referenced by product name, model number, and software build number.

1.3.1 Software Build

The software build for all models is the EMC® Data Domain Operating System (DD OS) version 5.5.4.0-525810.

1.3.2 Hardware Models

The TOE is comprised of the following hardware models:

Hardware Model	Installation and Setup Guide	Software
DD990	EMC® Data Domain DD990 Storage System Installation and Setup Guide	EMC® DD OS (Data Domain Operating System) version 5.5.4.0-525810.
DD670	EMC® Data Domain DD670 Storage System Installation and Setup Guide	
DD860	EMC® Data Domain DD860 Storage System Installation and Setup Guide	
DD890	EMC® Data Domain DD890 Storage System Installation and Setup Guide	
DD640	EMC® Data Domain DD640 Storage System Installation and Setup Guide	
DD140	EMC® Data Domain DD140 Storage System Installation and Setup Guide	
DD610	EMC® Data Domain DD610 Storage System Installation and Setup Guide	
DD630	EMC® Data Domain DD630 Storage System Installation and Setup Guide	
DD160	EMC® Data Domain DD160 Storage System Installation and Setup Guide	
DD620	EMC® Data Domain DD620 Storage System Installation and Setup Guide	
DD880	EMC® Data Domain DD880 Storage System Installation and Setup Guide	

Hardware Model	Installation and Setup Guide	Software
DD2200	EMC® Data Domain DD2200 Storage System Installation and Setup Guide	
DD2500	EMC® Data Domain DD2500 Storage System Installation and Setup Guide	
DD4200	EMC® Data Domain DD4200 Storage System Installation and Setup Guide	
DD4500	EMC® Data Domain DD4500 Storage System Installation and Setup Guide	
DD7200	EMC® Data Domain DD7200 Storage System Installation and Setup Guide	

Table 1 – TOE Hardware Models

Documentation for the EMC Data Domain systems operated in Common Criteria mode consists of the standard DD OS version 5.5 documentation set (identified in Section 1.5.4, TOE Guidance) and the relevant Installation and Setup Guide as shown in Table 1.

1.4 TOE OVERVIEW

The TOE is a series of disk-based inline deduplication appliances and gateways that optimize disaster recovery (DR) in the enterprise environment. These devices (known as the EMC Data Domain) vary in storage capacity and data throughput.

EMC Data Domain deduplication technology seamlessly integrates into existing Information Technology (IT) storage infrastructures. It eliminates redundant data from each backup image and stores only unique data thus reducing the amount of physical storage required for backup.

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. Multiple backup servers can share one EMC Data Domain system which is capable of handling multiple simultaneous backup and restore operations.

All systems run the EMC Data Domain Operating System (DD OS). DD OS provides secure administration for TOE configuration, management, and monitoring via command-line interface (CLI) or the EMC Data Domain System Manager (DD System Manager) graphical user interface (GUI). Use of both the CLI and GUI, as well as system events, is audited.

To protect against data loss from software and hardware failures, the EMC Data Domain systems are setup in a double parity RAID 6 (Redundant Array of Independent Disks) configuration and uses NVRAM (Non-Volatile RAM) to keep data synchronized during a hardware or power failure.

The TOE is a software and hardware TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the hardware and software described in Section 1.3. The EMC Data Domain Storage System models are stand-alone appliances.

1.5.1.1 Network Interfaces

In the CC-evaluated configuration of the TOE, secure access to administrative functions is provided through the following network interfaces:

Serial Interface – The serial interface is used to directly connect the TOE to a local management workstation that supports VT100 emulation. The serial port allows access to the TOE via Command Line Interface (CLI). The CLI permits an authorized administrator to configure TOE settings and display hardware status, feature configuration, and operation.

Ethernet Ports – Remote administration may be performed through any Ethernet port that has been configured by an authorized administrator to allow appropriate access for the Graphical User Interface (GUI) and CLI. When connected to a remote management workstation, these ports allow an authorized administrator to configure and monitor TOE features and settings.

1.5.2 TOE Boundary

Figure 1 represents the EMC Data Domain system in its evaluated configuration:

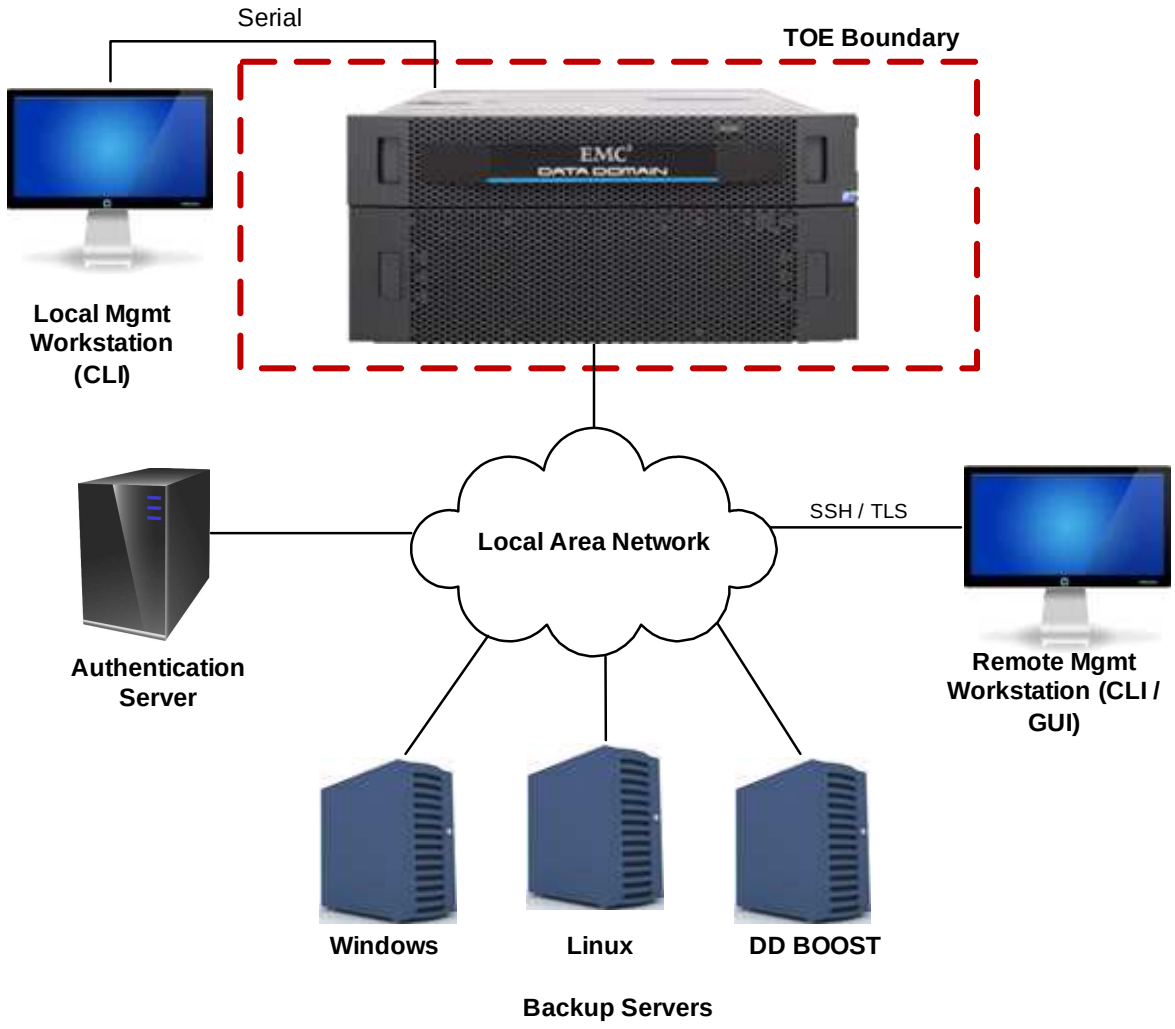

Figure 1 – TOE Diagram

1.5.3 TOE Environment

The following hardware and network components are required for operation of the TOE in the evaluated configuration:

Non-TOE Component	Hardware / Software Requirements
Local Management Workstation	General purpose computing platform that supports VT100 emulation.
Remote Management Workstation	General purpose computing platform that supports the Windows 7 operating system.
Windows Authentication Server	General purpose computing platform that supports the Windows 2008 R2 with Active Directory.

Non-TOE Component	Hardware / Software Requirements
Windows Backup Server	General purpose storage server supporting the CIFS client protocol. Windows 7 is used for this evaluation.
Linux Backup Server	General purpose storage server supporting the NFS client protocol. RHEL 6 is used for this evaluation.
DD Boost Backup Server	RHEL 6 hosting Netbackup 7.6 with DD BOOST 3.0.3.0 plugin is used for this evaluation.

Table 2 – Non-TOE Hardware and Software

1.5.4 TOE Guidance

In addition to the Installation and Setup guides identified in Table 1 (Section 1.3.2) the TOE includes the following guidance documentation:

- EMC® Data Domain Operating System Release notes, Version 5.5
- EMC® Data Domain Operating System Administration Guide, Version 5.5
- EMC® Data Domain Operating System Initial Configuration Guide, Version 5.5
- EMC® Data Domain Operating System Command Reference Guide, Version 5.5

1.5.5 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. The following breakdown also provides the description of the security features of the TOE, and follows the security functional classes described in Section 6.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events including system usage and administrative access events.
User Data Protection	The TOE provides role-based access control capabilities to ensure that only authorized users are able to administer the TOE. The TOE controls access from servers to backup and recovery resources, and provides deduplication functionality to limit the disk size required to support these functions. RAID 6 ensures the integrity of stored data.
Identification and Authentication	Users must identify and authenticate prior to accessing the TOE. Obscured feedback is provided during authentication.

Functional Classes	Description
Security Management	The TOE provides management capabilities locally via Command Line Interface and remotely via Web-Based GUI and CLI. Management functions allow authorized administrators to configure users, roles, and client access attributes.
Protection of the TSF	The TOE preserves the secure state in the event of up to two disk failures. The TOE provides reliable time stamps for auditable events.

Table 3 – Logical Scope of the TOE

1.5.6 Functionality Excluded from the Evaluated Configuration

1.5.6.1 Excluded TOE Operating Systems

Use of the following operating systems for TOE administration is supported but not included in this evaluation:

- Solaris
- Red Hat Linux
- SuSE Linux
- AIX
- HP-UX
- Oracle Enterprise Linux
- Linux

1.5.6.2 Excluded TOE Interfaces

Use of the following interfaces is not included in this evaluation:

USB Port – All instances of the TOE are equipped with a Universal Serial Bus (USB) port that may be used by an authorized administrator for DD OS system maintenance and updates. This port may also be used for connecting a USB keyboard during configuration.

FTP/FTPS – Authorized users can view system logs and alerts by accessing the TOE via File Transfer Protocol/File Transfer Protocol Secure (FTP/FTPS).

PS/2 Ports – Some older versions of the TOE support direct system access using a keyboard and mouse through Personal System/2 (PS/2) ports.

Telnet – Use of Telnet protocol is not permitted in the evaluated configuration of the TOE.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, to have extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile.

Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters, and no physical access to the TOE.

Threat	Description
T.ACCESS	An unauthorized person may attempt to bypass the TOE security policy to access protected resources.
T.ACCOUNT	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.
T.AUDACC	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment within an organization. The TOE must address the organizational security policies described in Table 5.

OSP	Description
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected to ensure that all users are held accountable for their actions.
P.MANAGE	The TOE shall be managed only by authorized administrators.
P.DUPDATA	The TOE must optimize performance and storage capacity by reducing the storage of duplicate data segments.

OSP	Description
P.PROTECT	The TOE shall incorporate mechanisms to protect against potential loss or disclosure of the data it has been entrusted to store.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

Assumptions describe the security aspects of the intended environment for the evaluated TOE. The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.LOCATE	During normal operation, the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security information it contains.
A.NOEVIL	Authorized administrators are non-hostile, appropriately trained, and follow all TOE guidance documentation.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide a means of logging security related events.
O.DATAOPT	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.OBSFEED	The TOE must provide obscured feedback to users while authentication is in progress.
O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack when in use.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.ACCOUNT	T.AUDACC	P.DETECT	P.DUPDATA	P.MANAGE	P.PROTECT	A.LOCATE	A.MANAGE	A.NOEVIL
O.ACCESS	X	X				X				
O.ADMIN	X	X	X			X				
O.AUDIT			X	X						
O.DATAOPT					X					
O.IDAUTH	X	X		X		X				
O.OBSFEED	X	X								
O.PROTECT							X			
OE.ADMIN									X	X
OE.PHYSICAL								X		

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat: **T.ACCESS**	An unauthorized person may attempt to bypass the TOE security policy to access protected resources.	
Objectives:	O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.OBSFEED	The TOE must provide protected feedback to users while authentication is in progress.
Rationale:	O.ACCESS helps to mitigate the threat by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE is restricted to authorized administrators. O.IDAUTH mitigates this threat by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE. O.OBSFEED mitigates this threat by providing users with obscured feedback while authentication is in progress.	

Threat: **T.ACCOUNT**	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.	
Objectives:	O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the

		TOE.
	O.OBSFEED	The TOE must provide protected feedback to users while authentication is in progress.
Rationale:	O.ACCESS helps to mitigate the threat by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.IDAUTH mitigates this threat by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE. O.OBSFEED mitigates this threat by providing users with obscured feedback while authentication is in progress, protecting authentication information from being used by an unauthorized person.	

Threat: **T.AUDACC**	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.AUDIT	The TOE must provide a means of logging security related events.
Rationale:	O.ADMIN helps mitigate this threat by only allowing authorized administrators access to TOE audit functions. O.AUDIT mitigates this threat by ensuring changes to the TSF data are logged.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.DETECT**	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected.	
Objectives:	O.AUDIT	The TOE must provide a means of logging security related events.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to

		the administrative functions and data of the TOE.
Rationale:	O.AUDIT ensures that the use of the TOE is recorded. This may be used to provide evidence of inappropriate activity. O.IDAUTH supports this policy by ensuring that the TOE has a clear identity for any user who may be misusing the TOE.	

Policy: **P.DUPDATA**	The TOE must optimize performance and storage capacity by reducing the storage of duplicate data segments.	
Objectives:	O.DATAOPT	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.
Rationale:	O.DATAOPT supports this policy by ensuring that storage capacity is maximized by eliminating multiple copies of the same data segments.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized administrators.	
Objectives:	O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.ACCESS supports this policy by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN ensures that access to the security functions of the TOE are restricted to authorized administrators. O.IDAUTH supports this policy by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE.	

Policy: P.PROTECT	The TOE shall incorporate mechanisms to protect against potential loss or disclosure of the data it has been entrusted to store.	
Objectives:	O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.
Rationale:	O.PROTECT ensures that the integrity of data it has been entrusted to store is protected from physical component failure or unauthorized access.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: A.LOCATE	During normal operation, the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack when in use.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security information it contains.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.ADMIN supports this assumption by ensuring that multiple competent administrators are given TOE management authority.	

Assumption: A.NOEVIL	Authorized administrators are non-hostile, appropriately trained, and follow all TOE guidance documentation.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.ADMIN supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive, non-hostile, and follow all administrator guidance.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

a. Duplicate data removal (FDP_DDR _EXT.1)

5.1.1 Family FDP_DDR_EXT: Duplicate Data Removal

Duplicate data removal functions involve optimizing data storage 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 data sets. The duplicate data removal family was modeled after FDP_SDI: Stored data integrity.

Family Behaviour

This family defines the requirements for duplicate data removal functionality.

Component Levelling

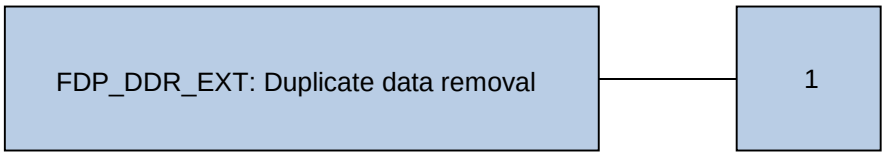

Figure 2 – FDP_DDR_EXT: Duplicate Data Removal Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.1.1 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [assignment: *action to be taken*] before writing new data to a storage container.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements (SARs).

6 SECURITY REQUIREMENTS

This section provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements consist of the following components from Part 2 of the CC and extended components defined in Section 5:

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_DDR_EXT.1	Duplicate data removal
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_SDI.2	Stored data integrity monitoring and action

Class	Identifier	Name
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Management Access Control SFP)
	FMT_MSA.1(2)	Management of security attributes (User Data Information Flow Control SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Management Access Control SFP)
	FMT_MSA.3(2)	Static attribute initialisation (User Data Information Flow Control SFP)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*none*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Management Access Control SFP*] on

[*Subjects: Authorized Administrators;*

Objects: TOE configuration data;

Operations: create, modify, delete].

6.2.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the [*Management Access Control SFP*] to objects based on the following: [

- *Subjects: Authorized Administrators*
  Security Attributes:
  a) User ID
  b) Role

- *Objects: TOE configuration data*
  Security Attributes: None
  ].

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 administrator with the appropriate role can manipulate the TOE configuration*].

FDP_ACF.1.3 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 following additional rules: [*none*].

6.2.2.3 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [*perform a global compression process and eliminate redundant data*] before writing new data to a storage container.

6.2.2.4 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*User Data Information Flow Control SFP*] on

[*Subjects: external servers;*

Information: stored user data;

Operations: read and write].

6.2.2.5 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

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*[1]
  Security Attributes: Identity of the server
- *Information: Stored user data*
  Security Attributes: Directory 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 external server can read and write stored user data if the identity of the external server is associated with the data's directory permissions*].

FDP_IFF.1.3 The TSF shall enforce the [*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*].

6.2.2.6 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

[1] External servers are called 'clients' in the Data Domain user documentation, and are identified by hostname or IP address.

Dependencies: No dependencies.

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

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

Application Note: Stored user data represents the objects for this family.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.2 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*the number of characters typed*] to the user while the authentication is in progress.

6.2.3.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MSA.1(1) Management of security attributes (Management Access Control SFP)

Hierarchical to: No other components.

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

FMT_MSA.1.1(1) The TSF shall enforce the [*Management Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*User ID and role*] to [*authorized administrators*].

6.2.4.2 FMT_MSA.1(2) Management of security attributes (User Data Information Flow Control SFP)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [*User Data Information flow control SFP*] to restrict the ability to [modify, delete, [*create*]] the security attributes [*server identity*] to [*authorized administrators*].

6.2.4.3 FMT_MSA.3(1) Static attribute initialisation (Access control SFP)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Management Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*authorized administrators*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_MSA.3(2) Static attribute initialisation (Information flow control SFP)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*User Data Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*authorized administrators*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) administer user account information;
b) administer TOE configuration functions; and
c) administer user data information flow control rules

].

6.2.4.6 FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

- *Admin*
- *User*
- *Security Officer*
- *Backup Operator*
- *Tenant-Admin*
- *Tenant-User*

].

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

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components

Dependencies: No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*up to two concurrent disk failures*].

6.2.5.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.DATAOPT	O.ENCRYP	O.IDAUTH	O.OBSFEED	O.PROTECT
FAU_GEN.1			X					
FAU_GEN.2			X					
FDP_ACC.1	X	X						
FDP_ACF.1	X	X						
FDP_DDR_EXT.1				X				
FDP_IFC.1								X
FDP_IFF.1								X

	O.ACCESS	O.ADMIN	O.AUDIT	O.DATAOPT	O.ENCRYP	O.IDAUTH	O.OBSFEED	O.PROTECT
FDP_SDI.2								X
FIA_UAU.2	X	X				X		
FIA_UAU.7							X	
FIA_UID.2	X	X				X		
FMT_MSA.1(1)		X						
FMT_MSA.1(2)		X						
FMT_MSA.3(1)		X						
FMT_MSA.3(2)		X						
FMT_SMF.1		X						
FMT_SMR.1		X				X		
FPT_FLS.1								X
FPT_STM.1			X					

Table 11 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action

Rationale:	FDP_ACC.1 meets this objective by enforcing an access control policy to ensure only authorized users can gain access to appropriate TOE functions and data. FDP_ACF.1 meets this objective by enforcing the rules and attributes that govern the access control policy. FIA_UAU.2 meets this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data.

Objective: **O.ADMIN**	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Management Access Control SFP)
	FMT_MSA.1(2)	Management of security attributes (User Data Information Flow SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Management Access Control SFP)
	FMT_MSA.3(2)	Static attribute initialisation (User Data Information Flow Control SFP)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FDP_ACC.1 supports this objective by only allowing authorized administrators access to management functions of the TOE access control policies. FDP_ACF.1 supports this objective by enforcing rules that only allow only users with the appropriate role to manipulate the TOE configuration. FIA_UAU.2 meets this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data.	

	FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data. FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by restricting the ability to manipulate the Management Access Control SFP security attributes to users with the admin and security roles. FMT_MSA.1(2) and FMT_MSA.3(2) support this objective by restricting the ability to manipulate the User Data Information Flow Control SFP security attributes to users with the admin and security roles. FMT_SMF.1 supports this objective by identifying the management functions authorized administrators are able to perform. FMT_SMR.1 meets this objective by supporting a list of authorized roles for the TOE.

Objective: O.AUDIT	The TOE must provide a means of logging security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 supports this objective by generating audit records for auditable events. FAU_GEN.2 supports this objective by associating a user identity with each auditable event generated. FPT_STM.1 provides a time stamp for each auditable event.	

Objective: O.DATAOPT	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.	
Security Functional Requirements:	FDP_DDR_EXT.1	Duplicate data removal
Rationale:	FDP_DDR_EXT.1 supports this objective by ensuring that storage capacity is maximized by eliminating multiple copies of the same data segments.	

Objective: O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_SMR.1	Security roles
Rationale:	FIA_UAU.2 supports this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data. FMT_SMR.1 meets this objective by supporting authorized roles for the TOE.	

Objective: O.OBSFEED	The TOE must provide protected feedback to users while authentication is in progress.	
Security Functional Requirements:	FIA_UAU.7	Protected authentication feedback
Rationale:	FIA_UAU.7 supports this objective by providing only the number of characters typed to users while authentication is in progress.	

Objective: O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.	
Security Functional Requirements:	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_SDI.2	Stored data integrity monitoring and action
	FPT_FLS.1	Failure with preservation of state
Rationale:	FDP_IFC.1 supports this objective by enforcing the User Data Information Flow Control SFP on external servers. FDP_IFF.1 supports this objective by identifying the rules and security attributes associated with the User Data Information Flow Control SFP. FDP_SDI.2 protects stored user data from integrity errors. FPT_FLS.1 protects stored user data from disk failure.	

6.4 DEPENDENCY RATIONALE

Table 12 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_DDR_EXT.1	None	N/A	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1)
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2)
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_FLS.1	None	N/A	
FPT_STM.1	None	N/A	

Table 12 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 13.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	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
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage

Assurance Class	Assurance Components	
	Identifier	**Name**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 13 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. A description of each of the TOE security functions follows.

7.1 TOE SECURITY FUNCTIONS

7.1.1 Security Audit

The TOE generates a set of log files determined by the system events that occur. Log files cannot be modified or deleted by any user within the DD System Manager but can be copied from the log directory and accessed through another application, such as Notepad. Log files can also be viewed in the CLI by using the *log view* command.

The following logs are generated by the TOE:

Log File Name / Location	Auditable events	Event Log Information
audit.log */ddvar/log/audit.log*	User login events	• Subject identity • Date and time
cifs.log */ddvar/log//debug/cifs/cifs.log*	CIFS activity	• Client server identity • Date and time
Messages */ddvar/log/messages*	General system events	• Commands executed • Startup and shut down of the audit functions • Date and time
secure.log */ddvar/log/debug/secure.log*	User events	• Successful and failed logins • User additions and deletions • Password changes • Date and time
access.log */ddvar/log/debug/sm/access_log*	GUI transactions	• Subject identity • Date and time

Table 14 – TOE Log Files

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2.

7.1.2 User Data Protection

The TOE enforces the Management Access Control SFP to control access to the administrative functions and configuration of the TOE. Only authorized Administrators have the ability to manipulate the TOE functions.

The User Data Information Flow Control SFP is implemented in a hierarchical manner. When an external server attempts to access a data directory, the identity of the server is checked against the directory permissions associated with the data being requested. For example, if an external server attempts to write files to a directory, but only read permissions are associated with that server, then the TOE prevents the data from being written to the directory.

The TOE uses RAID 6 to preserve the integrity of 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.

Data deduplication 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 store the rest of the unique user data.

Data Domain performs deduplication using the proprietary Stream-Informed Segment Layout (SISL) scaling architecture. The deduplication algorithm breaks the incoming data stream into segments and computes a unique fingerprint for the segment. This fingerprint is then compared to all others in the system to determine whether it is unique or redundant. Only unique data, and additional references to the previously stored unique segment, are stored to disk.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_DDR_EXT.1, FDP_IFC.1, FDP_IFF.1, FDP_SDI.2.

7.1.3 Identification and Authentication

The Identification and Authentication function ensures that a user requesting a TOE administrative function has provided a valid User ID and password and is authorized to access that service, based on the user's role.

When a user enters valid credentials at a TOE management interface, the user is granted access based on the user ID and role.

During the authentication process, only the number of characters typed is displayed while the user enters a password.

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

7.1.4 Security Management

Table 15 identifies the user roles and describes the TOE functions available to each:

User Role	Description
Admin	An admin role user can configure and monitor the entire Data Domain system. Most configuration features and commands are available only to admin role users. However, some features and commands require the approval of a security role user before a task is completed. The admin role users is capable of performing the following management functions: • administering user account information • administering TOE configuration functions • administering user data information flow control rules
User	The user role enables users to monitor systems and change their own password. Users who are assigned the user management role can view system status, but they cannot change the system configuration.
Security Officer	Users in the security officer role user can manage other security officers, authorize procedures that require security officer approval, and perform all tasks supported for user-role users. Many command options for administering sensitive operations require security officer approval.
Backup Operator	A backup-operator role user has all user role permissions and can also add, delete, reset and view CLI command aliases, and synchronize modified files.
Tenant-Admin	A tenant-admin role user can configure and monitor a specific tenant unit.
Tenant-User	The tenant-user role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the tenant-user management role can view tenant unit status, but they cannot change the tenant unit configuration.

Table 15 – TOE User Role Descriptions

The Data Domain appliance is installed with a default user account named *sysadmin*. The factory default password is the device's serial number, and the user is prompted to change the password on the first login. This account has admin permissions, and may not be deleted or modified. All administrative functions may be performed by a user in the admin role. Only the sysadmin user (the default user created during the DD OS installation) can create the first security officer, after which the privilege to create security officers is removed from the sysadmin user. After the first security officer is created, only security

officers can create other security officers. There are some tasks that must be performed by a user in the admin role, and then approved by a user in the security officer role. However, many these functions are outside of the scope of the evaluation.

User ID and role information may be administered by users in the admin role. Users in the tenant-admin role may perform these functions for their specific tenant unit. Only the sysadmin user is available by default. All other users must be added by a user in the admin, tenant-admin or security officer role. This is considered to be restrictive default values for the User ID and role attributes.

Users in the admin role may determine which external servers or clients are permitted access to the Data Domain resources. Clients are identified by hostname or IP address. By default, no clients are granted access. This is considered to be restrictive default values for the server identity attributes.

Both the CLI and GUI provide functionality to administer the user account information for authorized administrators, configure the TOE for basic setup and to allow access to external servers, and to review audit logs.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT.MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE uses a RAID 6 configuration to ensure that data remains consistent between physically separate disks within the same RAID group. The TOE ensures consistency between physically separate disks by specifying that RAID is to be used to protect the integrity of data stored on those disks.

The TOE also provides reliable time stamps for auditable events.

TOE Security Functional Requirements addressed: FPT_FLS.1, FPT_STM.1.

8 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
DD OS	Data Domain Operating System
DR	Disaster Recovery
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GUI	Graphical User Interface
IT	Information Technology
NFS	Network File System
NVRAM	Non-Volatile Random Access Memory
OSP	Organizational Security Policies
PP	Protection Profile
PS/2	Personal System/2
RAID	Redundant Array Independent Disk
SFP	Security Function Policy
SFR	Security Functional Requirement
SISL	Stream-Informed Segment Layout
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
VT	Virtual Terminal

Table 16 – Acronyms