EMC Corporation
Data Domain® Operating System
Version 5.2.1.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.11

Prepared for:

EMC²
where information lives®

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

Phone: +1 508 435 1000

http://www.emc.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the EMC® Data Domain® Operating System Version 5.2.1.0, 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 is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC Corporation Data Domain® Operating System Version 5.2.1.0 Security Target
ST Version	Version 0.11
ST Author	Corsec Security, Inc.
ST Publication Date	2013-03-18
TOE Reference	EMC® Data Domain® Operating System Version 5.2.1.0-331816
FIPS[1] 140-2 Status	N/A

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

EMC® DDOS[23] disk-based deduplication storage systems optimize data protection and disaster recovery performance. EMC® DDOS 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® DDOS systems support all leading enterprise backup and archive applications for seamless integration into existing Information Technology (IT) infrastructures. An EMC® DDOS 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.

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

An EMC® DDOS system works seamlessly with existing backup software: to a backup server, the EMC® DDOS 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® DDOS system, and each EMC® DDOS system can handle multiple simultaneous backup and restore operations. If additional throughput and capacity are needed, multiple EMC® DDOS systems can be attached to one or more backup servers. EMC® DDOS systems can also provide replication services, whereby one EMC® DDOS system acts as a backup for another EMC® DDOS system.

EMC® DDOS 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. Administrators use a secure connection to connect to both interfaces.

1.4 TOE Overview

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 EMC® DDOS storage optimizing operating system. The TOE runs on EMC® DDOS appliance hardware. The EMC® DDOS appliance hardware models are:

- DD120
- DD140
- DD160
- DD510
- DD530
- DD565
- DD580
- DD580g
- DD610
- DD620
- DD630

[2] DD – Data Domain®

[3] OS – Operating System

- DD640
- DD660
- DD670
- DD690
- DD690g
- DD860
- DD Archiver860
- DD880
- DD880g
- DD880GDA
- DD890
- DD890GDA
- DD990

1.4.2 Evaluated Configuration

As shown in Figure 1 below, the TOE encompasses the entire DDOS software image and excludes the hardware on which the DDOS executes. All functionality (except functionality called out in Section 1.4.6 below) of the DDOS is included within the TOE boundary.

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

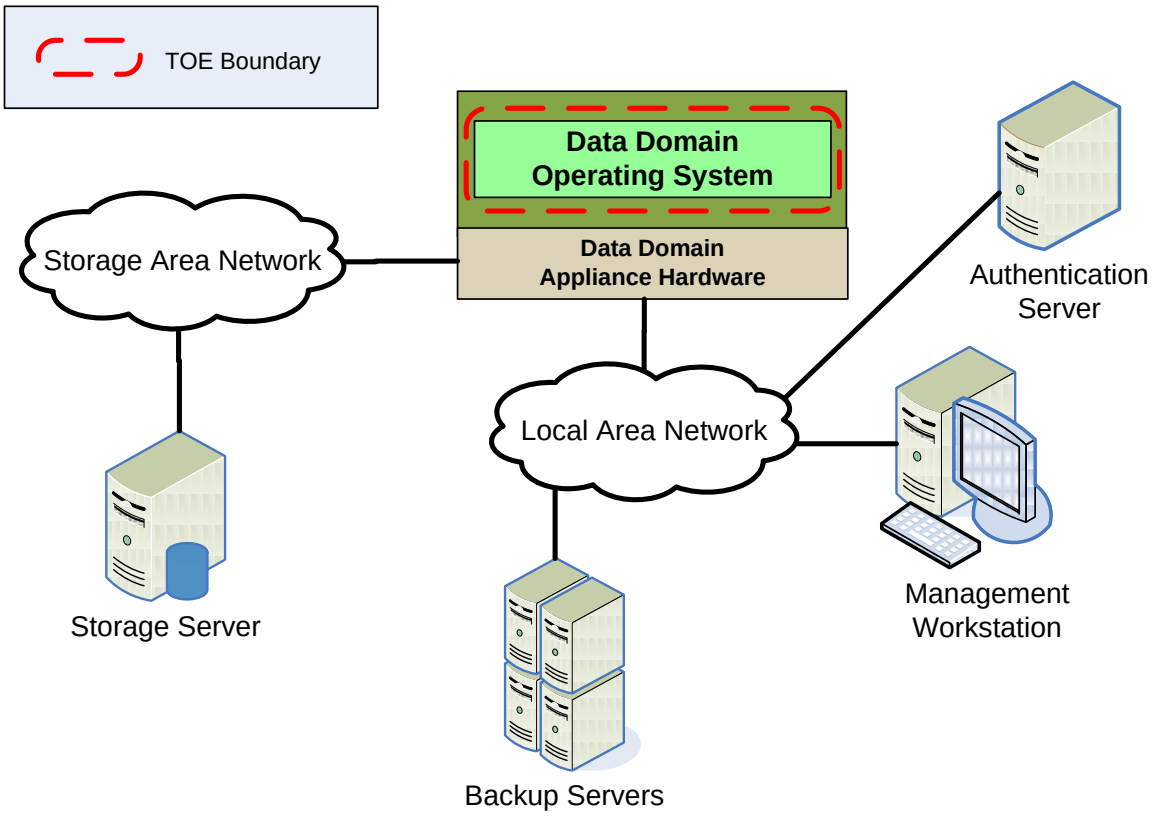

Figure 1 Deployment Configuration of the TOE

1.4.3 TOE Environment

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

- EMC® DDOS 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 DDOS 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
- Cryptographic Support
- User Data Storage
- Identification and Authentication
- Management

1.4.4.1 Audit

The TOE audits authentication events, connections/disconnections to the TOE, 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[4]) 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 the evaluated configuration only the users with Admin or SE[5] 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.logvisible=false*. Hence, the TOE provides audit review functions, and it restricts audit review to users with the appropriate permissions.

1.4.4.2 Cryptographic Support

The TOE uses FIPS-validated algorithms to provide symmetric encryption and decryption for stored user data. The vendor also affirms that the module performs in a compliant manner running the operational environment listed above. All cryptographic keys and CSPs are under the control of the guest operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution.

The keys[6] used for encryption and decryption operations are obtained by a local Key Manager (KM). The KM receives the keys from a key management server (such as RSA Key Manager or Data Domain Key Manager) and then stores the received keys in a name-value database persisted locally in the TOE. A Key

[4] See caveats in section 6.2.1 and 7.1.1 below.
[5] SE – Security Engineer
[6] There are no security claims around the management of the encryption and decryption keys. Encryption and decryption operations are provided by the RSA BSAFE module which has been vendor affirmed for DDOS; however, key management is provided by OpenSSL.

Table (KT) manages and provides access to the keys in the name-value database. The KT retrieves and forwards the locally stored keys to the TOE when encryption and decryption operation requests are made. In addition to providing access methods for the TOE to retrieve the current keys, the KT is also responsible for handling rekeying operations when new keys are received from the key management server. The KT handles this rekeying process as follows:

1. All encryption operations will use the new encryption key
2. Decryption operations will use the old encryption key until the rekeying operation is complete. Upon completion, both encryption and decryption will occur using the new exclusively.

1.4.4.3 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.

1.4.4.4 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). No visible feedback is given during the authentication process.

1.4.4.5 Management

Access Control roles for TOE users managing the TOE are implemented by the Management Access Control SFP. The TOE implements six user roles: User, Admin, Security Officer, SE, Backup Operator, and Data Access.

1.4.5 Guidance Documentation

The following product guides are part of the TOE:

- EMC® Data Domain Operating System Release Notes Version 5.2
- EMC® Data Domain Operating System Initial Configuration Guide Version 5.2
- EMC® Data Domain Operating System Command Reference Guide Version 5.2
- EMC® Data Domain Operating System Administration Guide Version 5.2

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

2 Conformance Claims

This section and Table 2 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2012-02-15 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Reporting Procedures (ALC_FLR.2)

3 Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[7] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the 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 4 Security Objectives. Table 3 below lists the applicable threats.

Table 3 Threats

Name	Description
T.DATA_STORAGE	Data could become corrupted due to incorrect system access by TOE users or an attacker could exhaust storage resources.
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.
T.SENSITIVE_DATA	An attacker or user might circumvent access controls to gain access to other users' confidential data.
T.OPERATIONAL_ERRORS	An attacker or user may exploit vulnerabilities introduced into the TOE configuration that cause the TOE to enter a configuration that is not able to enforce the security policies of the TOE. This could result in the user or attacker bypassing access controls and gaining access to TOE or user data that should not be accessible.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access (view, modify, delete) to user data.
T.UNKNOWN_STATE	A user or attacker may gain unauthorized access to TOE data or user

[7] IT – Information Technology

Name	Description
	data when the TOE is initially started or restarted after a failure, due to the security state of the TOE being unknown.

3.2 Organizational Security Policies

There are no organizational security policies defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 4 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 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.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 5 below.

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 store.
O.ACCESS	The TOE will ensure that users gain only authorized access to it and to resources that it controls.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to selectively view audit information and alert the administrator of identified potential security violations. The TOE will prevent improper values from being used for security attributes.
O.CRYPTOGRAPHIC_SERVICES	The TOE will make Data-At-Rest encryption services available to authorized user applications.
O.RECOVERY	Procedures and/or mechanisms will be provided to assure that recovery is obtained without a protection compromise, such as from system failure or discontinuity.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 IT Security Objectives

Name	Description

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.

4.2.2 Non-IT Security Objectives

Table 7 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 Non-IT Security Objectives

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

5 Extended Components

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

5.1 Extended TOE Security Functional Components

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
EXT_FPT_TRC.1	Internal TSF data consistency

5.1.1 Class EXT_FDD: User Data Deduplication

User Data Deduplication 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 Deduplication 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.

5.1.1.1 Duplicate Data Removal (EXT_FDD_DDR)

Family Behavior

This family defines the requirements for data deduplication functionality.

Component Leveling

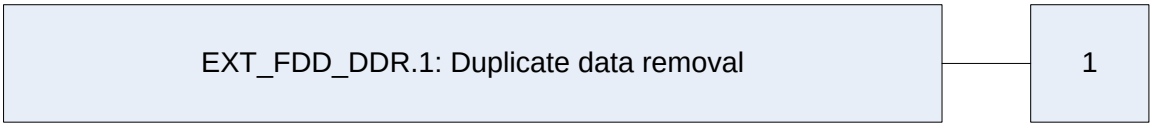

Figure 2 – EXT_FDD_DDR Duplicate Data Removal Family Decomposition

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.

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 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

5.1.2 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.

5.1.2.1 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

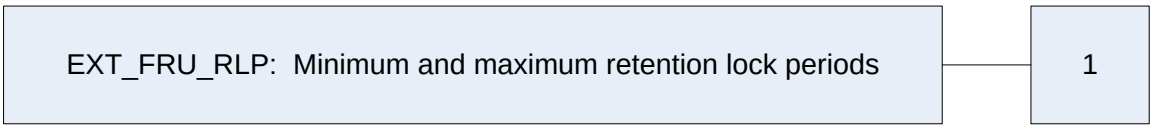

Figure 3 – EXT_FRU_RLP Minimum and maximum retention lock periods family decomposition

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 should 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
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-erasable 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-erasable format.
Dependencies: No dependencies

5.1.3 Class FPT: Protection of the TSF

EXT_FPT_TRC.1 has been created to require timely consistency of replicated TSF data. In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies, but that they will be corrected without undue delay.

This extended SFR addresses only the data consistency portion of the CC Part 2 FPT_TRC.1 SFR. The replication portion of FPT_TRC.1 is fulfilled by the TOE Environment, as demonstrated by OE.SECURE_COMMUNICATIONS. Therefore, the dependency upon FPT_ITT.1 is not required or appropriate for this extended SFR.

5.1.3.1 Internal TSF data consistency (EXT_FPT_TRC)

Family Behavior

This family defines the requirements for Internal TSF data consistency functionality.

Component Leveling

Figure 4 – EXT_FPT_TRC Internal TSF data consistency Family Decomposition

EXT_FPT_TRC.1 Internal TSF data consistency ensures that the TOE can recover from data inconsistencies between physically separate components.

Management: EXT_FPT_TRC.1

No management activities foreseen.

EXT_FPT_TRC.1 Internal TSF data consistency
Hierarchical to: No other components
EXT_FPT_TRC.1.1
The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state without undue delay.
Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended assurance components.

6 Security Requirements

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

6.1 Conventions

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

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

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the 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.

6.2 Security Functional Requirements

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

Table 9 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓	✓	
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FCS_COP.1	Cryptographic operation		✓		
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		✓		
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		✓		

Name	Description	S	A	R	I
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3(a)	Static attribute initialization	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialization				✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
EXT_FPT_TRC.1	Internal TSF data consistency				
EXT_FRU_RLP.1	Minimum and maximum retention lock periods				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*all connections to the TOE via SSH and user access protocols;*
d) *GUI events:*
    a. *logins;*
    b. *modifications to the system configuration/state;*
e) *CLI events:*
    a. *login and logout*;
    b. *modifications to system configuration/state*].

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 for login behavior, connections/disconnections, and general consistency issues encountered on the TOE's back-end**) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: The GUI and CLI do not log certain types of failure events; this is due to the way in which commands are processed by the system. In general, the GUI and CLI perform basic syntax and consistency checks; if the command fails due to an error of this type, the command is never issued to the back-end, thus an audit log is never generated. The same is also true for authorization failures. The role-based access check is performed at the front end; if a user is not authorized to perform a function, the command fails. However, since the command is never fully processed by the backend, the authorization failure is not logged. Specifically, with the GUI, access checks are built into the interface code, and users are only presented with UI elements appropriate for the user's role, therefore a failure based on authorization is not possible since the user is never capable of issuing a command for which the user is not authorized. The types of failures that are generated by the system include basic consistency checks (once the command reaches the back-end). For example, if a resource selected by a user is not available or the resource has been deleted.

Application Note: In some cases, as with the GUI passing commands to the back-end, some events are recorded with the identity of the application rather than the identity of the user. In these scenarios, the application identifier represents the subject identity.

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 [*authorized 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

6.2.3 Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the "Cryptographic Operations" column of Table 10 below*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the "Cryptographic Algorithm" column of Table 10 below*] and cryptographic key sizes [*the key sizes listed in the "Key Sizes (bits) column of Table 10 below*] that meet the following: [*the standards listed in the "Standards (Certificate #)" column of Table 10 below*].

Table 10 Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	AES[8] CBC[9], GCM[10]	128, and 256	FIPS 197 (cert #810)
Random Number Generation	Dual ECDRBG and HMAC-DRBG	N/A	SP 800-90 (cert #2)

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

[8] AES – Advanced Encryption Standard
[9] CBC – Cipher Block Chaining
[10] GCM – Galois/Counter Mode

6.2.4 Class EXT_FDD: User Data Deduplication

EXT_FDD_DDR.1
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.

6.2.5 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*] 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:*
    - *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 user can view audit data or manipulate the TOE configuration if the user has the appropriate role*].
FDP_ACF.1.3
The TSF shall explicitly authorized 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(a) 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*
        - *Identity associated with each set of 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 identity of the external server is associated with the data's 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 authorize 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(b) Static attribute initialization

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*[11] *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

[11] RAID – Redundant Array of Independent Disks

6.2.6 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_UAU.7 Protected authentication feedback
Hierarchical to: No other components
FIA_UAU.7.1
The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

6.2.7 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 [*add or remove systems, Summary for monitoring, Reports, Task Log, System status, System Data Management, System Replication, System Hardware, System Settings, System Maintenance*] 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 [*TOE audit and configuration data*] to [*administrators with the appropriate role*].
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1(a)
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(a)
The TSF shall allow the [*admin, SE*] 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_MSA.3(b) Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1(b)
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(b)
The TSF shall allow the [*admin, SE*] 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 (configuration data, i.e. licenses, network addresses, system host information, storage volumes, etc.)*] 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, Security Officer, Backup Operator, Data Access*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.9 Class FPT: Protection of the TSF

EXT_FPT_TRC.1 Internal TSF consistency

Hierarchical to: No other components.

EXT_FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state without undue delay.

Dependencies: No dependencies

6.2.10 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-erasable 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-erasable format.

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 11 Assurance Requirements summarizes the requirements.

Table 11 Assurance Requirements

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

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 12 lists the security functions and their associated SFRs.

Table 12 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	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
Cryptographic Support	FCS_COP.1	Cryptographic operation
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_FPT_TRC.1	Internal TSF data consistency
	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_UAU.7	Protected authentication feedback
	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 behavior
	FMT_MSA.1	Management of security attributes

TOE Security Function	SFR ID	Description
	FMT_MSA.3(a)	Static attribute initialization
	FMT_MSA.3(b)	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

7.1.1 Audit

The TOE audits all logins, CLI logouts, connections/disconnections to the CLI via SSH and end-user management protocols, and modifications to the system configuration or state resulting from actions performed on the TOE's GUI and CLI. Administrative commands entered via the CLI and GUI undergo basic role-based access checks and consistency checks prior to command processing; for example, if a user access the TOE and attempts to perform a privileged function, the CLI command will fail, or in the case of GUI access, the user is never presented the UI elements for the functions for which they are not authorized. Thus, if a command is never processed by the TOE backend, a failure event due to insufficient authorization or improper syntax may not be generated.

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. In general, failure messages are generated for failures related to authentication, and back-end processing errors; e.g. consistency issues. For example, if a user attempts to access a resource that is unavailable or has been deleted, or is inconsistent with the system state, a failure message is generated.

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 the evaluated configuration, 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.logvisible=false.* Hence, the TOE provides audit review functions, and it restricts audit review to users with the appropriate permissions.

The TOE audit logs are recorded in the following files:

- */ddrvar/log/audit.log*
- */ddrvar/log/messages.engineering*
- */ddrvar/log/secure.log*
- */debug/sm/sms.info*
- */debug/sm/ddsh.info*
- */debug/sm/em.info*
- */debug/sm/em_error.info*
- */debug/sm/error_log*
- */debug/sm/em_jvm.info*
- */debug/sm/access_log (Simple Network Management Protocol access logs)*
- */debug/cifs/cifs.log (Microsoft Management Console access logs)*

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

7.1.2 Cryptographic Support

The TOE uses FIPS-validated algorithms to provide cryptographic services. Cryptography is used for symmetric encryption and decryption of user data stored by the TOE. Encryption and decryption are provided by AES.

TOE Security Functional Requirements Satisfied: FCS_COP.1.

7.1.3 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 permissions and each permission set has an associated external server identity. Every time an external server attempts to access a file, the identity of the server is checked against the stored permissions for that server's identity, and if the permissions are sufficient then the access is allowed. For example, if an external server attempts to write changes to a file, but only has read permissions for that file, then the TOE prevents the data from being written to the file.

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. This meets the requirements for FDP_RIP.1 which specifies that the content of a resource (in this case stored data) is made unavailable when it is deallocated.

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. RAID 6 also guarantees that data remains consistent between physically separate disks within the same RAID group. Although the disks are not within the TOE boundary, the TOE software still controls which data is being stored using RAID. Therefore, the TOE ensures consistency between physically separate disks by specifying that RAID is to be used to guarantee the integrity of data stored on those disks.

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. The minimum period is the time the retention lock takes effect, until the retention lock expires. The maximum period is the duration that the retention period can be extended (up to 70 years). 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_FPT_TRC.1, EXT_FRU_RLP.1.

7.1.4 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. During authentication, only obscured feedback is given while the user types in a password.

Permissions are associated with user accounts for administrative users of the TOE. For regular users, the TOE stores permissions for each file and directory. Users are then assigned read, write, and execute permissions on a per-directory or per-file basis.

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

7.1.5 Management

Management Access Control roles are implemented in hierarchical manner. The "subjects" of the Policy are the users. Each user has a username, role, and an inherited role. The "objects" of the Management Access Control Policy are the audit data and TOE configuration data. The TOE performs a check with the user's role against the audit or configuration data's role every time a user attempts to access that data in order to provide proper access controls. By default, administrators are given the "user" role, allowing access to some commands. The administrator creating a new account can specify alternate values for this role.

The TOE implements six user roles: *User*, *Admin*, *Security Officer*, *Backup Operator*, *Data Access*, and *SE*. The User role is the least-privileged role, offering access to fewer commands, most of which display information only. The Admin role is the most-fully-privileged role that an end-user of the TOE can hold, allowing access to all DDOS system commands. The Security Officer role involves authorization oversight functionality where the Security Officer grants approval for certain sensitive operations. The Backup Operator role involves a subset of administrative functions related to backup operations only. The Data Access role is used only to access data stored on the TOE and does not have any management capabilities. The SE role is a special role that can be assumed by EMC® engineers in order to perform debugging and maintenance tasks that are not available to end-users.

Only administrative users with the Admin role are authorized to enable, disable, query and delete TOE audit data and query, modify, and delete TOE configuration data. The Admin role is also required to query, modify, and delete access permissions to TOE storage and stored data. Access controls for managing the TOE and for accessing storage are restrictive by default. Access to change the default values of, query, modify or delete TSF data is restricted to administrative users with the Admin role. Admins and Users may add or remove systems, generate and view reports, view summary information on the storage system, view task logs, view system status, run system data management commands, set up system replication, view system hardware, manage system settings, and perform system maintenance.

TOE Security Functional Requirements Satisfied: FDP_ACC.2, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3(a), FMT_MSA.3(b), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 13 below provides a mapping of the objects to the threats they counter.

Table 13 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_STORAGE Data could become corrupted due to incorrect system access by TOE users or an attacker could exhaust storage resources.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE 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 counters 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 store.	O.PROTECT counters 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 counters this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the TOE.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.AUDIT The TOE must provide a means of detecting and logging security-relevant events, and must provide	O.AUDIT counters this threat by ensuring that administrators can determine that improper data access or configuration change

Threats	Objectives	Rationale
	administrators with a means of reviewing the audit log.	attempts are being performed.
	OE.SECURE_SERVERS The TOE environment must provide servers configured per current corporate security policy guidelines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that each server connected to the TOE operates securely and does not intentionally compromise data.
	O.PROTECT The TOE must protect data that it has been entrusted to store.	O.PROTECT counters this threat by ensuring that the TOE provides adequate mechanisms to give only authorized servers access to the appropriately authorized data.
T.SENSITIVE_DATA An attacker or user might circumvent access controls to gain access to other users' confidential data.	O.PROTECT The TOE must protect data that it has been entrusted to store.	O.PROTECT counters this threat by ensuring that the TOE provides access controls to prevent unauthorized access to data. O.PROTECT also provides mechanisms to ensure that data is not corrupted.
	O.CRYPTOGRAPHIC_SERVICES The TOE will make Data-At-Rest encryption services available to authorized user applications.	O.CRYPTOGRAPHIC_SERVICES counters this threat by ensuring that the TOE is capable of providing FIPS-validated cryptographic services to applications.
T.OPERATIONAL_ERRORS An attacker or user may exploit vulnerabilities introduced into the TOE configuration that cause the TOE to enter a configuration that is not able to enforce the security policies of the TOE. This could result in the user or attacker bypassing access controls and gaining access to TOE or user data that should not be accessible.	O.CORRECT_TSF_OPERATION The TOE will provide the capability to selectively view audit information and alert the administrator of identified potential security violations. The TOE will prevent improper values from being used for security attributes.	The TOE must continue to operate correctly and enforce its security policies once it has been fielded. O.CORRECT_TSF_OPERATION ensures that only proper attributes will be accepted during configuration changes, and allows administrators to review configuration changes to ensure no improper configuration exists.
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access (view, modify, delete) to user data.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	Unauthorized users may physically access TOE resources. To mitigate this threat, OE.PHYSICAL restricts the physical access only to authorized personnel.
	O.PROTECT The TOE must protect data that it has been entrusted to store.	O.PROTECT enforces access rules by providing mechanisms to prevent the user data from being disclosed or modified by an unauthorized third party.

Threats	Objectives	Rationale
	O.ACCESS The TOE will ensure that users gain only authorized access to it and to resources that it controls.	Within the computing environment, O.ACCESS restricts all access controls to authorized users based on their user identity.
T.UNKNOWN_STATE A user or attacker may gain unauthorized access to TOE data or user data when the TOE is initially started or restarted after a failure, due to the security state of the TOE being unknown.	O.RECOVERY Procedures and/or mechanisms will be provided to assure that recovery is obtained without a protection compromise, such as from system failure or discontinuity.	After a failure, the security condition of the TOE may be unknown. To mitigate this threat, O.RECOVERY provides procedures and/or mechanisms to ensure that recovery without a protection compromise is obtained.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined in this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 14 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security will be provided for the TOE and its environment.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information.
A.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 upholds this assumption by ensuring that the TOE environment provides reliable timestamps to the TOE.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.
A.NOEVIL	NOE.NOEVIL	NOE.NOEVIL upholds this

Assumptions	Objectives	Rationale
Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	assumption by ensuring that administrators managing the TOE are non-hostile, appropriately trained, and follow all administrator guidance.

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

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_FDD: User Data Deduplication requirements were created to specifically address the data deduplication 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 were 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.

An extended SFR called EXT_FPT_TRC.1: Internal TSF data consistency was created to address inconsistencies in stored data. In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies, but that they will be corrected without undue delay.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements defined in this Security Target.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 below shows a mapping of the objectives and the SFRs that support them.

Table 15 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 supports this objective by storing administrative credentials for each user.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by requiring each administrator to be successfully authenticated before allowing access to TOE management functionality.
	FIA_UID.2 User identification before any action	FIA_UID.2 supports this objective by requiring each administrator to be successfully authenticated before allowing access to TOE management functionality.
	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 supports this objective by granting the ability to modify the behavior of the TOE security functionality to certain roles managed by the TOE.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by ensuring that only authorized administrators can modify TOE security attributes.
	FMT_MSA.3(a) Static attribute initialization	FMT_MSA.3 supports this objective by providing default permissive values for data access to a new data object upon creation, and allowing only authorized administrators to change this default.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by implementing a role-based access control scheme for management functionality.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 supports this objective by specifying each of the management functions that are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by defining specific roles to govern management of the TOE.
O.AUDIT	FAU_GEN.1	FAU_GEN.1 supports this

Objective	Requirements Addressing the Objective	Rationale
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.	Audit data generation	objective by ensuring that the TOE generates audit records of all administrative commands.
	FAU_GEN.2 User identity association	FAU_GEN.2 supports this objective by ensuring that the TOE associates each audit record with the identity of the user that caused the event that was logged.
	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by only allowing authorized administrators to review the audit log.
	FAU_SAR.2 Restricted audit review	FAU_SAR.2 supports this objective by only allowing authorized administrators to review the audit log.
	FDP_ACC.2 Complete access control	FDP_ACC.2 supports this objective by enforcing an access control policy that restricts the viewing of audit data to only authorized administrators.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 supports this objective by enforcing an access control policy that restricts the viewing of audit data to only authorized 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	EXT_FDD_DDR.1 supports this objective by identifying and removing segments of data sent to the TOE for storage if those segments are already present in the datastore.
O.PROTECT The TOE must protect data that it has been entrusted to store.	FDP_ACC.2 Complete access control	FDP_ACC.2 supports this objective by enforcing 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	FDP_ACF.1 supports this objective by providing access control functionality to manage access to the TOE.
	FDP_IFC.2 Complete information flow control	FDP_IFC.2 supports this objective by providing an information flow control policy that ensures that only authorized servers can gain access to stored user data.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by providing information flow control functionality to manage access to the stored data managed by the TOE.
	FDP_RIP.1 Subset residual information protection	FDP_RIP.1 supports this objective by ensuring 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	FDP_SDI.2 supports this objective by protecting stored user data from integrity errors.
	FIA_UAU.7 Protected authentication feedback	FIA_UAU.7 ensures that no feedback that affects the ability of users to circumvent the authentication mechanism is presented during the authentication process. The TOE is allowed to provide information that would allow the user to use the authentication mechanism in a correct manner , but not provide information that may allow alteration to their presentation that would thwart the mechanism.
	FMT_MSA.3(b) Static attribute initialization	FMT_MSA.3(b) supports this objective by specifying default restrictive values for clients accessing data storage.
	EXT_FRU_RLP.1 Minimum and maximum retention lock periods	EXT_FRU_RLP.1 supports this objective by protecting locked files from modification or deletion during the period for which a retention lock has been defined.
O.ACCESS The TOE will ensure that users gain only authorized access to it and to resources that it controls.	FDP_ACC.2 Complete access control	FDP_ACC.2 enforces an access control policy on subjects and objects and operations among them. The policy specifies the access rules between subjects and objects controlled by the TOE. While authorized users are trusted to some extent, this requirement ensures only authorized access is allowed to objects.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1 Security attribute based access control	FPD_ACF.1 specifies the access control policy rules that will be enforced by the TSF and determines if an operation among subjects and named objects is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a named object based upon security attributes.
	FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the attributes of users, including an identity that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE (e.g., the TOE associates an identity with any role the user may assume).
	EXT_FPT_TRC.1 Internal TSF data consistency	EXT_FPT_TRC.1 ensures that the TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner. The ability to ensure that the TSF data is consistent, between parts of the TOE, affords the TOE the ability to maintain the security policies current throughout all parts of the TOE and limits the opportunity of an outdated security policy to be enforced on parts of the TOE that may be permitting unauthorized access to the TOE and its resources.
O.CORRECT_TSF_OPERATION The TOE will provide the capability to selectively view audit information and alert the administrator of identified potential security violations. The TOE will prevent improper values from being used for security attributes.	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by providing administrators with the ability to view the audit records, thereby allowing review of any configuration changes made to the TOE.
O.CRYPTOGRAPHIC_SERVICES The TOE will make Data-At-Rest encryption services available to authorized user applications.	FCS_COP.1 Cryptographic operation	FCS_COP.1 supports this objective by providing a list of cryptographic algorithms available for use on the TOE.
O.RECOVERY Procedures and/or mechanisms will be provided to assure that	EXT_FPT_TRC.1 Internal TSF data consistency	EXT_FPT_TRC.1 provides a mechanism to bring the TOE into a consistent state. The ability to

Objective	Requirements Addressing the Objective	Rationale
recovery is obtained without a protection compromise, such as from system failure or discontinuity.		ensure that the TSF data is consistent, between parts of the TOE, provides the TOE the ability to maintain the security policies current throughout all parts of the TOE and limits the opportunity of an outdated security policy to be enforced on parts of the TOE that may be permitting unauthorized access to the TOE and its resources.

8.5.2 Security Requirements Rationale for Refinement

This Security Target defines refinements to FDP_SDI.2: Stored data integrity monitoring and action. The refinement for FDP_SDI.2 was to clarify that the object being referred to is user data.

8.5.3 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. 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.

8.5.4 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 16 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 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 time stamps that are used by the TOE. Environmental Objective OE.TIME

SFR ID	Dependencies	Dependency Met	Rationale
			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	✓	
FCS_COP.1	FCS_CKM.1	✓	This dependency is not met nor required for this Security Target because the user data protection is not the primary functionality of this TOE.
	FCS_CKM.4	✓	This dependency is not met nor required for this Security Target because the user data protection is not the primary functionality of this TOE.
EXT_FDD_DDR.1	None	Yes	
FDP_ACC.2	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	FDP_ACC.2 is hierarchical to FDP_ACC.1.
	FMT_MSA.3(a)	✓	
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	FDP_IFC.2 is hierarchical to FDP_IFC.1.
	FMT_MSA.3(b)	✓	
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.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1.
FIA_UID.2	None	✓	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	FDP_ACC.2, which is

SFR ID	Dependencies	Dependency Met	Rationale
			hierarchical to FDP_ACC.1, deals with the management of the TOE.
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1	✓	Although FMT_MSA.1 does not apply to FMT_MSA.3(b), FMT_MSA.1 is not required for FMT_MSA.3(b) because the User Data Information Flow Control SFP does not permit access for the purpose of managing security attributes, and management functionality in support of the User Data Information Flow Control SFP is covered by FMT_MTD.1 and FMT_SMF.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_FPT_TRC.1	None	✓	
EXT_FRU_RLP.1	None	✓	

9 Acronyms

This section and Table 17 define the acronyms used throughout this document.

9.1 Acronyms

Table 17 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC-Message Authentication Code
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CIFS	Common Internet File System
CM	Configuration Management
CTR	Counter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
ECDRBG	Elliptical Curve Deterministic Random Bit Generator
ECDSA	Elliptical Curve Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Secure Hypertext Transfer Protocol
IT	Information Technology
KM	Key Manager
KT	Key Table
NIS	Network Information Service
OFB	Output Feedback
OS	Operating System
PP	Protection Profile
PUB	Publication
RAID	Redundant Array of Independent Disks

Acronym	Definition
SFR	Security Functional Requirement
SP	Special Publication
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

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