Dell EMC Unity OE v5.2

Security Target

Version 1.5

December 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0	9 February 2022	Updated TOE version, hardware models, and TLS cipher suites.
1.1	23 May 2022	Updated TOE version to 5.2.
1.2	22 June 2022	Addressed CB ORs.
1.3	19 July 2022	Addressed CB ORs.
1.4	17 October 2022	Addressed evaluator ORs.
1.5	9 December 2022	Updated AGD version reference.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell EMC Unity OE v5.2 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Dell EMC Unity OE v5.2 is a midrange capacity storage system comprised of the Unity hardware platform and the Unity Operating Environment (OE) software.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell EMC Unity OE v5.2 Build: 5.2.0.0.5.173
Security Target	Dell EMC Unity OE v5.2 Security Target, v1.5

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

d) EAL2+ ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CEE	Common Event Enabler
DACL	Discretionary Access Control List
DAE	Disk Array Enclosure
DPE	Disk Processor Enclosure
D@RE	Data at Rest Encryption

Term	Definition
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Services
FC	Fibre Channel
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTML5	Hypertext Markup Language 5
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SAN	Storage Area Network
SMB	Server Message Block
SP	Storage Processor
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEMCLI	Unified Element Manager Command Line Interface
VASA	vStorage API for Storage Awareness
WWN	World Wide Name

2 TOE Description

2.1 Type

4 The TOE is a midrange capacity storage system comprised of the Unity hardware platform and the Unity Operating Environment (OE) software.

5 The Unity hardware houses the disks in the storage array which are managed by the storage processors. It provides Network Access Server (NAS) and Storage Area Network (SAN) services by interfacing with the front-end clients (application hosts) and the back-end storage disks.

6 Application hosts (such as database servers, file servers, etc.) can access the Unity storage through traditional block and file protocols. The TOE presents storage to application hosts as a standard network-based virtual file server, or in the form of Logical Units (LUNs) to block-based client machines.

7 Unity supports the following storage protocols:

- File Storage Protocols
  - Common Internet File System (CIFS) / Server Message Block (SMB v2 and v3)
  - Network File System (NFS v3, v4, and v4.1)
- Block Storage Protocols
  - Internet Small Computer System Interface (iSCSI)
  - Fibre Channel (FC)

8 Each LUN is a useable storage system volume that the TOE can expose to individual hosts. Application hosts can only access LUNs for which permission has been granted by an authorized administrator.

9 Each File-based NAS server on the TOE can be configured to interface with a Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) server. When a request for data access is made from a File-based client machine, the TOE checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the user.

10 The TOE is managed by authorized administrators through the Unified Element Management Command Line Interface (UEMCLI) (also known as the Unisphere CLI), the Unisphere Graphical User Interface (GUI) and the Representational State Transfer Application Programming Interface (REST API). Administrators are assigned a user role that provides them with access to specific TOE features and functions.

11 The UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The UEMCLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. The Unisphere GUI is an HTML5 application that runs within a web browser. To access the functions available via Unisphere, an authorized administrator must open a web browser and enter the Internet Protocol (IP) address or hostname of the Unity management port. Administrators interact with the REST API by accessing resources using HTTP GET, POST, and DELETE requests.

12 The TOE is a combined software and hardware TOE. The Unity hardware consists of a disk processor enclosure (DPE) that contains two storage processors (SPs) and houses 25 disk drives. It may also include one or more optional disk-array enclosures (DAEs) containing additional disk drives. The DAEs are available in a 15 drive, 3.5-inch disk 3-unit (3U) enclosure, a 25 drive, 2.5-inch disk 2-unit (2U) enclosure, or an 80 drive, 2.5-inch disk 3U enclosure.

2.2 Usage

13 The TOE is a stand-alone appliance consisting of the Unity hardware and the Unity OE software.

14 The TOE in its evaluated configuration is shown in Figure 1.

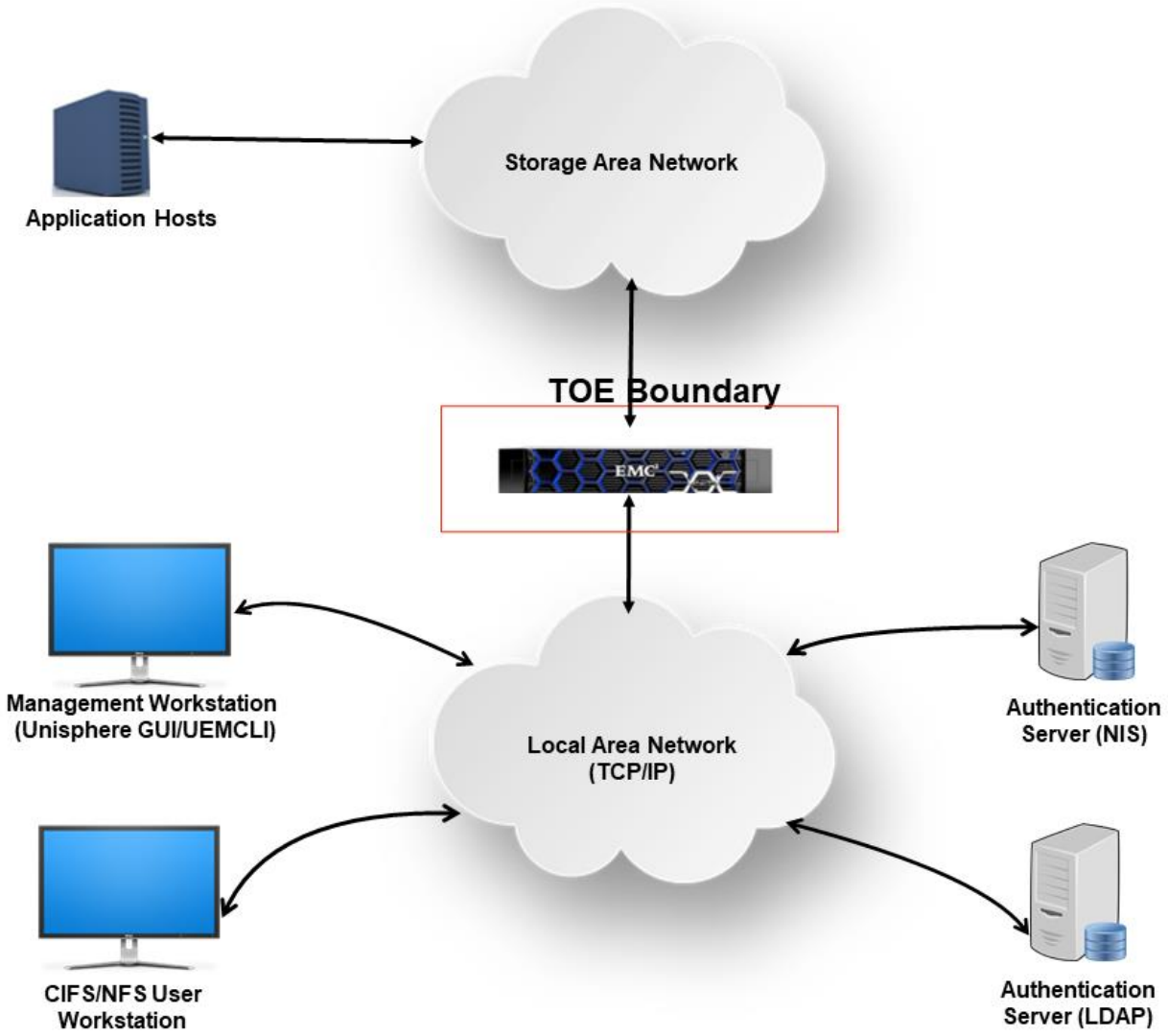

Figure 1: Example TOE deployment

2.3 Security Functions

15 The TOE provides the following security functions:

a) **Security Audit.** The TOE generates audit records for administrator login attempts and changes to the TOE configuration.

b) **User Data Protection.** The TOE only allows authorized application servers access to stored user data. The integrity of stored data is protected using RAID technology.

c) **Identification and Authentication.** TOE administrators must identify and authenticate prior to gaining access to the TOE management functionality.

d) **Security Management.** The TOE provides management capabilities via a web-based GUI, REST API and a CLI. Management functions allow authorized administrators to configure system access and storage settings.

e) **Protection of the TSF.** The TOE provides reliable time stamps for auditable events.

f) **Trusted Path/Channels.** Communications between the TOE and remote administrators and between the TOE and the LDAP server are protected using TLSv1.2.

2.4 Physical Scope

16 The physical boundary of the TOE is the Unity OE software operating on the hardware appliances shown in Table 3.

Table 3: TOE models and capabilities

TOE Component	Description
Hardware	Unity 380/380F
	Unity 480/480F
	Unity 680/680F
	Unity 880/880F
Software	Unity Operating Environment (OE) 5.2.0.0.5.173
	Unisphere 5.2.0.0.5.173
	Unisphere CLI version 5.2.0.1642972

2.4.1 TOE Delivery

17 The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system.

2.4.2 Guidance Documents

18 All guidance documentation is provided in Portable Document Format (PDF) online at the Dell Unity Info Hub, Published 28 June 2021: https://www.dell.com/support/kbdoc/en-us/000126652/dell-emc-unity-info-hub-product-documents-and-information.

19 The TOE also includes the following Common Criteria Guide:

- DellEMCUnityEAL2_AGD_1.1.pdf

2.4.3 Non-TOE Components

20 The TOE operates with the following components in the environment:

a) **Authentication Server.** The TOE makes use of a NIS Authentication server.

b) **Authentication Server.** The TOE makes use of a LDAP Authentication server.

c) **Management Workstation.** Workstation required to access and manage the TOE.

d) **User Workstation.** The TOE makes use of CIFS/NFS user workstation.

e) **Application Hosts.** The TOE makes use of application hosts.

2.5 Logical Scope

21 The logical scope of the TOE comprises the security functions defined in section 2.3.

2.5.1 Excluded Functions

22 The following functions are outside of the logical TOE scope (and have not been evaluated):

- Data at Rest Encryption (D@RE)
- Common Event Enabler (CEE)
- File-level retention
- Replication
- EMC Secure Remote Services support (ESRS)
- UnityVSA
- CloudIQ (Unity Cloud Edition)

10 **Note**: The vStorage API for Storage Awareness (VASA) Interface is not to be used in the evaluated configuration.

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
T.ACCESS	Access to user data could be improperly granted to application hosts which should not have access to it, and users with access to those hosts.
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.UNAUTH	A hostile/unauthorized user could gain access to stored data by bypassing the protection mechanisms of the TOE.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.ATTRIBUTE	The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

Table 6: Organizational Security Policies

Identifier	Description
P.RAID	User data must be protected from loss due to disk failure.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	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 those parts of the TOE critical to the enforcement of security are protected from any physical and logical attack.
OE.SERVER	The operational environment shall provide an Active Directory server and a NIS server for maintaining access control security attributes for file-based storage on the TOE.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
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.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators and LDAP authentication requests.
O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.

5 Security Requirements

5.1 Conventions

23 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by a numerical indicator in parenthesis (e.g. “FMT_MSA.1(2)”).

5.2 Extended Components Definition

24 The TOE does not claim extended components.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Generation
FAU_SAR.1	Audit Review
FDP_ACC.1(1)	Subset access control (Block Storage)
FDP_ACC.1(2)	Subset access control (File Storage)
FDP_ACF.1(1)	Security attribute based access control (Block Storage)
FDP_ACF.1(2)	Security attribute based access control (File Storage)
FDP_SDI.2	Stored data integrity monitoring and action
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1(1)	Management of security attributes (Block Storage)
FMT_MSA.1(2)	Management of security attributes (File Storage)
FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
FMT_MSA.3(2)	Static attribute initialisation (File Storage)

Requirement	Title
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted path

5.3.1 Security Audit (FAU)

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) [*Administrator login attempts, the following administrator actions that result in a configuration change to the storage array:*

- *adding, modifying, or deleting LUNs*
- *adding, modifying, or deleting CIFS shares*
- *adding, modifying, or deleting SMB shares*
- *adding, modifying, or deleting NFS mounts*
- *changes to host access permissions*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.2 User Data Protection (FDP)

FDP_ACC.1(1) Subset Access Control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(1) Security attribute based access control (Block Storage)

FDP_ACC.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] on [

- *Subjects: Hosts (application servers);*
- *Objects: LUNs;*
- *Operations: Read and write*].

FDP_ACC.1(2) Subset Access Control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(2) Security attribute based access control (File Storage)

FDP_ACC.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] on [

- *Subjects: Users (accessing storage from client machines);*
- *Objects: CIFS and SMB shares, and NFS mounts;*
- *Operations: Read, write, execute*].

FDP_ACF.1(1) Security attribute based access control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(1) Subset access control (Block Storage)

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] to objects based on the following: [

- *Subjects: Hosts (application servers);*
    - *Security Attributes:*
        - *iSCSI Qualified Name (IQN)*
        - *World Wide Name (WWN)*
- *Objects: LUNs*

- *Security Attributes:*
  - *IQN access list*
  - *WWN access list*].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[A valid subject of the TOE is allowed to read and write to TOE storage if the IQN or WWN of the subject is included in the list of hosts that have access to the LUN*].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[none*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

FDP_ACF.1(2) Security attribute based access control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(2) Subset access control (File Storage)

FMT_MSA.3(2) Static attribute initialization

FDP_ACF.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] to objects based on the following:

- *Subjects: Users (accessing storage from client machines);*
  - *Security Attributes:*
    - *Username*
    - *Authentication status (success or failure)*
    - *IP address (for NFS access)*
- *Objects: File shares*
  - *Security Attributes:*
    - *NFS Mount permissions: Unix-style ACLs for each file and directory*
    - *CIFS and SMB Share Permissions: NT-style Discretionary Access Control Lists (DACLs) for each file and directory*

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[A successfully authenticated subject of the TOE is allowed to perform an operation if the content of the Access Control List (containing permissions) for the object authorizes the Subject to perform the desired operation*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

- *For CIFS and SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects and control over the overall share permissions for the entire domain;*
- *For NFS access, the user must access the NFS mount from a computer running an IP address listed in the allowed hosts configuration for the TOE;*
- *For NFS access, subjects that are authorized as superusers (root) can perform all operations on all objects;*
- *For root users accessing an NFS mount, access will be permitted if the host that the root user is using to connect to the NFS mount is listed under the 'trusted hosts' list in the TOE configuration*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*]

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

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 **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 5 and RAID 6; mirrored data for RAID 1/0*]

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*reconstruct the user data for RAID 5 and RAID 6; replace erroneous data with mirrored data for RAID 1/0; and log an alert*].

5.3.3 Identification and Authentication (FIA)

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **Administrators** ~~users~~: [*UserID, password, role*].

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.

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.

5.3.4 Security Management (FMT)

FMT_MSA.1(1) Management of security attributes (Block Storage)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1(1) Subset access control (Block Storage) 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 [*Block Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*WWN and IQN access lists] to* [*the Administrator and Storage Administrator roles*].

FMT_MSA.1(2) Management of security attributes (File Storage)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1(2) Subset access control (File Storage)

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 [*File Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*trusted hosts*] to [*the Administrator and Storage Administrator roles*].

FMT_MSA.3(1) Static attribute initialisation (Block Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1(1) Management of security attributes (Block Storage)

FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Block Storage 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 [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attribute initialisation (Block Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1(2) Management of security attributes (File Storage)

FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*File Storage Access 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 [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

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: [

- *viewing administrative information;*
- *administering the Block Storage Access Control SFP;*
- *administering the File Storage Access Control SFP;*
- *managing storage; and*
- *managing user account information*
- *LDAP configuration*]

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: [

- *Operator*
- *Storage Administrator*
- *Administrator*].

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

5.3.5 Protection of the TSF (FPT)

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.

5.3.6 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*communications with external LDAP servers*].

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*remote administration*]].

5.4 Assurance Requirements

25 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2.

Table 10: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
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
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
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

26 This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. Table 11 provides information on how the TOE satisfies the SFRs outlined in Section 5.

Table 11: SFR Fulfillment

SFR	Fulfilment
FAU_GEN.1.1	The TOE generates audit records for startup and shutdown of the audit function, all administrator login attempts, and all administrator actions that result in a configuration change.
FAU_GEN.1.2	Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event (success or failure)
FAU_SAR.1.1	Authorized administrators can view the audit records from the UEMCLI or Unisphere GUI.
FAU_SAR.1.2	The audit records are presented in a manner suitable for a user to interpret the information.
FDP_ACC.1.1(2)	All access to storage is performed via a CIFS/SMB or NFS client on behalf of the user. These clients are basic pieces of software (such as the CIFS client within Windows Explorer) used to map and access file-based storage. The TOE enforces the File Storage Access Control SFP on users connecting to the storage on the TOE for NFS and CIFS/SMB.

SFR	Fulfilment
FDP_ACF.1(2)	After successful authentication for NFS users, the TOE checks user permissions for each file or directory's ACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. After successful authentication for CIFS/SMB users, the TOE checks user permissions for each file or directory's DACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. The ability to connect to an NFS mount, and CIFS/SMB share, is granted to users by Administrators or Storage Administrators. Users are associated with CIFS/SMB shares via an access list, while a list of IP addresses is associated with NFS mounts as an access list. Individual file and directory access control management is granted to CIFS/SMB users with File Owner or Change Permissions set in the DACL for the user. NFS users with the root role can modify permissions for all files and directories, or users with the File Owner or Change Permissions for any given file or directory can manage access controls for those particular files and directories. A Linux/Unix host can mount to the Unity-hosted NFS Shared Folder Server if the host has been explicitly authorized. Similarly, a Windows user can map to the Unity-hosted CIFS/SMB NAS Servers if the user has been explicitly authorized. The export of a CIFS/SMB Shared Folder Server is determined in part by the Server Configuration LDAP setting. The Unity-hosted CIFS/SMB Shared Folder Server must be in a Windows domain with an LDAPv3-compatible server set up. A Windows client machine can map to the share only if it is a member of the defined domain. For CIFS/SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects. Client machine access to the Unity-hosted NFS Shared Folder Server can be configured based on IP address or network host name, IP subnet range, or a Netgroup. For the NFS access protocol, users connecting to TOE storage who are superusers can perform all operations on all objects. Clients must be recognized as "trusted" by the system in order to submit a root request, otherwise it will be mapped to the "nobody" role. Each file and directory has an ACL associated with it. Each ACL has a set of permissions that are granted or explicitly denied to that user. Whenever a user requests an access to a file or directory, the TOE utilizes its File Storage Access Control SFP (stored with each file and directory) to decide whether or not that access is permitted.

FDP_ACC.1(1), FDP_ACF.1(1)	The TOE enforces the Block Storage Access Control Security Function Policy (SFP) which is used to manage access from block-based application servers to configured Logical Units on the TOE. Access must specifically be granted for a host to access storage. When a host is configured, the administrator provides: • the name of the host • the IP address of the host • For iSCSI access, the iSCSI address (iSCSI Qualified Name (IQN)) of the host. Within the Storage Area Network (SAN), this is the address of the iSCSI initiator • For FC access, the WWN of the host. This is the unique address of the Host Bus Adapter (HBA) that initiates the connection to the storage resources • Access settings. The options are: o No access o LUN access o Snapshot access o LUN and Snapshot access When a LUN is configured, the administrator identifies: • Name and description of the storage resource • The storage size associated with the LUN • The hosts that have access to this resource. Hosts are identified by address: o For iSCSI, this is the IQN o For FC access, this is the WWN of the host When a user attempts to access storage resources, Unity verifies the IQN or WWN of the host initiator and verifies that the host has access to the requested LUN target before allowing access. Storage may be accessed as a LUN or a snapshot. A snapshot is a point-in-time copy of data stored on the LUN. It provides a record of the content in the targeted storage resource at a particular date and time, and may be used to support data protection and recovery. The presentation of stored data as a snapshot is beyond the scope of the evaluation; however, the Block Storage Access Control SFP applies equally to both access types. Both Windows and Linux hosts may access storage via iSCSI and FC as follows. • iSCSI Access o For a Windows host, the host must be able to access the iSCSI interface. The Microsoft iSCSI initiator service must be started. o For a Linux host, hosts connect to LUN storage resources by using Linux iSCSI software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage. • FC Access o On the Windows host, the server connection must be added using Microsoft Storage Manager for SANs. Storage Manager for SANs is a Microsoft Management Console (MMC) snap-in used to create and manage logical unit numbers (LUNs) on Fibre Channel.

SFR	Fulfilment
	○ Hosts connect to LUN storage resources by using Linux FC software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage.
FDP_SDI.2	The TOE also ensures the integrity of user data. Unity may be configured with Redundant Array of Independent Disks (RAID) levels 1/0, 5 or 6. Each of these provides fault tolerance for integrity errors or disk failure. The RAID implementation provides mechanisms to continuously check data integrity while reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators may configure 'hot spare' disk drives. These hot spares are used when a disk failure has been detected by the system. Once a failure has been detected, the drive that has been lost will be recreated on the hot spare. The Administrator can then replace the failed drive and configure it as a new hot spare. This process does not interfere with user data access. With RAID 1/0, two or more groups of two mirrored (RAID 1) disks are put in a RAID 0 array, or a stripe of mirrors. In the case of a disk failure, the mirrored data is recovered. For a RAID 5 implementation, data is striped across several disks, and parity data is divided across all the disks in the array. RAID 6 also stripes data across several disks, but uses double parity data distributed across multiple disks for added protection. When an integrity error is detected, an alert is placed in a log file. Administrators may view alerts via the Alerts page of Unisphere or from the UEMCLI.
FIA_ATD.1, FIA_UAU.2, FIA_UID.2	The TOE uses an LDAPv3-compatible server in the TOE environment to provide authentication services for both Administrators and CIFS/SMB file-based users. A NIS server is used to provide authentication services for NFS file-based users. For all authentication processes, once the username and password have been verified, the TOE uses the message returned from the authentication server to assign an administrative role, or a role to file-based users. The TOE also supports the use of local authentication. In this case, the UserID, password and role are maintained by the TOE. The TOE verifies the UserID and password on login and assigns a role. Administrators can access the TOE through a web browser or through a command line interface. Identification and authentication must be completed before Administrators are provided with access to the TOE. The TOE maintains the UserID, password and role for Administrators subject to local authentication, and only the role information for users authenticating via an LDAP directory. Windows environments use an LDAPv3-compatible server for authentication. A Windows host can only map to a CIFS Shared Folder Server if the Windows host is on the same domain as Unity, and the Windows domain with an LDAPv3-compatible server is set up. For NFS, users are authenticated against a NIS server. The server from which the request is coming is identified and authenticated based on the username and password. If the user ID is "root" then the host must also be assigned as a "trusted host" within the TOE configuration.

SFR	Fulfilment
FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1	The TOE is shipped with a factory default Management account (admin) and password (Password123#) for initial access and configuration. With this default account, administrators can reset default passwords, configure the system settings, create user accounts, and allocate storage. Changing the default password for the admin account is a requirement during the initial configuration process. Once the TOE has been configured, authorized administrators can access the TOE management functions via the UEMCLI, REST API, or the Unisphere GUI. Each administrator is assigned a role which determines TOE access capabilities. The Administrator role has access to all of the TOE's functions. The storage administrator can Change own local login password, create and delete storage, add storage objects, such as LUNs, shares, and storage groups to a storage resource, view storage configuration and status, view Unisphere user accounts, view current software or license status, change management interface language, view log and alert information. The operator can only view current software or license status, change management interface language, view log and alert information, view storage configuration and status, change own login password. Default attributes for the Block Access Control SFP are considered to be restrictive because an application host will not have access to storage resources until its WWN or IQN is specifically listed in the LUN's host access list. The TOE provides mechanisms to govern which hosts can access which LUNs. Default attributes for the File Access Control SFP are considered to be restrictive because trusted host does not exist until entered by an Administrator. The Security Management functions allow Administrators assigned the appropriate role to configure this functionality. Client machines accessing the TOE via CIFS, SMB, or NFS protocols do not have access until the user is authenticated. Once authenticated, the user is granted access according to the Access Control List associated with each file and directory. CIFS/SMB, and NFS file and directory attributes that can be modified include read, write, and execute permissions. There are no set default permissions.
FPT_STM.1	The TOE provides reliable time stamps for auditable events. Time information is obtained from the underlying OS.

SFR	Fulfilment
FTP_ITC.1	Communications with external LDAP servers used for remote authentication are protected using TLSv1.2. The following cipher suites are supported: • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 • TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 • TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

SFR	Fulfilment
FTP_TRP.1	All communications with remote administrators via the Web GUI and REST API are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration: • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_CCM • TLS_DHE_RSA_WITH_AES_128_CCM_8 • TLS_DHE_RSA_WITH_AES_256_CCM • TLS_DHE_RSA_WITH_AES_256_CCM_8 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

7 Rationale

7.1 Security Objectives Rationale

27 Table 12 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 12: Security Objectives Mapping

	T.ACCESS	T.ACCOUNT	T.EAVES	T.UNAUTH	T.UNDETECT	OSP.RAID	A.ATTRIBUTE	A.LOCATE	A.NOEVIL
O.ADMIN	X	X		X	X				
O.AUDIT					X				
O.IDAUTH		X		X	X				
O.INTEGRITY						X			
O.PROTCOMMS			X						
O.PROTECT	X								
OE.ADMIN									X
OE.PHYSICAL								X	
OE.SERVER							X		

28 Table 13 provides the justification to show that the security objectives are suitable to address the security problem.

Table 13: Suitability of Security Objectives

Element	Justification
T.ACCESS	**O.ADMIN** mitigates this threat by only allowing authorized administrators the ability to manage TOE access functions. **O.PROTECT** mitigates this threat by identifying application hosts by name before allowing access to protected data.

Element	Justification
T.ACCOUNT	**O.ADMIN** mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. **O.IDAUTH** mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.
T.EAVES	**O.PROTCOMMS.** Mitigates this threat by requiring that the TOE encrypt communications with remote administrators and with external LDAP servers.
T.UNAUTH	**O.ADMIN** mitigates this threat by providing authorized administrators the ability to manage TOE security functions. **O.IDAUTH** mitigates this threat by ensuring that all users are identified and authenticated prior to gaining access to the TOE security management functions.
T.UNDETECT	**O.ADMIN** mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. **O.AUDIT** counters this threat by ensuring that the TOE tracks all management actions taken against the TOE. **O.IDAUTH** mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.
OSP.RAID	**O.INTEGRITY** supports this policy by ensuring that the TOE provides the ability to protect data in the case of disk failure.
A.ATTRIBUTE	**OE.SERVER s**upports this assumption by providing the attributes required by the TOE to make access control decisions for File-based storage.
A.LOCATE	**OE.PHYSICAL** supports this assumption by protecting the TOE from physical and logical attack.
A.NOEVIL	**OE.ADMIN** supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

29 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 14: Security Requirements Mapping

	O.ADMIN	O.AUDIT	O.IDAUTH	O.INTEGRITY	O.PROTCOMMS	O.PROTECT
FAU_GEN.1		X				
FAU_SAR.1		X				X
FDP_ACC.1(1)						X
FDP_ACC.1(2)						X
FDP_ACF.1(1)						X
FDP_ACF.1(2)				X		
FDP_SDI.2	X		X			
FIA_ATD.1	X		X			X
FIA_UAU.2	X		X			X
FIA_UID.2	X					X
FMT_MSA.1(1)	X					X
FMT_MSA.1(2)	X					X
FMT_MSA.3(1)	X					X
FMT_MSA.3(2)	X					X
FMT_SMF.1	X					
FMT_SMR.1		X				
FPT_STM.1		X				
FTP_ITC.1					X	
FTP_TRP.1					X	

Table 15: Suitability of SFRs

Objectives	SFRs
O.ADMIN	**FDP_ATD.1** supports this objective by ensuring that the TOE maintains security attributes for administrative users. **FDP_UAU.2 and FDP_UID.2** support this objective by ensuring that only authorized administrators have access to TOE functions and data. **FMT_MSA.1(1) and FMT_MSA.3(1)** support this objective by identifying the management restrictions of the Block Storage Access Control SFP. **FMT_MSA.1(2) and FMT_MSA.3(1)** support this objective by identifying the management restrictions of the File Storage Access Control SFP. **FMT_SMF.1** meets this objective by ensuring that the management functions are utilized to securely manage the TOE. **FMT_SMR.1** supports this objective by ensuring that specific roles are defined to govern management of the TOE.
O.AUDIT	**FAU_GEN.1** supports this objective by generating records for auditable events. **FAU_SAR.1** supports this objective by ensuring that the TOE provides the ability to review the audit trail. **FPT_STM.1** ensures that a time stamp is provided for each auditable event.
O.IDAUTH	**FIA_ATD.1** supports this objective by ensuring that the TOE maintains security attributes for administrative users. **FIA_UAU.2** meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. **FIA_UID.2** supports this objective by ensuring that the identity of each TOE Administrator is known before allowing access to TOE functions and data.
O.INTEGRITY	**FDP_SDI.2** meets this objective by providing the RAID functionality that protects against integrity errors due to a hardware fault.
O.PROTCOMMS	**FTP_ITC.1** requires encrypted communications with remote LDAP servers. **FTP_TRP.1** requires encrypted communications for remote administration.

Objectives	SFRs
O.PROTECT	**FDP_ACC.1(1) and FDP_ACF.1(1**) support this objective by identifying the rules and attributes of the Block Storage Access Control SFP, which are used to control application host access to data stored on the TOE. **FDP_ACC.1(2) and FDP_ACF.1(2)** support this objective by identifying the rules and attributes of the File Storage Access Control SFP, which control user access to data stored on the TOE. **FDP_UAU.2 and FIA_UID.2** support this objective by ensuring that only authorized administrators have access to TOE functions and data, and are identified and authenticated before being provided with TOE access. **FMT_MSA.1(1) and FMT_MSA.3(1)** support this objective by restricting the management of the Block Storage Access Control SFP to authorized administrators. **FMT_MSA.1(2) and FMT_MSA.3(2)** support this objective by restricting the management of the File Storage Access Control SFP to authorized administrators. **FMT_SMF.1** meets this objective by ensuring that the management functions are utilized to securely manage the TOE, thus protecting the integrity of stored user data.

Table 16: Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FDP_ACC.1(1)	FDP_ACF.1(1)	Met
FDP_ACC.1(2)	FDP_ACF.1(2)	Met
FDP_ACF.1(1)	FDP_ACC.1(1)	Met
	FMT_MSA.3(1)	Met
FDP_ACF.1(2)	FDP_ACC.1(2)	Met
	FMT_MSA.3(2)	Met
FDP_SDI.2	None	-
FIA_ATD.1	None	-
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2

SFR	Dependency	Rationale
FIA_UID.2	None	-
FMT_MSA.1(1)	FDP_ACC.1(1), or FDP_IFC.1	Met by FDP_ACC.1(1)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.1(2)	FDP_ACC.1(2), or FDP_IFC.1	Met by FDP_ACC.1(2)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3(1)	FMT_MSA.1(1)	Met
	FMT_SMR.1	Met
FMT_MSA.3(2)	FMT_MSA.1(2)	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_STM.1	None	-
FTP_ITC.1	None	-
FTP_TRP.1	None	-