Dell PowerProtect Data Manager v19.22

Security Target

Version 1.8

July 2026

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
0.1	February 24th, 2025	Initial Draft.
1.0	March 5th, 2025	Draft for evaluation.
1.1	May 8th, 2025	Addressed evaluator ORs.
1.2	December 2nd, 2025	Updated TOE version and guidance references. Addressed CB ORs.
1.3	December 29th, 2025	Updated TOE version. Other misc. updates.
1.4	27 February 2026	Updated supported algorithms and guidance references.
1.5	1 April 2026	Updated TOE version.
1.6	15 May 2026	Updated AGD version.
1.7	10 June 2026	Updated AGD version.
1.8	13 July 2026	Addressed Certifier comments.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell PowerProtect Data Manager v19.22 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Dell PowerProtect Data Manager v19.22 is a software-defined data backup and recovery[1] solution that integrates with other Dell data protection products, enabling data protection as a service.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell PowerProtect Data Manager v19.22 Build 19.22.0-24
Security Target	Dell PowerProtect Data Manager v19.22 Security Target, v1.8

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC:2022 Release 1

b) CC:2022 Part 2 extended

c) CC:2022 Part 3 conformant

d) CC:2022 Part 5 conformant

e) Package - EAL2 augmented with ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
DDVE	Data Domain Virtual Environment
EAL	Evaluation Assurance Level

[1] In the context of this ST, the term “restore” is used to specify the operation. The terms “recovery” or “recover” are used to specify the purpose of the operation.

Term	Definition
GUI	Graphical User Interface
HANA	High-Performance Analytic Appliance
HTML	Hypertext Markup Language
LDAP	Lightweight Directory Access Protocol
NAS	Network-Attached Storage
NTP	Network Time Protocol
OSP	Organizational Security Policy
OVA	Open Virtual Appliance
PDF	Portable Document Format
PP	Protection Profile
REST	Representational Stat Transfer
SAP	Systems, Applications and Products
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SP	Service Pack
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine

2 TOE Description

2.1 Type

4 The TOE is a data manager that facilitates scheduled and on-demand (self-service) backup and restore operations.

2.2 Usage

5 As shown in

6 Figure 1, the TOE is a virtual appliance that allows administrators to provision data paths between asset sources and storage targets, enabling users to initiate backup and restore operations on user data. Administrators can create protection policies to automate, schedule, and monitor backups for VMware Virtual Machines.

7 Self-service users can perform on-demand backup and restore operations using a Web GUI or REST API. Administrators can manage the TOE using the Web GUI and REST API. A CLI provides access to the underlying SLES15 SP4 operating system used during installation and configuration.

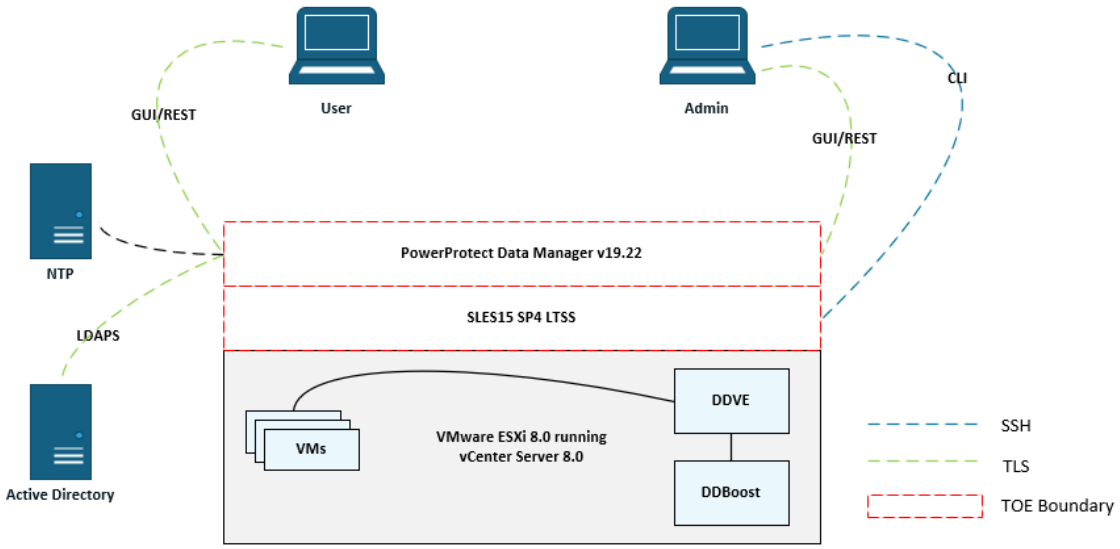

Figure 1: Example TOE Deployment

2.3 Security Functions

8 The TOE provides the following security functions:

a) **Security Audit.** Audit entries are generated for security related events. The audit logs may be reviewed and filtered by authorized administrators.

b) **User Data Protection.** The TOE provides role-based access control capabilities to ensure that only authorized administrators are able to administer the TOE. Only users with the appropriate role may perform backup and restore operations. Retention periods can be associated with protection policies on stored backup data.

c) **Identification & Authentication.** Users are identified and authenticated prior to being granted access to TOE functions. Local and LDAP authentication is supported in the evaluated configuration.

d) **Security Management.** The TOE provides management capabilities via a web based Graphical User Interface (GUI), a CLI and REST API. Management functions allow the administrators to manage access control, configure system settings, and view audit records.

e) **Trusted Path/Channels.** Communications between the TOE and remote administrators is protected using TLS (Web GUI and REST API) and SSHv2 (CLI). Communications between the TOE and self-service users is protected using TLS (Web GUI and REST API). Communications between the TOE and the Active Directory server are protected using TLS.

2.4 Physical Scope

9 The physical boundary of the TOE is the PowerProtect Data Manager v19.22 software packaged with the SLES15 SP4 operating system. The TOE runs as a virtual appliance on a VMware ESXi 8.0 Hypervisor running vCenter Server 8.0, on general-purpose server hardware.

2.4.1 TOE Delivery

10 The TOE software is downloaded as an Open Virtual Appliance (OVA) from the Dell Support portal. Downloads are available to logged-in customers at https://www.dell.com/support.

2.4.2 Guidance Documents

11 The following guidance documentation is provided in PDF format and available to customers upon request:

a) PowerProtect Data Manager 19.22 Administrator Guide, February 2026, Rev.02

b) PowerProtect Data Manager 19.22 Deployment Guide, February 2026, Rev.02

c) PowerProtect Data Manager 19.22 Security Configuration Guide, November 2025, Rev. 01

d) PowerProtect Data Manager 19.22 VMware Virtual Machine User Guide, November 2025, Rev. 01

12 The TOE also includes the following REST API guide, available online at: https://developer.dell.com/apis/4378/versions/19.22.0/docs/introduction.md

a) PowerProtect Data Manager (V19.22.0) REST API

13 **Note**: The latest revisions of all documentation is provided in HMTL format from the Dell Info Hub: https://www.dell.com/support/kbdoc/en-ca/000196987/dell-powerprotect-data-manager-info-hub-product-documents-and-information.

14 The TOE also includes the following Common Criteria Guide, available to customers in PDF upon request to their Dell account team:

- Dell PowerProtect Data Manager v19.22 Common Criteria Guide, Version 1.7

2.4.3 Non-TOE Components

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

a) **Hardware**. General purpose server hardware.

b) **VMware ESXi 8.0 Hypervisor**. The virtualization platform on which the TOE operates. Supports the TOE-protected virtual machines.

c) **vCenter Server 8.0**. ESXi administration server.

d) **User Workstation**. General purpose computing platform. Supports user backup and restore operations.

e) **Management Workstation**. General purpose computing platform. Supports TOE administration.

f) **DDVE**. Data Domain virtual appliance running DDVE v8.3. Virtual data storage supporting backup and recovery.

g) **DD Boost**. SLES15 SP4 hosting DD Boost 8.6. Supports backup and recovery.

h) **Active Directory**. Windows Server 2022 running Active Directory for user authentication.

i) **NTP**. Provides the NTP service supporting time stamps for audit records and determining retention periods.

2.4.4 Excluded Functionality

16 The following features are excluded from this evaluation:

a) Log offloading

b) SupportAssist

c) Data Deduplication

d) Data Replication

17 **Note**: Data deduplication and replication functionality is provided by DDVE and DD Boost in the operational environment and is not included in evaluated configuration.

18 The following asset types are also supported by the TOE but are excluded from this evaluation:

- File Systems
- Kubernetes Clusters
- MS Exchange Server and SQL Server Databases
- Oracle Databases
- SAP HANA Databases
- Network-Attached Storage (NAS) Shares
- PowerStore, PowerMax, and VMAX Storage

2.5 Logical Scope

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

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
T.ACCOUNT	An unauthorized user could gain access to TOE configuration information or perform operations for which no access rights have been granted.
T.DATALOSS	Failure of infrastructure, human error, or malicious attack may result in the loss of critical user data.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.UNDETECT	Users (unauthorized or authorized) may be able to access TOE data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.

3.2 Assumptions

Table 4: Assumptions

Identifier	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.STORAGE	The TOE will rely on external storage for maintaining backup and recovery data.
A.TIME	The TOE will rely on the operational environment for reliable time.
A.USER	Non-administrative users of the TOE are trusted and follow all guidance.

3.3 Organizational Security Policies

Table 5: Organizational Security Policies

Identifier	Description
P.REPO	The data repository shall secure the user data in a manner sufficient with common security practices and will only be used to support the TOE backup and recovery operations.
P.RETAIN	The TOE shall provide a means to identify a retention period before which data is not to be deleted, and prevent data from being deleted prior to the expiry of the retention period.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical and logical attack.
OE.STORAGE	Storage repositories used for backup and recovery data will be provided by the operational environment.
OE.TIME	The TOE environment will provide reliable time.
OE.USER	Non-administrative users of the TOE shall be trustworthy and follow all guidance.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the users of the TOE and administrators in their management of the security functions provided by the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit events for changes to the TOE configuration, and use of the TOE data channels. Audit records must be readable by authorized administrators.
O.IDAUTH	The TOE must ensure that users are identified and authenticated prior to allowing access to the administrative functions and data of the TOE.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators, self-service users, and LDAP authentication.
O.RECOVERY	The TOE shall provide a mechanism to recover data from critical loss.
O.REPO	The TOE must provide a mechanism for defining storage repositories used for backup and recovery data.
O.RETAIN	The TOE must prevent the deletion of user data prior to expiry of the assigned retention period.

5 Security Requirements

5.1 Conventions

20 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 adding a number with parenthesis (e.g. “FDP_ACC.1(2)”).

5.2 Extended Components Definition

21 Table 8 identifies the extended components which are incorporated into this ST.

Table 8: Extended Components

Component	Title	Rationale
FDP_REC_EXT.1	Backup and Recovery of Data	No existing CC Part 2 SFRs address the requirement to perform backup and recovery operation on user data. A new family was created within the User Data Protection (FDP) class to address the backup and recovery of user data.
FDP_REC_EXT.2	Self-Service Backup and Recovery of Data	
FDP_RET_EXT.1	Retention of Data	No existing CC Part 2 SFRs address retention requirements for stored data. A new family was created within the User Data Protection (FDP) class to address the retention of data.

5.2.1 Backup and Recovery (FDP_REC_EXT)

5.2.1.1 Family Behavior

22 This family provides requirements that address backup and recovery of user data, asset discovery, and storage management.

5.2.1.2 Component Leveling

5.2.1.3 Management: FDP_REC_EXT.1

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

a) Manage asset sources.
b) Manage protection storage.
c) Manage protection policies.
d) Backup and restore operations.

5.2.1.4 Audit: FDP_REC_EXT.1

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

a) Changes to asset sources.
b) Changes to protection storage.
c) Changes to protection policies.
d) Backup and restore operations.

FDP_REC_EXT.1 Backup and Recovery of Data

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset Access Control
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security Roles

FDP_REC_EXT.1.1 The TSF shall allow discovery of data assets and storage targets.

FDP_REC_EXT.1.2 The TSF shall provide administrators with the ability to configure the data path.

FDP_REC_EXT.1.3 The TSF shall provide administrators with the ability to initiate backup and restore operations on all user data.

5.2.1.5 Management: FDP_REC_EXT.2

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

a) None specified.

5.2.1.6 Audit: FDP_REC_EXT.2

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

a) Backup and restore operations.

FDP_REC_EXT.2 Self-Service Backup and Recovery of Data

Hierarchical to: No other components.

Dependencies: FDP_REC_EXT.1 Backup and Recovery of Data

FDP_REC_EXT.1.1 The TSF shall allow users to initiate on-demand backup and restore operations on personal user data.

5.2.2 Retention of Data (FDP_RET_EXT.1)

5.2.2.1 Family Behavior

27 This family provides requirements that address retention of user data while it is stored within containers controlled by the TOE Security Functionality (TSF).

5.2.2.2 Component Leveling

5.2.2.3 Management: FDP_RET_EXT.1

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

a) Setting the retention period.

5.2.2.4 Audit: FDP_RET_EXT.1

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

a) Minimal: changes to the retention period.

FDP_RET_EXT.1 Retention of data

Hierarchical to:	No other components.
Dependencies:	FDP_REC_EXT.1 FPT_STM.1
FDP_RET_EXT.1.1	The TSF shall allow a retention period to be assigned to protected user data.
FDP_RET_EXT.1.2	Where a retention period has been assigned to user data, the TSF shall deny requests to delete the data until the retention period has expired, or has been removed.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FDP_ACC.1(1)	Subset access control (Users)
FDP_ACC.1(2)	Subset access control (Administrators)
FDP_ACF.1(1)	Security attribute based access control (Users)
FDP_ACF.1(2)	Security attribute based access control (Administrators)
FDP_REC_EXT.1	Backup and recovery of data
FDP_REC_EXT.2	Self-service backup and recovery of data
FDP_RET_EXT.1	Retention of data
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
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 audit data 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;

c) *[user login, user configuration changes, asset configuration changes, storage configuration changes, protection policy configuration changes, backup and restore operations].*

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

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

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

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

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 [*authorized users]* with the capability to read [*all audit information]* from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit data 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 (Users)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*Backup and Restore SFP*] on
[*Subjects: Users*[2]*, Administrators*[3]
Objects: virtual machines
Operations: view, backup, restore]

FDP_ACC.1(2) Subset access control (Administrators)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*Management Access Control SFP*] on
[*Subjects: Administrators*
Objects: Security Management data and functions
Operations: view, create, modify, delete].

FDP_ACF.1(1) Security attribute based access control (Users)

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the [*Backup and Restore SFP*] to objects based on the following: [
Subjects: Users, Administrators
Subject attributes: role, resource group
Objects: virtual machines
Object 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: [*a user or administrator may perform backup and restore operations if the user is assigned to a role that permits access and belongs to the appropriate resource group*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*an authorized user or administrator assigned to the appropriate role and resource group may perform backup operations on virtual machines if a data path exists between the asset and the storage target*].

[2] Users are non-administrators with the ability to perform on-demand backup and restore operations on their own user data.

[3] Administrators have the ability to configure scheduled backup and restore operations on all user data.

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

FDP_ACF.1(2) Security attribute based access control (Administrators)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [*Management Access Control SFP*] to objects based on the following: [*Subjects: Administrators* *Subject attributes: role, resource group* *Objects: security management data and functions* *Object 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 administrator may access security management data and functions if the user is assigned to a role that permits access and belongs to the appropriate resource group].*
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_REC_EXT.1 Backup and Recovery of Data

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FDP_REC_EXT.1.1	The TSF shall allow discovery of data assets and storage targets.
FDP_REC_EXT.1.2	The TSF shall provide administrators with the ability to configure the data path.
FDP_REC_EXT.1.3	The TSF shall provide administrators with the ability to initiate backup and restore operations on all user data.

FDP_REC_EXT.2 Self-Service Backup and Recovery of Data

Hierarchical to:	No other components.
Dependencies:	FDP_REC_EXT.1 Backup and Recovery of Data
FDP_REC_EXT.1.1	The TSF shall allow users to initiate on-demand backup and restore operations on personal user data.

FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FDP_REC_EXT.1

FPT_STM.1

FDP_RET_EXT.1.1 The TSF shall allow a retention period to be assigned to protected user data.

FDP_RET_EXT.1.2 Where a retention period has been assigned to user data, the TSF shall deny requests to delete the data until the retention period has expired, or has been removed

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 users: [

- *Username*
- *Password*
- *Role*
- *Resource Group*

].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*the following minimum requirements:*

- *contains a minimum of nine characters to a maximum of 100 characters*
- *contains at least one numeric character*
- *contains at least one uppercase character*
- *contains at least one lowercase character*
- *contains at least one special character from the list of the following acceptable characters:*
  - !@#$%^&*()_-+=~{}[]<>?/`:;',.|\" (*spaces are also allowed)*
- *contains only letters from the English alphabet*

- *does not contain other sensitive information associated with user account such as first and last names, username, or email address*].

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_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*the following authentication mechanisms:*

- *Local authentication*
- *LDAP authentication*

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following rules:*

- *Local authentication – The username and password entered matches the local accounts database.*
- *LDAP authentication – The username and password entered matches a valid domain username and the password stored in the Active Directory server.*

].

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 TSF-mediated actions on behalf of that user.

5.3.4 Security Management (FMT)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Management Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes

[

- *Create, view, edit, delete identity providers*
- *Create, view, edit, and delete users*
- *Create, view, edit, and delete assets*
- *Add, view, edit, and delete protection policy assets*
- *Create, view, edit, and delete asset sources*
- Create, view, edit, and delete resource groups
- *Create, view, edit, and delete asset hosts*
- *Create, view, edit, and delete storage targets*
- *Create, view, edit, and delete protection policies*
- *Create, view, edit, and delete retention policies*

]
to [*users assigned the appropriate role as defined in Table 11*].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

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

FMT_MSA.3.2 The TSF shall allow the [*administrator assigned the appropriate role*] 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: [*view audit records, view assets, manage assets, view asset sources, manage asset sources, view host, manage host, view storage targets, manage storage targets, view protection policies, manage protection policies, view copies, manage copies, manage users, configure authentication providers, view resource groups, manage resource groups, perform on-demand backup operations, perform on-demand restore operations, monitor backup jobs*].

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 [*root, admin, support, Administrator, Security Administrator, Backup Administrator, Restore Administrator, User, Backup Operator, Restore Operator*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.3.5 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 [*communication with an external authentication server*].

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 of the TOE, self-service backup and restore operations*]

5.4 Assurance Requirements

30 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2+ (ALC_FLR.2).

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

6.1 Security Audit

Related SFRs: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1

31 The TOE generates audit records for the following events:

- startup and shutdown of its audit functions
- user login
- user configuration changes (add, modify, delete)
- asset configuration changes (add, modify, delete)
- storage configuration changes (add, modify, delete)
- protection policy configuration changes (add, modify, delete)
- backup and restore operations

32 Each audit record includes the date and time of the event, type of event, outcome of the event, and the user identity associated with the event (if applicable). All audit records are presented in a manner suitable for administrators to interpret the information. With the exception of OS-level login/logout events and startup/shutdown of the audit functions, only authorized administrators assigned the Administrator, Security Administrator, and User role may view all audit records via the Web GUI. OS-level login/logout events and startup/shutdown of the audit functions are recorded and viewed over the CLI. The root, admin, and Support roles may view these records.

33 The TOE requires that a Network Time Protocol (NTP) service be available. Time from the NTP service is used by the TOE to provide reliable time stamps on audit records.

6.2 User Data Protection

Related SFRs: FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(2), FDP_ACF.1(2), FDP_REC_EXT.1, FDP_REC_EXT.2, FDP_RET_EXT.1

34 The TOE enforces the Management Access Control SFP on the administrative functions. Only administrators assigned the appropriate role and resource group have access to management functions and data as defined in Table 11 below. At a high level, the following roles and associated privileges are provided by default:

Administrator - Responsible for setup, configuration, and all PowerProtect Data Manager management functions. The Administrator role provides systemwide access to all functionality.

Security Administrator - Manages user accounts and roles, privileges, audit logs, and authentication sources.

Backup Administrator - Can backup assets and manage copies at the asset level but cannot back up at the protection policy level.

Restore Administrator - Responsible for completing restore operations using backups that exist in protection storage and with resources that the system administrator has already configured.

Backup Operator – Perform on-demand backup operations on individual VMs.

Restore Operator – Perform on-demand restore operations on protected backups.

User - Provides read-only access to monitor activities and operations.

35 Before any backup and restore operations can be performed, an authorized administrator must configure the following:

- Protection Storage - Protection storage is the set of configured target storage systems where the TOE stores backup copies. DDVE is used as the storage target in the evaluated configuration.
- Asset Host / Assets - Assets reside within the asset host (or source). Asset sources are the mechanism that PowerProtect Data Manager uses to manage assets and communicate with the protection storage where backup copies of the assets are stored. For virtual machines protection, the vCenter server is the asset source and the virtual machines are the assets. When a vCenter server is added as an asset source in PowerProtect Data Manager, an automatic discovery of VMware entity information from the vCenter server is initiated. The initial vCenter server discovery identifies all ESXi clusters, hosts, and virtual machines within the vCenter server.
- Protection Policies - Protection Policies configure and manage the entire life cycle of backup data, which includes backup type, assets, backup start/stop time, backup device, and backup retention.

36 The TOE enforces the Backup and Recovery SFP on both Administrators and Users. Administrators can configure protection policies to run regular backup schedules on all assets and asset sources. Protection policies can specify the policy name, asset, backup schedule, storage target, and retention period. Administrators may also perform restore activities at any time on all backups.

37 Users assigned the Backup Operator and Restore Operator roles have the ability to perform on-demand backup and restore operations on individual VMs, only if an administrator-configured data path exists between the asset and storage target.

6.3 Identification and Authentication

Related SFRs: FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2

38 All users of the TOE (Administrators and self-service users) must successfully identify and authenticate before being granted access to any TOE functions. Authentication is enforced on all user interfaces (Web GUI, REST API, and CLI). Both local and Active Directory authentication are supported in the evaluated configuration. Only local authentication is enforced on the CLI.

39 The TOE maintains the username, password, role, and resource group security attributes for all users. The privileges granted to each user is dependant on their assigned role and resource group, as discussed in section 6.4 below.

40 By default, the TOE maintains the following minimum password requirements:

- contains a minimum of nine characters to a maximum of 100 characters
- contains at least one numeric character
- contains at least one uppercase character
- contains at least one lowercase character
- contains at least one special character from the list of the following acceptable characters:
- !@#$%^&*()_-+=~{}[]<>?/`:;',.|\" (spaces are also allowed)
- contains only letters from the English alphabet

- does not contain other sensitive information associated with user account such as first and last names, username, or email address.

Application Note: Minimum password requirements are only enforced for local accounts. Active Directory only supports the role and resource group attributes for LDAP users. Group-to-role mapping is configured in the evaluated configuration.

6.4 Security Management

Related SFRs: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

41 The TOE restricts access to all management functions and backup/restore operations based on role and assigned resource group. Permissions are additive, so user authorization is the sum of the applicable resource group and role. A resource is an asset on which users can perform operations. A resource group is a construct that enables administrators to manage and refine authorization by tagging related resources to which that authorization should apply. Resource groups define or restrict the scope on which users with a given role can exercise that authority.

42 The default roles and privileges are described in Table 11 below. The default values are considered restrictive in that a user must exist and be assigned the appropriate role and resource group before being granted access to the associated privilege. Only authorized administrators assigned the appropriate role have the ability to override the default values, as described in Table 11.

Table 11: Roles and Privileges

Privilege	Role						
	Administrator	Security Administrator	Backup Administrator	Restore Administrator	User	Backup Operator	Restore Operator
View audit records	Y	Y	N	N	Y	N	N
View Assets	Y	Y	Y	Y	Y	N	N
Manage Assets	Y	N	Y	N	N	N	N
View asset sources	Y	N	Y	Y	Y	N	N
Manage asset sources	Y	N	N	N	N	N	N
View host	Y	N	Y	Y	Y	N	N
Manage host	Y	N	N	Y	N	N	N
View storage targets	Y	N	Y	Y	Y	N	N
Manage storage targets	Y	N	N	N	N	N	N
View protection policies	Y	N	Y	N	Y	N	N

Privilege	Role						
	Administrator	Security Administrator	Backup Administrator	Restore Administrator	User	Backup Operator	Restore Operator
Manage protection policies	Y	N	N	N	N	N	N
View copies	Y	N	Y	Y	N	N	N
Manage copies	Y	N	Y	N	N	N	N
Manage users	Y	Y	N	N	N	N	N
Configure authentication providers	Y	Y	N	N	N	N	N
View resource groups	Y	Y	N	N	N	N	N
Manage resource groups	Y	Y	N	N	N	N	N
On-demand backup operations	N	N	N	N	N	Y	N
On-demand restore operations	N	N	N	N	N	N	Y
View jobs (activities)	Y	N	Y	Y	Y	Y	Y

43 The TOE also comes preloaded with three user accounts providing access to the Linux operating system, as follows:

root – Provides root privilege elevation for CLI commands. To use the root account, login as admin and execute the `su` command.

admin – Provides administrative SSH access to the system console (CLI).

support – Provides SSH view access to the system console (CLI).

44 In the evaluated configuration, the CLI is only used for verification of local login/logout and audit shutdown events as described in Section 6.1 above. The SSH protection mechanisms are described in Section 6.5.2 below. Once deployed, the TOE is managed through the Web GUI and REST API.

6.5 Trusted Path/Channel

Related SFRs: FTP_ITC.1, FTP_TRP.1

6.5.1 Web GUI and REST API Communications

45 All communications with remote administrators via the Web GUI and REST API are protected using TLSv1.2 and TLSv1.3. The following default cipher suites are supported in the evaluated configuration:

TLSv1.2

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLSv1.3

- TLS_WITH_AES_128_GCM_SHA256
- TLS_WITH_AES_256_GCM_SHA384

6.5.2 CLI Communications

46 When the CLI is used, the connection between the Dell PowerProtect Data Manager v19.22 and the remote administrator is protected from modification and disclosure using SSHv2. The TOE supports password-based authentication. The following algorithms are supported in the evaluated configuration:

Encryption Algorithms: aes192-ctr, aes256-ctr, aes128-gcm@openssh.com , aes256-gcm@openssh.com.

MAC Algorithms: hmac-sha2-256, hmac-sha2-512.

Key Exchange Algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512

Server Host Keys: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256

6.5.3 Active Directory Communications (LDAP Authentication)

47 TOE communications with the external Active Directory (LDAP) server are protected using TLSv1.2 and TLSv1.3. The following cipher suites are supported in the evaluated configuration:

TLSv1.2

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLSv1.3

- TLS_WITH_AES_128_GCM_SHA256
- TLS_WITH_AES_256_GCM_SHA384

7 Rationale

7.1 Security Objectives Rationale

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

Table 12: Security Objectives Mapping

	T. ACCOUNT	T.DATALOSS	T.EAVES	T. UNDETECT	P.REPO	P.RETAIN	A. LOCATE	A. MANAGE	A.STORAGE	A.TIME	A.USER
O.ADMIN	X										
O.AUDIT				X							
O.IDAUTH	X										
O.PROTCOMMS			X								
O.RECOVERY		X									
O.REPO					X						
O.RETAIN						X					
OE.ADMIN								X			
OE.PHYSICAL							X				
OE.STORAGE									X		
OE.TIME				X						X	
OE.USER											X

49 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.ACCOUNT	**O.ADMIN** mitigates this threat by ensuring that access to the security functions of the TOE is restricted to authorized users. **O.IDAUTH** mitigates the threat by providing the means for users to authenticate prior to gaining access to the functions assigned to that user.
T.DATALOSS	**O.RECOVERY** mitigates this threat by providing backup and restore mechanisms for critical user data.
T.EAVES	**O.PROTCOMMS** mitigates this threat as it requires the TOE to encrypt communications with remote administrators, self-service users, and external authentication providers.
T.UNDETECT	**O.AUDIT** mitigates this threat by ensuring that audit records are generated for security relevant events. **OE.TIME** supports the O.AUDIT objective by providing accurate time for those audit records.
P.REPO	**O.REPO** supports this policy by ensuring that administrators of the TOE can define an appropriate storage repository to backup data.
P.RETAIN	**O.RETAIN** supports this policy by ensuring that the TOE prevents deletion of user data prior to expiry of the assigned retention period.
A.LOCATE	**OE.PHYSICAL** supports this assumption by ensuring that the operational environment provides physical and logical protection of the TOE.
A.MANAGE	**OE.ADMIN** supports this assumption by ensuring the availability of trained, competent administrators who are trustworthy and not malicious.
A.STORAGE	**OE.STORAGE** supports this assumption by ensuring the operational environment provides adequate and reliable storage for all user data backups.
A.TIME	**OE.TIME** supports this assumption by ensuring that an NTP service is configured, providing the TOE with reliable time.
A.USER	**OE.USER** supports this assumption by ensuring that self-service users of the TOE are trustworthy, trained, and follow all guidance.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

50 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.PROTCOMMS	O.RECOVERY	O.REPO	O.RETAIN
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAR.1		X					
FDP_ACC.1(1)	X						
FDP_ACC.1(2)	X					X	
FDP_ACF.1(1)	X						
FDP_ACF.1(2)	X					X	
FDP_REC_EXT.1					X		
FDP_REC_EXT.1					X		
FDP_RET_EXT.1							X
FIA_ATD.1			X				
FIA_SOS.1			X				
FIA_UAU.2			X				
FIA_UAU.5			X				
FIA_UID.2			X				
FMT_MSA.1	X					X	

	O. ADMIN	O. AUDIT	O. IDAUTH	O.PROTCOMMS	O.RECOVERY	O.REPO	O.RETAIN
FMT_MSA.3	X					X	
FMT_SMF.1	X					X	
FMT_SMR.1	X					X	
FTP_ITC.1				X			
FTP_TRP.1				X			

Table 15: Suitability of SFRs

Objectives	SFRs
O.ADMIN	**FDP_ACC.1(1/2), FDP_ACF.1(1/2)** ensure that only users and administrators assigned the appropriate role have access to the privileged functions provided by the TOE. **FMT_MSA.1** ensures that access to the security attributes supporting access control functions is restricted to authorized administrators. **FMT_MSA.3** ensures that default values for the security attributes that make up that TSF data are restrictive. **FMT_SMF.1** provides functionality to support the management of the TOE and TOE users. **FMT_SMR.1** provides the security roles for TOE administrators.
O.AUDIT	**FAU_GEN.1, FAU_GEN.2** outline what data must be included in audit records and what events must be audited. **FAU_SAR.1** provides the means to review audit records.

Objectives	SFRs
O.IDAUTH	**FIA_ATD.1** meets this objective by ensuring that the TOE maintains appropriate security attributes for authenticated users. **FIA_SOS.1** meets this objective by ensuring that user passwords are of sufficient strength. **FIA_UAU.2** meets this objective by ensuring that TOE users are successfully authenticated before gaining access to TOE functions and data. **FIA_UAU.5** meets the objective by ensuring local and Active Directory authentication mechanisms are used. **FIA_UID.2** meets this objective by ensuring that the identity of each TOE user is known before allowing access to TOE functions and data.
O.PROTCOMMS	**FPT_ITC.1** meets this objective by ensuring that the TOE encrypts communications with an external authentication server. **FTP_TRP.1** meets this objective by ensuring that the TOE encrypts communications with remote administrators and self-service users.
O.RECOVERY	**FDP_REC_EXT.1, FDP_REC_EXT.2** meet this requirement by providing the ability to perform backup and restore operations on critical user data.
O.REPO	**FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1** meet this requirement by providing the capabilities and appropriate roles used to manage storage targets for data backup and recovery operations. **FDP_ACC.1(2) and FDP_ACF.1(2)** supports this objective by enforcing the management access controls to ensure only authorized administrators can configure storage targets.
O.RETAIN	**FDP_RET_EXT.1** ensures that data is not deleted prior to the expiry of the retention period.

Table 16: Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Not met, as the TOE relies on the operational environment for time.
FAU_GEN.2	FAU_GEN.1	Met
	FIA_UID.1	Met
FAU_SAR.1	FAU_GEN.1	Met

SFR	Dependency	Rationale
FDP_ACC.1(1)	FDP_ACF.1	Met by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	Met by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1	Met by FDP_ACC.1(1)
	FMT_MSA.3	Met
FDP_ACF.1(2)	FDP_ACC.1	Met by FDP_ACF.1(2)
	FMT_MSA.3	Met
FDP_REC_EXT.1	FDP_ACC.1	Met by FDP_ACC.1(1)
	FMT_SMF.1	Met
	FMT_SMR.1	Met
FDP_REC_EXT.2	FDP_REC_EXT.1	Met
FDP_RET_EXT.1	FDP_REC_EXT.1	Met
	FPT_STM.1	Not met, as the TOE relies on the operational environment for time.
FIA_ATD.1	None	-
FIA_SOS.1	None	-
FIA_UAU.2	FIA_UID.1	Met
FIA_UAU.5	None	-
FIA_UID.2	None	-
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1(2)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met

SFR	Dependency	Rationale
FTP_ITC.1	None	-
FTP_TRP.1	None	-