CC Huawei OceanProtect Software 1.6.0 Security Target

Issue	**1.10**
Date	**2025-12-09**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy*. For details about this policy, visit the following web page:

https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page:

https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:

https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:

https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:

https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

About This Document

Change History

Date	Issue	Change Description	Author
2025-12-09	1.10	Public Version	Huawei Technologies Co., Ltd.

Contents

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title: CC Huawei OceanProtect Software 1.6.0 Security Target

Version: 1.10

Date: 2025-12-09

Developer: Huawei Technologies Co., Ltd.

1.2 TOE REFERENCE

The TOE is identified as follows:

TOE name: Huawei OceanProtect Software

TOE version: 1.6.0

Series: X Series, E Series

Developer: Huawei Technologies Co., Ltd.

NOTE

Huawei OceanProtect software includes OceanProtect DataBackup and OceanProtect Storage, both of which are version 1.6.0. Both OceanProtect DataBackup and OceanProtect Storage are part of the OceanProtect software, and there is a slight difference in their version information display.DeviceManager is the web console for OceanProtect Storage, displaying version "v1.6.0". ProtectManager is the web console for

OceanProtect DataBackup, displaying version "OceanProtect DataBackup 1.6.0 ".

1.3 TOE OVERVIEW

This section provides the usage and major security features of the TOE, as well as the TOE type and major non-TOE hardware/software required by the TOE.

As the next-generation intelligent all-flash storage benchmark, the Huawei OceanProtect is designed to back up data of mission-critical services in data centers of large enterprises in especially financial and manufacturing industries.

Based on end-to-end acceleration and the active-active high-reliability architecture, Huawei OceanProtect features rapid backup, rapid recovery, efficient reduction, and high reliability. With the fastest recovery speed, it can help users achieve efficient backup and recovery and greatly reduce the TCO. It is widely used in industries such as government, finance carrier, healthcare, and manufacturing.

Major security features of OceanProtect is as follow:

- Backup and recovery of user data
- Audit generation and reviewing functions
- Secure, role-based administration with access control
- Identification and authentication

1.4 TOE DESCRIPTION

The TOE is defined as Huawei OceanProtect software, which runs on specific hardware devices, and its boundary will be described in more detail in the next chapter. The TOE runs on the entire X series and E series of Huawei OceanProtect. All products of the series run the same software and differ only in storage and computing resources. The evaluated types of Huawei OceanProtect are:

- X Series: X3000, X6000, X8000, X9000
- E Series: E1000, E6000, E8000

1.4.1 TOE Physical Scope

The TOE is made up of the OceanProtect DataBackup, OceanProtect Storage System, and PAM, OpenSSH,and lftp components in the Euler OS. The Client on Windows and Linux is out of the TOE range. The components are described in as follow, and depicted in Figure 1-1.

Table 1-1 TOE Subsystems

Subsystem	**Description**
OceanProtect DataBackup (hereinafter **DataBackup)**	The **DataBackup** software, version 1.6.0. This software component is used to manage the backups, archives, and restores. The software contains the backup catalog, which contains the

Subsystem	Description
	internal database with information about OceanProtect' s backed-up data and configuration. The ProtectManager is a web console for backup management, which is part of **Databackup.** In the X series, the OceanProtect Databackup software is deployed on Huawei OceanProtect Storage. In the E series, the OceanProtect Databackup is deployed on the Huawei Taishan server.
OceanProtect Storage System (hereinafter **Storage**)	The **Storage** software, version 1.6.0. This software component is deployed on OceanProtect Backup Storage Hardware Platform, which is designed to manage the storage hardware. The DeviceManager is a web console in the **Storage**, which is designed to simplify configuration and management of storage systems. The administrator can redirection to the DeviceManager through ProtectManager.
Euler OS	The TOE including Linux operating system (Euler OS V2.0 SP12) based on kernel 5.10 (Euler OS Kernel Version 5.10.0-136.12.0.86.h1425.eulerosv2r12) is running underlying hardware.

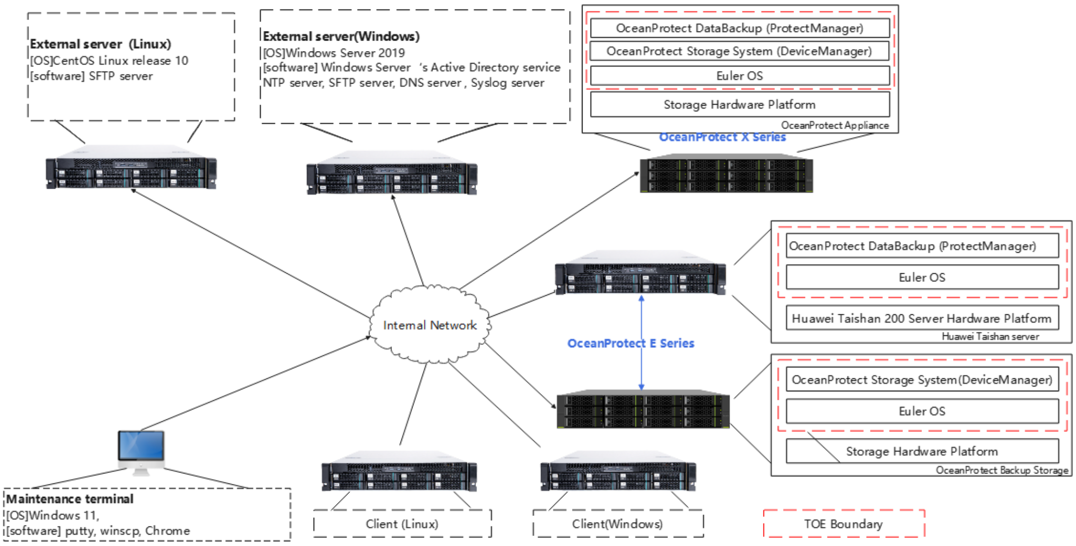
Table 1-2 Non-TOE scope

Non-TOE	Description
Client	The data protect client software, is required for backup of host files and databases on hosts. The client software to be installed is determined based on the type of applications to be protected, and application data protection is implemented on the hosts. The client software to be installed in Windows or Linux OS. The minimum version of Windows is windows server 2016 x86_64. For Linux systems, different Linux distributions are compatible with different minimum versions. The minimum version of Oracle Linux is Oracle Enterprise Linux 7.4 ; The minimum version of SUSE Linux is SUSE Linux Enterprise Server 11. The minimum version of Red Hat Linux is Red Hat Enterprise Linux 6.4. The minimum version of Rocky Linux is Rocky Linux 9.4. The minimum version of CentOS Linux is CentOS 6. The minimum version of Alma Linux is Alma Linux 8.5. For client deployed on Windows OS, the CIFS client can access files on the TOE through CIFS protocol. For client deployed on Linux OS, the

Non-TOE	Description
	TOE provides NFS protocol for backup data.
The OceanProtect Backup Storage Hardware Platform	The storage hardware platform for OceanProtect, on which the Storage software runs.
Huawei Taishan Server Hardware Platform	The Taishan server hardware is an arm-based server platform developed by Huawei, which have a 2U 2-socket rack server with 64 cores. It is designed to provide high performance, low power consumption, and easy to manage and deploy.
External server（Windows）	Hardware Rack servers or PCs with at least one 100M/1G Ethernet port. Software Windows Server 2019 OS natively incorporated LDAP service which is in Windows Server’s Active Directory service.NTP server, SFTP server, DNS server , Syslog server in Windows Server 2019 SAML IDP server
External server（Linux）	CentOS Linux release 10 SFTP server
Maintenance terminal	Hardware Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial DB9 port Software Windows 11 OS Brower Google Chrome 64+ JRE (Java Runtime Environment 1.8), PuTTY 0.83(Used for accessing SSH and SFTP interfaces), WinSCP 6.5, Python 3.9.5, notepad ++, Postman(Used for accessing RESTful interfaces), Foxmail

During a backup, the Client sends backup data across the network to **DataBackup**. The **DataBackup** manages the backup task that is specified in the backup policy. During a restore, administrators can browse, and then select the backed-up data to recover.

Figure 1-1 TOE Diagram


External server (Linux)
[OS]CentOS Linux release 10
[software] SFTP server
External server(Windows)
[OS]Windows Server 2019
[software] Windows Server 's Active Directory service
NTP server, SFTP server, DNS server , Syslog server
OceanProtect DataBackup (ProtectManager)
OceanProtect Storage System (DeviceManager)
Euler OS
Storage Hardware Platform
OceanProtect Appliance
OceanProtect X Series
Internal Network
OceanProtect DataBackup (ProtectManager)
Euler OS
Huawei Taishan 200 Server Hardware Platform
Huawei Taishan server
OceanProtect E Series
OceanProtect Storage System(DeviceManager)
Euler OS
Storage Hardware Platform
OceanProtect Backup Storage
Maintenance terminal
[OS]Windows 11,
[software] putty, winscp, Chrome
Client (Linux)
Client(Windows)
TOE Boundary

In the X series, both the OceanProtect **DataBackup** software and the **Storage** software are deployed on Huawei OceanProtect Appliance. One appliance device can manage and store backup copies at the same time.

In the E series, the OceanProtect **DataBackup** is deployed on the Huawei Taishan 200 server, a 2U 2-socket rack server with 64 cores. One OceanProtect **DataBackup** can manage multiple OceanProtect **Storage**. The **Storage** runs on the OceanProtect media storage hardware platform.

In addition, the software package and the guidance documentation are delivered to the customer site by downloading from support website. The guidance documentation has been published to the OceanProtect device's help information. Customers can access it through the OceanProtect system's Web portal under Help -> Online Help. The download links of delivery parts in the table 1-3 can also be obtained via the Huawei TAC service hotline(https://e.huawei.com/en/about/service-hotline) or the sales team.

📖 **NOTE**

Online Help information is built into the software package and updates with software upgrades.

Table 1-3 Document list

Type	Delivery Item	Version
Storage Subsystem Software	OceanProtect_BackupStorage_1.6.0_Software.tgz	1.6.0
DataBackup Subsystem Software	OceanProtect_DataProtect_1.6.0_image_ARM_64.tgz	1.6.0
	OceanProtect_DataProtect_1.6.0_chart_ARM_64.tgz	1.6.0
Product Guidance	CC Huawei OceanProtect Software 1.6.0 AGD_PRE	1.1

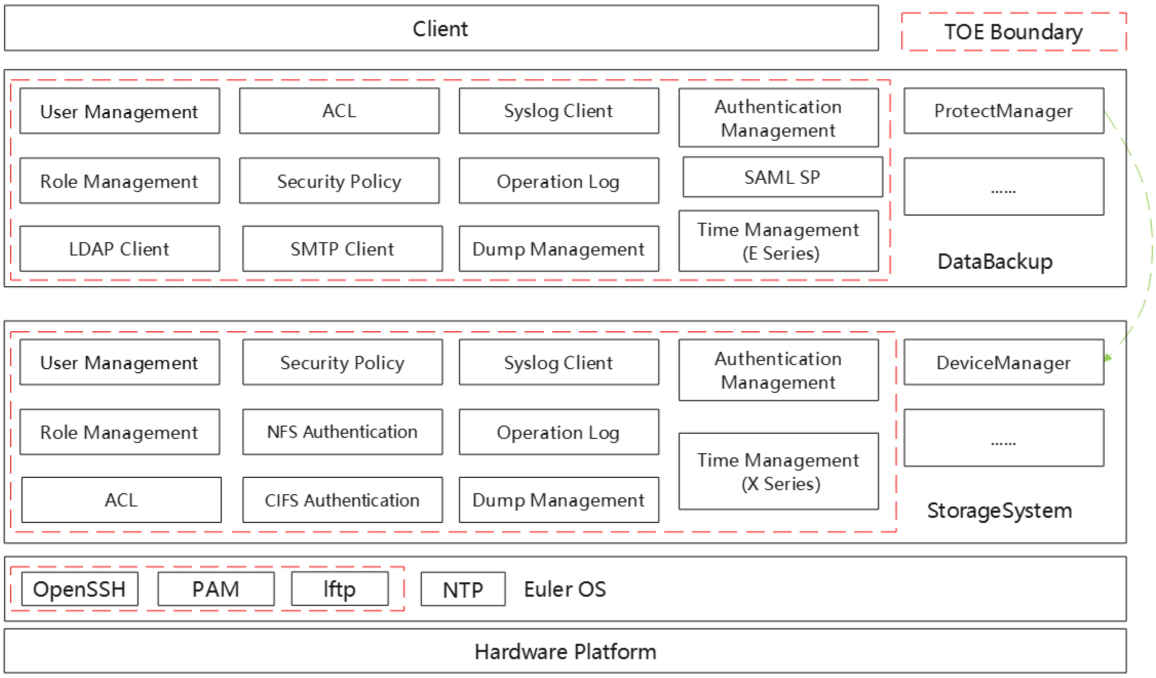
	1.1.pdf	
	CC Huawei OceanProtect Software 1.6.0 AGD_OPE 1.1.pdf	1.1
	OceanProtect DataBackup 1.5.0-1.6.0 Error Code Reference.pdf	01
	OceanProtect Backup Storage 1.x Error Code Reference.pdf	01
	OceanProtect Appliance 1.6.0 REST Interface Reference.pdf	05
	OceanProtect Backup Storage 1.6.0 REST Interface Reference.pdf	02
	OceanProtect DataBackup 1.5.0-1.6.0 Administrator Guide.pdf	09
	OceanProtect DataBackup 1.5.0-1.6.0 Command Reference.pdf	01

1.4.2 TOE Logical Scope

The logical boundary of the TOE includes the interfaces and functions within the physical boundary. The TOE boundary from a logical point of view is represented by the elements that are displayed with a red dotted box within the rectangle in the figure.

The Figure 1-2 reflects the basic structure of the TOE with respect to subsystems and modules. The TOE provides all the security features. Security features are implemented through one or more modules

Figure 1-2 Basic structure of TOE



The logical boundary of the TOE may be broken down by the security features described in 5.2 SECURITY FUNCTIONAL REQUIREMENTS. Table 1-4 summarizes the logical scope of the TOE.

Table 1-4 Logic Scope of the TOE

TOE Security Functionality	Description
Security Audit	Audit entries are generated by TOE for security-related backup events.
Access Control	The TOE provides a role-based access control capability both in **DataBackup** and **Storage**, to ensure that only authorized administrators are able to administer the TOE.
Identification and Authentication	The TOE ensures that users are identified and authenticated prior to being granted access to TOE functions.
Authorization	The TOE ensures that proper permissions is grant to identify sessions which are generated with subset of identified users' attributes
Security Management	The TOE provides management capabilities via ProtectManager. Management functions allow the administrators to configure users and roles, and manage backup and recovery functionality.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST is *CC Part 2 conformant* [CC: 2022, Revision 1, CCMB-2022-11-002], and *CC Part 3 conformant* [CC: 2022, Revision 1, CCMB-2022-11-003].

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

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

2.3 PACKAGE CLAIM

ST claims conformance to the EAL2 augmented by ALC_FLR.2 assurance package.

3 SECURITY PROBLEM DEFINITION

3.1 ASSETS

The threat agents to the TOE are considered to be unauthorized users with public knowledge of how the TOE operates and who possess the skills and resources to alter TOE configuration settings, or parameters, or both. The threat agents do not have physical access to the TOE. The following is an enumeration of the subjects and objects participating in the policy.

TSF data:

- Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
  - User identities.
  - Locally managed passwords.
  - Locally managed access levels.
- Audit data: The data which is provided by the TOE during security audit logging.
  - Audit records.
- Configuration data for the TOE, which is used for configuration data of security features and functions.
- Back up data. An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.

Non-TSF data:

- Configuration data destined to the TOE processed by non-security features and functions.
  - Operation configuration data.
  - Device management configuration data.

3.2 THREATS

This section specifies the threats that are addressed by the TOE.

The threat agents are divided into two categories:

- Non-TOE user or application without rights for accessing the TOE.
- TOE user (a human user, server, or application using the functionality of the TOE).

The threat agents do not have physical access to the TOE.

The following lists the threats that addressed by the TOE

- **T.Un-Auth**
  - **Threat agent:** Non-TOE user or application without rights for accessing the TOE.
  - **Asset:** All assets.
  - **Adverse action:** A non-TOE user gains access to the TOE through LAN.
- **T.Un-Privilege**
  - **Threat agent:** TOE user (a user or application using the functionality of the TOE).
  - **Asset: TSF data**.
  - **Adverse action:** A user of the TOE authorized to perform certain actions and access certain information gains access to unauthorized commands or information through LAN.

3.3 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. The following lists the OSPs presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in a Common Criteria evaluated configuration.

- **P.Auth**
  - The TOE shall be managed only by authorized users.
- **P.Account**
  - The authorized users of the TOE shall be held accountable for their actions within the TOE.
- **P.Leakage**
  - TOE users should avoid incorrect TOE access to prevent data to become corrupted;
  - Non-TOE users or applications should avoid unauthorized data modification, and Inadequate configuration actions through LAN should be avoided.

3.4 ASSUMPTIONS

- **A.Manage**

  It is assumed that the administrators of the TOE are non-hostile, sufficiently trained, and follow all administrator guidance. They will not write down their passwords.
- **A.Physical**

It is assumed that the TOE and its operational environment are protected against unauthorized physical access.

- **A.Network**

  The TOE environment will provide a secure network communication to protect user data that is sent to and received from the TOE.

- **A.Timestamp**

  The TOE environment will provide reliable time to the TOE.

4 SECURITY OBJECTIVES

The security objectives are divided into two solutions, which are the security objectives for the TOE and the security objectives for the operational environment. These solutions are provided by two entities: the TOE and the operational environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

O.Auth

The TOE must require each user/server to be successfully authenticated before allowing any action from user access.

O.Privilege

The TOE must allow authorized users to access only appropriate TOE functions and data. The TOE should implement different authorization roles that can be assigned to administrators in order to restrict the functionality available to individual administrators.

O.Admin

The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.

O.Audit

The TOE must generate audit records for security related events.

O.Protect

The TOE must ensure the integrity of all TSF data, including backup data, audit records, by protecting itself from unauthorized access.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

- **OE.Manage**

  The TOE environment must ensure that the administrators of the TOE is non-hostile, appropriately trained, and follows all administrator guidance. Also, users, applications and servers must be trustworthy when they access the TOE within the local network.
- **OE.Physical**

  The TOE environment should be protected against unauthorized physical access.
- **OE.Network**

  The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
- **OE.TIME**

  The operational environment will provide reliable timestamps to the TOE.

4.3 SECURITY OBJECTIVES RATIONALE

The tracing shows how the security objectives trace back to the threats, OSPs, and assumptions as described in the security problem definition. The security objective rationale also demonstrates that all the given threats, OSPs, and assumptions are addressed.

Table 4-1 Mapping objectives to threats and OSPs

Objective	Threat, OSP, Assumption	Rationale
O.Auth	**T.Un-Auth**	**O.Auth** counters this threat by ensuring that all actions must be after authentication.
	P.Auth	**O.Auth** enforces this policy by ensuring that only authenticated users can manage user data.
	P.Leakage	**O.Auth** enforces this policy by ensuring that only authenticated servers can read and write the user data.
O.Privilege	**T.Un-Privilege**	**O.Privilege** counters this threat by ensuring that all actions must be after authorization.
	P.Account	The TOE must be able to identify users prior to allowing access to TOE functions and data.
	P.Auth	**O.Privilege** enforces this policy by ensuring that allow only authorized users to access only appropriate TOE functions and data.
O.Admin	**T.Un-Auth**	**O.Admin** counters this threat by ensuring that the TOE will provide all the functions necessary to support the administrators in their management of the

Objective	Threat, OSP, Assumption	Rationale
		security of the TOE.
	P.Auth	**O.Admin** enforces this policy by ensuring that the TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE.
O.Audit	**T.Un-Auth**	**O.Audit** counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	T.Un-Privilege	**O.Audit** counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	P.Account	The TOE must generate audit records for security related events.
O.Protect	**T.Un-Auth**	**O.Protect** counters this threat by ensuring that all actions must be after authentication.
	T.Un-Privilege	**O.Protect** counters this threat by ensuring that all actions must be after authorization.
	P.Account	The TOE must generate audit records for security related events.
	P.Auth	**O.Protect** enforces this policy by ensuring that the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.
OE.Manage	**A.Manag**e	**OE.Manage** enforces this policy by ensuring that administrators are trustworthy and competent to operate the TOE and its environment. Also, users, applications and servers are trustworthy while within the local network.
OE.Physical	**A.Physical**	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.Network	**A.Network**	**OE.Network** will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
OE.Time	**A.Timestamp**	**OE.Time** will provide reliable timestamp for the TOE

5 SECURITY REQUIREMENTS

This chapter provides the functional and assurance requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 CONVENTIONS

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

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

5.2 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 5-1 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 5-1 Summary of Security Functional Requirements

Class	Identifier	Name	S	A	R	I
Security Audit (FAU)	FAU_GEN.1	Audit data generation	✓	✓		
	FAU_GEN.2	User identity association				
	FAU_SAR.1	Audit review		✓		
	FAU_SAR.3	Selectable audit review		✓		
User Data Protection (FDP)	FDP_ACC.1	Subset access control		✓		
	FDP_ACF.1	Security attribute based access control		✓		
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action				
	FIA_UID.2	User identification before any action				
Security Management (FMT)	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		✓		

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

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

- Component relationships
  - Hierarchical to: No other components.
  - Dependencies: FPT_STM.1 Reliable time stamps[1]
- **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;

[1] Although FPT_STM.1 is not included, OE.Time ensures that the IT environment provides reliable time for the TOE.

c) [***no other auditable events***].

- **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, [***audit relevant information described in table “****Audit Record Contents in* ***DataBackup” and table “****Audit Record Contents in* ***Storage”***].

5.2.1.2 FAU_GEN.2 User identity association

- Component relationships
  - 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.

5.2.1.3 FAU_SAR.1 Audit review

- Component relationships
  - Hierarchical to: No other components.
  - Dependencies: FAU_GEN.1 Audit data generation
- **FAU_SAR.1.1**

  The TSF shall provide [***the users whose role is System Administrator or Auditor as defined in FMT_SMR.1.1***] 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.

5.2.1.4 FAU_SAR.3 Selectable audit review

- Component relationships
  - Hierarchical to: No other components.
  - Dependencies: FAU_SAR.1 Audit review
- **FAU_SAR.3.1**

  The TSF shall provide the ability to apply [***selection, filtering***] of audit data based on [***Severity, Object, Occurred At, Type and Status for selection and Nodes, Alarm ID for filtering***].

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1 Subset access control

- Component relationships
  - Hierarchical to: No other components.

  - Dependencies: FDP_ACF.1 Security attribute based access control
- **FDP_ACC.1.1**

  The TSF shall enforce the [***Role Based Access Control SFP***] on [

  - ***Subjects: users;***
  - ***Objects: TSF data, backup data;***
  - ***Operations: configure, backup, recover***

  ].

5.2.2.2 FDP_ACF.1 Security attribute-based access control

- Component relationships
  - Hierarchical to: No other components.
  - Dependencies:

    FDP_ACC.1 Subset access control

    FMT_MSA.3 Static attribute
- **FDP_ACF.1.1**

  The TSF shall enforce the [***Role Based Access Control SFP***] to objects based on the following: [

  - ***Subjects: users;***
  - ***Subject attributes: user role;***
  - ***Objects: TSF data, backup data;***
  - ***Object attributes: Resource set***

  ].
- **FDP_ACF.1.2**

  The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***users assigned a role with the appropriate privileges are able to modify TSF data to configure backup and recovery operations***].
- **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***].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_UAU.2 User authentication before any action

- Component relationships
  - 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.

5.2.3.2 FIA_UID.2 User identification before any action

- Component relationships
  - 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.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MSA.1 Management of security attributes

- Component relationships
  - 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 [***Role Based Access Control SFP***] to restrict the ability to [**query, modify, delete, *create***] the security attributes [***mentioned in*** 6.5 SECURITY MANAGEMENT] to [***the authorized roles identified in the table 6-4 and 6-6***].

5.2.4.2 FMT_MSA.3 Static attribute initialisation

- Component relationships
  - 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 [***Role Based 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 [***System Administrator role, Super administrator role which defined in FMT_SMR.1 table 6-4 and table 6-6***] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.3 FMT_SMF.1 Specification of Management Functions

- Component relationships
  - Hierarchical to: No other components
  - Dependencies: No dependencies
- **FMT_SMF.1.1**

The TSF shall be capable of performing the following management functions: [***User Management, User Policy Management, Network Service Management, Audit, Backup Resource Management via ProtectManager***].

5.2.4.4 FMT_SMR.1 Security roles

- Component relationships
  - Hierarchical to: No other components
  - Dependencies: FIA_UID.1 Timing of identification
- **FMT_SMR.1.1**

  The TSF shall maintain the roles [***the authorized roles identified in the table 6-4 and 6-6***].
- **FMT_SMR.1.2**

  The TSF shall be able to associate users with roles.

5.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 5-2.

Table 5-2 TOE security assurance requirements

Assurance Class	Assurance Components	Description
Development(ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents(AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support(ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security target evaluation(ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements

Assurance Class	Assurance Components	Description
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests(ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment(AVA)	AVA_VAN.2	Vulnerability analysis

5.4 SECURITY REQUIREMENTS RATIONALE

The evaluation assurance level 2+ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE. EAL2 provides suitable assurance for commercial requirements while ALC_FLR.2 makes sure that the flaws identified are being handled properly.

The following table provides a mapping of SFRs to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 5-3 Mapping SFRs to objectives

Objective	Security Functional Requirement	Rationale
O.Auth The TOE must require each user/server to be successfully authenticated before allowing any action from user access.	FIA_UAU.2	The requirement meets the objective by ensuring that the TOE authenticates each user before any action.
	FIA_UID.2	The requirement meets the objective by ensuring that the TOE identifies each user before any action.
	FMT_SMF.1	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
O.Privilege	FDP_ACC.1	The requirement meets the objective by ensuring that

Objective	Security Functional Requirement	Rationale
The TOE must allow authorized users to access only appropriate TOE functions and data.		the TOE has an access control policy that allows only authorized users to gain data from the TOE.
	FDP_ACF.1	The requirement meets the objective by ensuring that only authorized users gain access to data protected by the TOE.
	FIA_UID.2	The requirement meets the objective by ensuring that the TOE identifies each user before any action.
	FMT_MSA.1	The requirement meets the objective by ensuring that the security attributes of users in the TOE can be changed only by authorized users.
	FMT_SMF.1	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
	FMT_SMR.1	The requirement meets the objective by ensuring that specific roles are defined for management of the TOE.
O.Admin The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.	FAU_SAR.1	This requirement meets the objective by ensuring that the audit review functionality can be managed.
	FMT_MSA.1	The requirement meets the objective by defining the access permissions each role has to the security attributes of the SFP.
	FMT_MSA.3	The requirement meets the objective by ensuring that the default values for security attributes of users in the TOE can be managed.
	FMT_SMF.1	The requirement meets the objective by ensuring that the TOE manages the

Objective	Security Functional Requirement	Rationale
		authentication policy of users.
O.Audit The TOE must generate audit records for security related events.	FAU_GEN.1	The requirement meets the objective by ensuring that the TOE generates audit records of security related events.
	FAU_GEN.2	The requirement meets the objective by ensuring that the audit functionality is able to associate audit records with the identity of the user whose actions generate such records.
	FAU_SAR.1	The requirement meets the objective by ensuring that all audit records can be reviewed by authorized users in a suitable format.
	FAU_SAR.3	The requirement meets the objective by ensuring that authorized users have access to the audit records.
	FMT_SMF.1	The requirement meets the objective by ensuring that the TOE manages the audit configuration of servers.
O.Protect The TOE must ensure the integrity of all TSF data, including backup data, audit records, by protecting itself from unauthorized access.	FDP_ACC.1	The requirement meets the objective by ensuring that the TOE has an access control policy that allows only authorized users to gain data from the TOE.
	FDP_ACF.1	The requirement meets the objective by ensuring that only authorized users gain access to data protected by the TOE.
	FIA_UAU.2	The requirement meets the objective by ensuring that the TOE authenticates each user before any action.
	FIA_UID.2	The requirement meets the objective by ensuring that the TOE identifies each user

Objective	Security Functional Requirement	Rationale
		before any action.
	FMT_MSA.1	The requirement meets the objective by providing the functionality that determines the attributes used by the access control policy..
	FMT_SMF.1	The requirement meets the objective by ensuring that the TOE manages the authentication policy of users.
	FMT_SMR.1	The requirement meets the objective by ensuring that specific roles are defined for management of the TOE.

6 TOE SUMMARY SPECIFICATION

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

6.1 SECURITY AUDIT

The TOE provides an audit trail for all essential operations and alarms.

Different audit components run on **DataBackup**, **Storage** and **Euler OS**. Auditing is enabled by default, and cannot be turned off. All non-query operations will be recorded in the operation logs. Typically, these operations include startup and shutdown of the TOE, login, logout, configuration change, user management, and security settings. All audit trails are stored locally in the TOE's persistent media.

In **DataBackup**, audit records contain the following information. An audit record is composed of 8 basic items in Table 6-1.

Table 6-1 Audit Record Contents in **DataBackup**

Field	Description
Severity	Indicates the event level of a log.
Description	The details of the action that was performed. Including the identity of the user who performed the action.
Type	Event type, including Operation log, Run log, and Cleared alarm. Cleared alarm indicates the alarm event that is cleared.
Object	Indicates the function domain in which the event occurs.
Occurred At	The time that the action was performed.

Field	Description
Alarm ID	Indicates the ID of an alarm event. User can query the corresponding document to find the alarm details.
Status	Operation result of the event.
Node name	Storage where the event occurs.

In **Storage**, audit records contain the following information. An audit record is composed of 7 basic items in Table 6-2.

Table 6-2 Audit Record Contents in **Storage**

Field	Description
Severity	Indicates the event level of a log. Including Info, Warning, Major, and Critical.
Description	The details of the action that was performed. Including the identity of the user who performed the action.
Type	Event type, including Operation log, Run log, Recovered alarm, Current alarm and Security log.
Object	Indicates the function domain in which the event occurs.
Occurred	The time that the action was performed.
ID	Indicates the ID of an alarm event. User can query the corresponding document to find the alarm details.
Status	Operation result of the event.

users can log into ProtectManager in **DataBackup** and DeviceManager in **Storage** to select, filter, and review audit records, provided they have the appropriate permissions

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3.

6.2 ACCESS CONTROL

Access Control indicates that rules can be formulated by proper Users to globally control the access of a specific user to the TOE.

The TOE supports two Access Control mechanisms for Users:

- The IP Whitelist is configured globally to limit access from IP addresses out of the list. The elements of the list are single IP addresses or ranges. A user can not establish session to access the TOE if the IP address out of the list.
- Login Method is a list including CLI, SFTP, DeviceManager, RESTful. A user can access the TOE only using the method/protocol included in this list configured for the user by other proper Users.

The TOE also supports Access Control mechanisms for NFS or CIFS services at the same time. In data access, the TOE provides NAS service to back up data between TOE and clients.

- For client deployed on Windows OS, the CIFS client can access files on the TOE through CIFS protocol, after AD domain authentication (Kerberos) passing, if the Windows user has proper permissions to match DAC policies.
- For client deployed on Linux OS, the TOE provides NFS protocol for backup data. The TOE supports both NFSv3 and NFSv4 protocols. For the NFSv3 protocol, the trustlist can be used to ident the IP addresses of NFS clients. For the NFSv4 protocol, the Kerberos can be used to restrict user access to specific files or directories through access control lists (ACLs)

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FMT_SMR.1.

6.3 IDENTIFICATION AND AUTHENTICATION

The purpose of authentication and identification is to make sure a user can access the TOE only after the TOE has identified the user identity as the right account.

By default, OceanProtect has four built-in accounts.

Table 6-3 list of built-in accounts

Accounts	Roles	Description
sysadmin	System Administrator	Built-in account, which can be used to log in to the GUI and invoke REST APIs.
mmdp_admin	Data Protection Administrator	Built-in account, which cannot be used to log in to the GUI and can only be used to invoke REST APIs.
cluster_admin	System Administrator	Multiple X series OceanProtect can form a cluster. cluster_admin is a built-in machine-machine account, which cannot be used to log in to the GUI and can only be used to invoke REST APIs.
mm_audit	Auditor	Built-in account, which cannot be used to log in to the GUI and can only be used to invoke REST APIs.

In this table, the sysadmin and cluster_admin accounts share the same role, which means they have the same permissions, but the login mode of the two accounts is different.

The TOE provides local and remote authentication modes:

In local authentication mode, the user identities are stored locally in the TOE. The identification factors include the password and one time password (OTP) sent through email. The TOE supports 2 kinds of combinations: password and OTP, password only. The combination of a user's identification factors can be chosen by another user whose role has the proper permissions.

- When the password is used, the result of identification is based on the comparison between the hash of the input password and the one stored in the TOE.

- When the OTP is used, an email with the OTP will be sent to the recipient configured by other users with proper permissions. The OTP is generated by the TOE randomly. A user is allowed to log in to the TOE only when the input OTP is same as the one generated by the TOE.

NOTE

The built-in account cannot use the OTP because **mmdp_admin**, **cluster_admin**, **mm_auditis** are machine-machine account and does not need to be configured. **sysadmin** is the default system administrator account. If there are errors with the mail server or configuration issues, it can render the OceanProtect Databakup unusable.

In remote authentication mode, the user identities are stored in a remote LDAP server (which means a server in compliance with the standard LDAP protocol, such as the AD server and OpenLDAP server).

- The LDAP server's essential information (including the IP address, port, and protocol) is configured by a user who has the **System Administrator** role. In this type of identification, the TOE acts as an LDAP client. The input user name and password are forwarded to the LDAP server through the standard LDAP protocol and are verified by the LDAP server.

In data access, the TOE provides NAS service to back up data between TOE and clients.

- For client deployed on Windows OS, the TOE maintains NTFS-Style files and provides CIFS protocol for backup data. Local authentication and AD domain authentication (Kerberos) are supported for file access in the TOE. In local authentication, the accessible users and passwords are verified by the TOE. In AD domain authentication, the accessible users are authenticated by the AD server.
- For client deployed on Linux OS, the TOE provides NFS protocol for backup data. The TOE supports both NFSv3 and NFSv4 protocols. For the NFSv3 protocol, the trustlist can be used to ident the IP addresses of NFS clients. For the NFSv4 protocol, the Kerberos can be used to confirm the identity of the communicating between TOE and client.

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

6.4 AUTHORIZATION

Authorization is to grant proper permissions to identify sessions which are generated with subset of identified users' attributes, so that the identified Users have rights to execute specified commands in the TOE.

The TOE implements authorization according to the core RBAC model modified slightly. Role Based Access Control is used to govern access to the TSF data that determines how and when automated backups are run, and to the backup data that is used when data is restored.

The following Table 6-4 lists the built-in roles of the **DataBackup**.

Table 6-4 Built-in roles in **DataBackup**

Role	Description
System Administrator	This role has all system permissions.
Data Protection	This role has data protection permissions, such as backup and

Role	Description
Administrator	restoration.
Disaster Recovery Administrator	This role has permissions to query cluster and capacity information, perform SAML user operations (add, delete, modify, and query), and manage quotas and functions.
Remote Device Administrator	This role can be used for authentication between the source and target clusters during copy replication.
Auditor	This role has only read-only permission but can audit the system.

The **System Administrator** role has all the permissions in the system. In addition to the permissions of other built-in roles, it also has configuration and management permissions for the system, such as user management, permission management, and managing the configuration of third-party servers. The **System Administrator** can create different roles based on service requirements of different users to restrict users' operation permissions on the system, ensuring service system stability and service data security.

For the built-in **Disaster Recovery Administrator**, **Remote Device Administrator**, and **Auditor** roles, each role has only one corresponding function and permission. therefore, the permissions and roles are inherently bound together and do not need to be separated. For example, the **Remote Device Administrator** role is permitted only to allow remote replication in a cluster, and the **Auditor** role can audit the system with the read-only permission.

For the built-in **Data Protection Administrator**, it includes a wide range of permissions, such as resource management, protection management, and other functions, as detailed in Table 6-5. Therefore, role-based permission management can be implemented by assigning specific roles to different users. Permissions cover access to and operations on resources. shows the details of permission information.

Table 6-5 Permission information in **DataBackup**

Permission Category	Permissions
Resource Management	• **Client management**: refers to permissions for client operations, including client registration, client update, client software package management, resource scanning, remarks setting, log export, log level configuration, enabling and disabling of automatic host name synchronization, and host deletion. • **Production resource management**: refers to permissions for operations on production resources and production resource groups, such as registering, deleting, modifying, and scanning production resources or production resource groups on the resource page.
Protection Management	• **Backup**: includes the permissions for operations of adding, modifying, removing, activating, and disabling protection, as well as backup. For end-to-end (E2E) backup jobs, you need to select **Client management**, **Production resource management**, **Backup**, and **SLA management**. • **Replication**: includes the permissions for operations of adding, modifying, removing, activating, and disabling protection, as well as replication. For E2E replication jobs, you need to select **Client**

Permission Category	Permissions
	management, **Production resource management**, **Backup**, **Replication**, and **SLA management**. • **Archive**: includes the permissions for operations of adding, modifying, removing, activating, and disabling protection, as well as archive. For E2E archive jobs, you need to select **Client management**, **Production resource management**, **Backup**, **Archive**, and **SLA management**. • **SLA management**: refers to the operation permissions on the SLA page, including creating, deleting, cloning, and modifying SLAs. • **Rate limiting policy management**: refers to operation permissions on rate limiting policies, including creating, modifying, and deleting rate limiting policies.
Copy Management	• **Restoration to the original location**: includes the permissions for restoration to the original location. For jobs of E2E restoration to the original location, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Restoration to the original location**. • **Restoration to a new location**: includes the permissions for restoration to a new location. For jobs of E2E restoration to a new location, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Restoration to a new location**. • **Restoration to a local host**: includes the permissions for restoration to a local host. For jobs of E2E restoration to the local host, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Restoration to a local host**. • **Restoration drill**: includes the permissions for creating, activating, disabling, modifying, and deleting drill plans in restoration drills. For E2E restoration drill jobs, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Restoration drill**. • **Copy deletion**: includes the permission for deleting copies. For E2E copy deletion jobs, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Copy deletion**. • **Copy index**: includes the permission for creating and deleting copy indexes. For E2E copy index jobs, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Copy index**. • **Live mount**: includes the live mount permission. For E2E live mount jobs, you need to select **Client management**, **Production resource management**, **Backup**, **SLA management**, and **Live mount**. • **Live mount policy management**: includes the permissions for creating, cloning, modifying, and deleting mount update policies.
Data Security	• **Air Gap management**: includes the permissions for creating, modifying, and disabling Air Gap policies. • **Ransomware protection and WORM policy**: includes the permissions for creating, modifying, and deleting ransomware

Permission Category	Permissions
	protection and WORM policies. - **Data anonymization**: includes all operation permissions under **Data Security > Data Anonymization**, such as the permissions for creating and cloning anonymization policies.
Reports	**Report**: includes the permissions for creating, downloading, and deleting reports, sending emails, as well as creating, deleting, modifying, and immediately executing report subscriptions.

The following Table 6-6 lists the built-in roles of the **Storage**.

Table 6-6 Built-in roles in **Storage**

Role	Description
Super administrator	All permissions over the system
Administrator	All permissions except user management, role management, global WORM compliance clock management, litigation hold file management, S3 key management, storage system power-off and restart, and running of major management O&M commands in the developer view, engineer view, and diagnostic view
Security administrator	System security configuration permissions, including management of security policies, security rules, HyperCDP objects, disks, certificates, disk data destruction policies, key services, antivirus functions, and file service snapshots
SAN resource administrator	Basic management permissions on SAN resources, including management of disk domains, storage pools, disks, controller enclosures or disk enclosures, recycle bin policies, internal objects, LUNs, application type objects, initiators, targets, iSNS servers, mapping views, host groups, hosts, port groups, LUN groups, ports, controllers, interface modules, omtask, and storage connectivity
NAS resource administrator	Management permissions on NAS resources, including management of disk domains, storage pools, ports, DNS load balancing services, BGP configurations, BGP peers, NFS services, share services, file services, domain authentication information, dtree services, quota services, CIFS services, Kerberos realm configurations, file signatures, application type objects, audit logs, omtask, and storage connectivity
Data protection administrator	Data protection management permissions, including management of recycle bin policies, internal objects, LUNs, clone LUNs, application type objects, initiators, mapping views, host groups, hosts, ports, remote devices, block service snapshots, HyperCDP objects, snapshot consistency groups (CGs), HyperClone, clone CGs, LUN CGs, LUN groups, remote replication, CGs, DR Star, quorum servers, omtask, storage connectivity, protection groups, file systems, clone file systems, dtree services, file service snapshots, quota services, NDMP services, file system migration

Role	Description
	policies, vStore services, and container storage
Remote device administrator	Cross-device data protection management permissions, including management of recycle bin policies, internal objects, LUNs, initiators, mapping views, host groups, hosts, port groups, LUN groups, ports, HyperCDP objects, HyperClone, clone CGs, block service snapshots, snapshot CGs, CGs, remote devices, remote replication, quorum servers, SmartQoS, LUN migration, system information, mirroring policies, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, and NDMP services. This role is used for remote authentication in cross-device data protection scenarios.
Monitor	Routine O&M permissions, such as information collection, performance collection, and inspection, including alarm policy management, log information export (such as system logs, configuration information, and diagnosis files), system log management, configuration file management, running data (configuration information) management, Call Home (eService) service management, and management of the CLI views that can be switched over
NDMP backup administrator	NDMP backup service management permissions, including management of initiators, mapping views, host groups, hosts, port groups, LUN groups, ports, HyperCDP objects, HyperClone, clone CGs, block service snapshots, snapshot CGs, CGs, remote devices, remote replications, quorum servers, SmartQoS, LUN migration, system information, mirroring policies, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, and NDMP services
Remote assistance administrator	All permissions except user management, role management, security policy management, security rule management, storage system power-on, power-off, and restart, omtask authentication mode management, deletion of files and directories in file systems, privileged deletion of enterprise WORM file systems, Call Home (eService) service management and query, and running of major and minor O&M management commands in the developer view, engineer view, and diagnostic view

The key points of the implementation of the core RBAC model are described as below:

- Every action of Users is achieved by a command, and every command has one or more permissions associated to it. This relationship is built in the TOE. A user can execute a command only if the user's permission list contains this command's permission.
- A set of permissions composes a role. The TOE supports 5 built-in roles that cannot be modified or deleted as Table 6-4 and Table 6-6.
- A user is authorized to perform certain operations and is forbidden to perform certain operations. This is achieved by comparing the permissions held by the account's assigned role and the permissions of the commands which bearing the operations.

TOE Security Functional Requirements addressed: (FDP_ACC.1, FDP_ACF.1, FMT_SMR.1)

6.5 SECURITY MANAGEMENT

The OceanProtect **DataBackup**'s mainly security functions as follow, users with the **System Administrator** role can implement security management:

- **User Management**, including the user password, user lockout status, user's role and other credentials.
- **Security Policies**, including the password policy, weak password dictionary, session timeout duration, login policy, and IP whitelist.
- **Network Service Management**, including Light Directory Access Protocol (LDAP), Secure File Transfer Protocol (SFTP), Simple Mail Transfer Protocol (SMTP).
- **Audit**, including audit review, audit record selection and filtering
- **Backup Resource Management**, including data backup/restoration task, backup policy Management, and backup clients Management.

The **OceanProtect Storage** is managed by the **DataBackup.** The **System Administrator** role can redirection to the DeviceManager through ProtectManager. In the TOE, the **Storage** provides the following security functions for the backup data:

- If the client is deployed on the Windows OS, OceanProtect use CIFS protocol to back up data. the **Storage** is responsible for configuring CIFS protocol-related security settings, such as memtioned in 6.3 IDENTIFICATION AND AUTHENTICATION.
- If the client is deployed on the Linux OS, OceanProtect use NFS protocol to back up data. The **Storage** supports both NFSv3 and NFSv4 protocols-related security settings, such as memtioned in 6.3 IDENTIFICATION AND AUTHENTICATION.
- **User Management**, including the user password, user lockout status, user's role and other credentials.
- **User Policy Management**, including the user name length, password complexity, access failure policy, and user lockout policy.
- **Access Control List Management**, including the login method list and IP whitelist.
- **Network Service Management**, including Syslog, Light Directory Access Protocol (LDAP), Secure File Transfer Protocol (SFTP), Simple Mail Transfer Protocol (SMTP).
- **Audit**, including audit review, audit record selection and filtering

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7 TERMINOLOGY AND ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
CC	Common Criteria
RBAC	Role Based Access Control
OSP	Organizational Security Policy
NTP	Network Time Protocol
NAS	Network Attached Storage
NFS	Network File System
CIFS	Common Internet File System
PAM	Pluggable Authentication Modules