Hitachi Device Manager Software,
Hitachi Tiered Storage Manager Software

Security Target

2017/01/10

Version 1.0.28

Hitachi, Ltd.

This document is a translation of the evaluated and certified security target written in Japanese.

Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software
Security Target

Trademarks

- Active Directory is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Microsoft is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Windows is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.
- Internet Explorer is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Java and JDK are trademarks or registered trademarks of Oracle Corporation and its affiliates in the United States and other countries.
- Kerberos is the name of a network authentication protocol developed by MIT (the Massachusetts Institute of Technology).

Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software Security Target

- Table of Contents -

1. ST introduction

This section identifies the ST and the TOE, and provides an overview and description of the TOE.

1.1. ST reference

ST title: Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software Security Target

ST version: 1.0.28

Identification name: HDvM_HTSM-ST

Date: January 10, 2017

Author: Hitachi, Ltd.

1.2. TOE reference

TOE name: Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software

TOE version: 8.0.1-02

Keyword: Access Control Devices and Systems

Developer: Hitachi, Ltd.

1.3. TOE overview

1.3.1. TOE type and security functions

(1) TOE type

The target of evaluation (TOE) falls into the category "Access Control Devices and Systems".

The TOE consists of Hitachi Device Manager Software (abbreviated hereafter to *HDvM*) and Hitachi Tiered Storage Manager Software (abbreviated hereafter to *HTSM*), which are storage management software products in the Hitachi Command Suite series.

The Hitachi Command Suite series consists of products such as HDvM, HTSM, Hitachi Replication Manager Software (abbreviated hereinafter to *HRpM*), Hitachi Compute Systems Manager (abbreviated hereinafter to *HCSM*), Hitachi Tuning Manager Software (abbreviated hereinafter to *HTnM*). The Hitachi Command Suite series is provided together on one storage medium, and the user can choose and install only those products in the series that are necessary for the user's operations.

Note that HDvM and HTSM, which are the TOE, commonly manage security function, and this common security function is called a common component, hereinafter referred to as *HBase*.

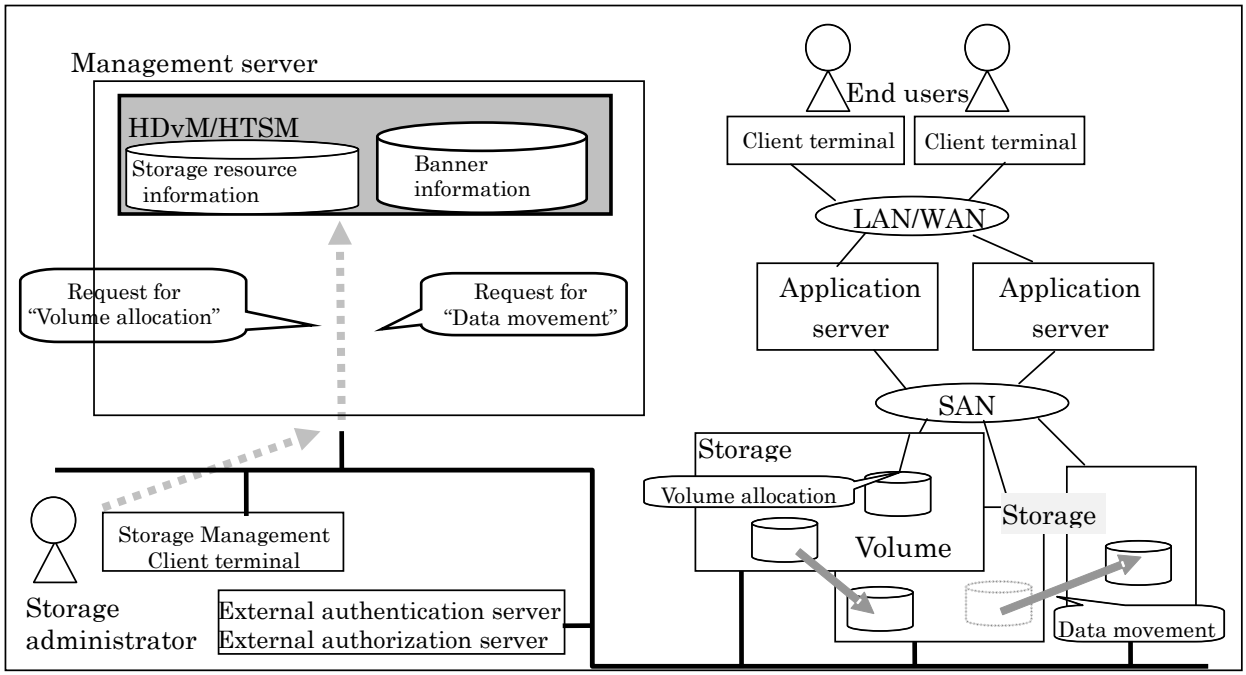


Fig. 1-1 Overview

A storage system houses multiple volumes within its chassis. Storage systems are connected to the application servers that execute the applications used for business operations, and the information that is necessary to execute these applications is stored in the storage systems' volumes. The TOE's (HDvM/HTSM) role is to manage the storage systems by performing actions such as volume allocation (enabling access to the appropriate storage system volumes from the application servers).

A storage administrator uses the TOE to perform integrated storage system management. This allows the storage administrator to perform operations on a large number of volumes and storage systems from the TOE, as shown above.
In **Fig. 1-1**, the storage administrator requests the required operation, such as volume allocation, from a storage management client terminal. The TOE provides functionality to control access to resource information by using HBase common functions for the storage management software.

(2) Security functions

The TOE security functions are as follows:

- Identification and authentication function

  The identification and authentication function uses user IDs and corresponding passwords to authenticate users, and generates and maintains sessions based on the results.

- Security information fundamental management function
  The security information fundamental management function manages the deletion of account information, the modification or deletion of permissions information, and the creation, viewing, modification, or deletion of banner information. It also sets security parameters.
- Storage resource access control function
  The storage resource access control function assigns storage resource information to resource groups, and manages modifications to storage resource information using the security information fundamental management function.
- Warning banner function
  The warning banner function enables the input and display of warning message data to be viewed by users who perform TOE operations.

1.3.2. TOE configuration

The physical TOE consists of the libraries and programs below.

Fig. 1-2 shows the software configuration that includes the TOE. The modules implementing the TOE security functions are shaded.

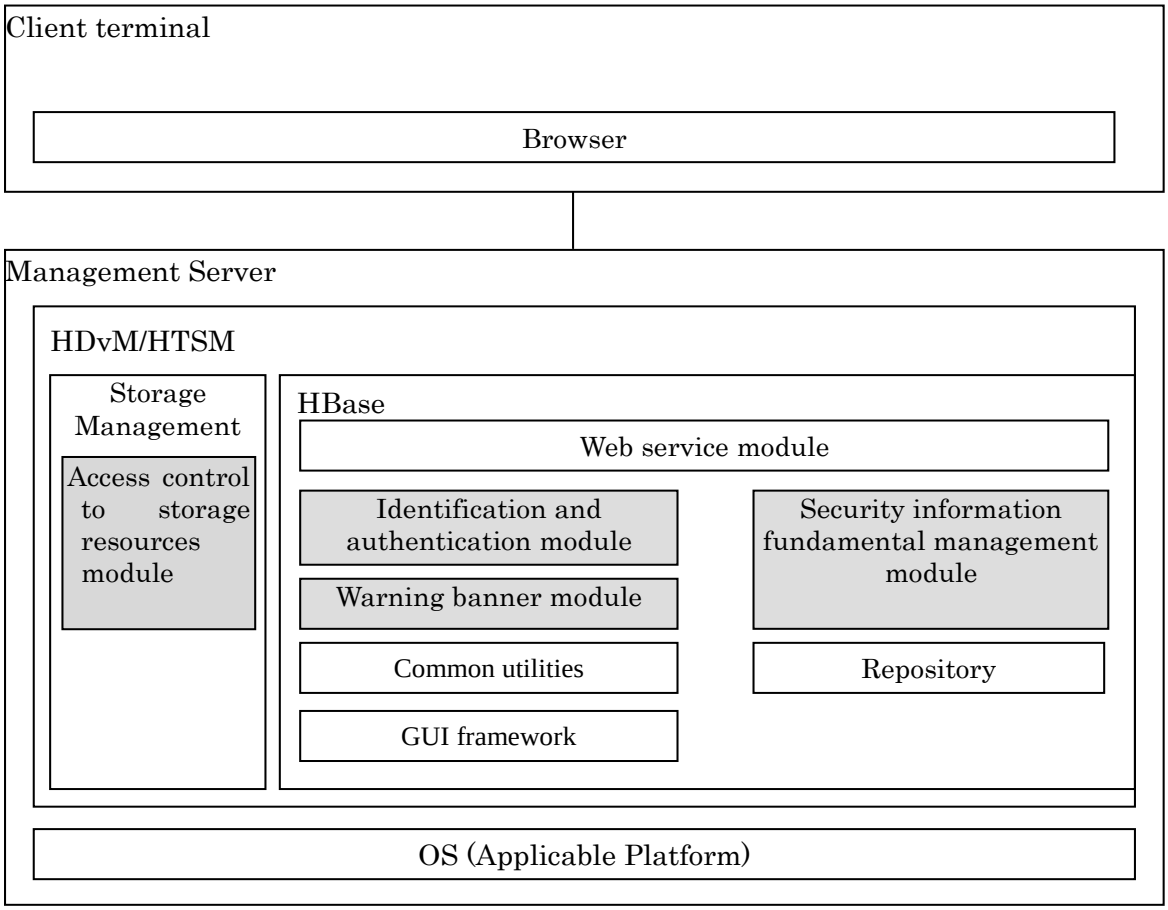


Fig. 1-2 Software configuration including the TOE

- The identification and authentication module implements the identification and authentication functionality of the TOE.
- The security information fundamental management module implements the security information fundamental management functionality of the TOE.
- The warning banner module is a module that implements the warning banner functionality of the TOE.
- The common utilities implements the common functions of the TOE.
- The web service module implements the TOE web service.
- The GUI framework implements the TOE's graphical user interface (GUI).
- The repository is the database that stores data for the TOE.
- The storage management functionality enables the management of storage systems, such as management of the environment settings for the storage system or volume creation.

The access control to storage resources module controls access to resources by associating information about storage resource information with the HBase security functionality (the

security information fundamental management module).

1.3.3. TOE operating environment

1.3.3.1. Environment in which the TOE is used

Fig. 1-3 shows an example of a system configuration that uses the TOE.

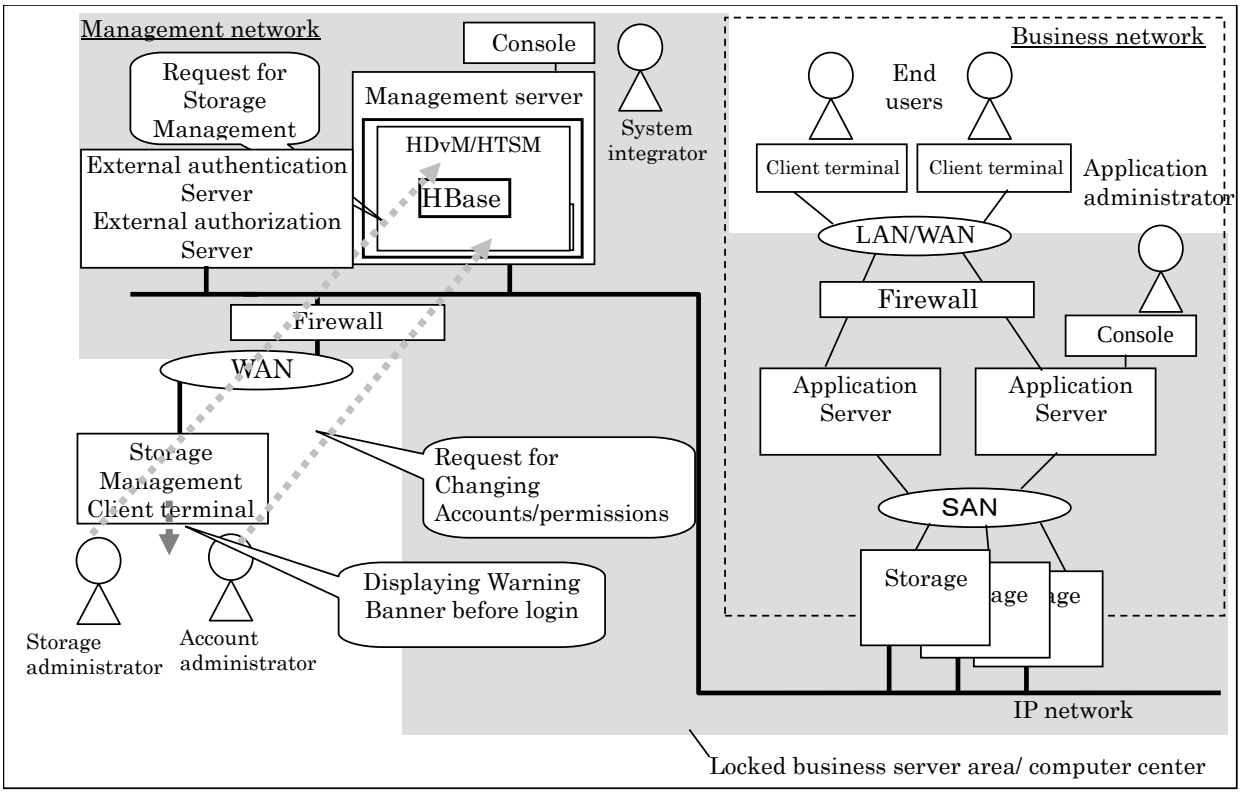


Fig. 1-3 TOE model

In **Fig. 1-3**, solid lines indicate physical cabling and devices, and dotted lines indicate actions and boundaries. Shading indicates a locked business server area, such as a computer center.

Management servers, application servers, storage systems, and peripheral devices are installed in the business server area. Physical entry to and exit from this area are controlled by using locks or similar means.

The management network and the business network within the firewall are called internal networks. All networks outside the firewall are called external networks.

Management servers, storage systems, and peripheral devices are connected to the management network. Application servers, storage systems, and peripheral devices are connected to the business network. The internal networks are protected from external networks by a firewall.

A storage system that belongs to both an external and an internal network has two independent

NICs: one connects to the management network and the other connects to the business network. As a result, the management and business networks are separated so that one cannot interfere with the other.

To access the TOE via an external network, storage administrators and account administrators must use a storage management client terminal to issue operation requests to the TOE. At this time, the TOE continuously displays a warning banner in the login window cautioning TOE operators (including users) about illegal use. In addition, storage administrators and account administrators must use difficult-to-guess passwords to access the TOE.

Fig. 1-3 shows a configuration that includes an external authentication server and an external authorization server. The external authentication server can be used in place of the TOE identification and authentication functionality. The TOE can grant permissions to a group registered on the external authorization server as long as the group name has already been registered beforehand in the TOE. Users in the group who have been successfully identified and authenticated by the external authentication server can use the TOE within the scope of the permissions granted by the TOE.

The external authentication and authorization server and management server are set up in the same management network. However, if confidentiality and integrity can be maintained between the servers, the servers can be located in different business server areas. Note that if confidentiality and integrity cannot be maintained between the servers, the servers must be located in the same business server area.

1.3.4. TOE evaluation configuration

Hardware/Software specification required for TOE is described below, although it is not part of TOE.

1.3.4.1. Hardware requirements (Management Server hardware requirements for installing the TOE)

Model name: HP Compaq dc7900SF/CT

CPU: Intel Core2 Quad

RAM: 8 GB

Vitual Memory: 11701MB

HDD: 1,000 GB

1.3.4.2. Software requirements

(1) Storage management client

Internet Explorer 9 (32bit) on Windows 7 SP1 with Flash Player 14.0

(2) External authentication server and external authorization server

Microsoft Active Directory(Windows Server 2012 R2 (x64))

(3) Management server

Windows Server 2012 R2 (x64)

(4) Installed programs for the management server

Java™ SE Development Kit 8, Update 92

1.4. TOE description

1.4.1. Logical TOE boundary

Table 1-1 lists the TOE functions. The TOE security functions are shaded.

Table 1-1 TOE functions

Function		Overview
Identification and authentication function		This function enables users to be identified and authenticated by using user IDs and corresponding passwords, and generates and maintains sessions according to the authentication results.
Security information management function	Security information fundamental management function	This function enables the management of security information, such as the deletion of account information, the modification and deletion of permissions information, and the creation, viewing, modification, and deletion of banner information. This function also sets security parameters.
	Storage resource access control function	This function enables the control of access to storage resources in cooperation with the security information fundamental management function.
Warning banner function		This function enables the input and display of warning message data to be viewed by those who perform TOE operations.
Storage management function		This function enables the management of storage systems, such as the specification of environment settings and the creation of volumes.

(1) Identification and authentication function

This function identifies and authenticates a TOE user when the user logs on to the TOE, and this function determines a user's security role by referencing the TOE's ACL table. (Section 1.4.4 explains security roles.)

In the course of identification and authentication, if repeated attempts to authenticate the same user fail a certain number of times, the TOE automatically locks the user's account to prevent repeated login attempts by unauthorized users. In this case, internal identification function is used.

The TOE can also use the external authentication function of an external authentication server instead of the TOE's internal authentication function. When an account is registered, the account administrator specifies whether internal authentication or external authentication is to be used for a specific account. Internal authentication and external authentication are independent functions, and each account is to be authenticated by either internal authentication or external authentication, not both. After operation begins, the account administrator is able to change this setting for an account.

To use the external authentication function, the user IDs registered on the external authentication server must also be registered in the TOE. An account registered only on the external authentication server will result in an identification failure in the TOE. Each account is authenticated by the internal or external authentication function specified by the account administrator, and obtains the security role.

The external authentication group linkage function assigns permissions managed in the TOE to groups and accounts managed by an external authentication server. TOE decides account permissions after obtaining information of accounts and account groups. In addition, identification and authentication operations should be performed by the external authentication function when the external authentication group linkage function is used.

The external authentication group linkage function does not require that accounts registered on the external authentication server be registered in the TOE. If a user ID or password has not been registered in the TOE, the TOE uses the external authentication server to identify and authenticate the user. The external authentication server uses the user ID and password registered on the external authentication server to identify and authenticate the user, and then returns the result to the TOE. If the user is successfully identified and authenticated, the TOE queries the external authorization server for information about the group and the accounts belonging to the group in accordance with the result.

When the external authentication group linkage function is used and the same user ID is registered in the TOE and on the external authentication server, the account information in the TOE is used to identify and authenticate the user. (Therefore, even if a system integrator account (System) exists on the external authentication server, the account in the TOE is used as the System account. This means that even if a System account is created on the external authentication server, that account cannot obtain the system integrator's permissions.)

When the external authentication function or the external authentication group linkage function is used, the TOE does not automatically lock the accounts registered in the TOE or on the external authentication server. If an external authentication server is to be used, an external authentication server that has a function similar to the TOE automatic account locking function must be used in order to prevent threats such as illegal logins achieved through repeated authentication attempts.

(2)-1 Security information fundamental management function

For users registered in the TOE, the TOE manages user IDs, passwords, and lock statuses as account information. Also, the TOE manages each user’s permission information as a security role. The TOE stores the variable parameters for automatic account locking and for the password complexity check as security parameters. When a password is set, the TOE checks whether the

password satisfies the conditions set in the security parameters.

When the external authentication function or the external authentication group linkage function is used, the above TOE functions cannot be used, in which case an external authentication server that has the TOE functions described above must be used in order to protect against threats such as illegal logins achieved through repeated authentication attempts.

The TOE manages the warning messages about the illegal use of TOE as banner information, and provides methods for creating, deleting, and modifying banner information according to the requests of TOE users.

(2)-2 Storage resource access control function

This function associate storage resource information to account information of the security information fundamental management function, and creates the ACL table. And this function controls access to storage resource information for each security role of TOE users derived from the ACL table..

(3) Warning Banner function

Banner information is entered by the system integrator or an account administrator from a TOE window that allows warning banner messages to be edited. The system integrator is also able to log in to the machine on which the TOE is installed and use a warning banner edit command to set banner information. The banner information must be set before TOE operation begins.

Regardless of the method used to set banner information, the TOE displays the banner information in the login window.

The following explains how to use the TOE.

(1) Preparation by the system integrator

- The system integrator purchases all necessary information system resources, including the TOE.
- The system integrator installs and connects the devices on which the TOE is to be installed, builds the prerequisite environment for the TOE, installs the TOE, sets up the TOE, and confirms that the TOE operates correctly.
- The system integrator creates an account for the account administrator with the appropriate account management permissions based on the default account and default password, and notifies the account administrator of this information.

(2) Account management by the account administrator

- The account administrator acquires an appropriate account and password.
- The account administrator uses this account and password to access the TOE, and is

authenticated by the TOE.

- The account administrator uses the TOE to create the accounts for other account administrators and storage administrators, based on the source information for the accounts to be set up. The account administrator also sets attributes such as permissions for the created accounts.
- The account administrator notifies other account administrators and storage administrators of the created account information.

(3) Storage management by the storage administrator

- The storage administrator acquires an appropriate account and password.
- The storage administrator uses this account and password to access the TOE, and is authenticated by the TOE. After authentication, the storage administrator acquires the permissions corresponding to the account.
- After being authenticated by the TOE, the storage administrator manages storage systems and resources to the extent allowed by the storage administrator's assigned permissions.

1.4.2. Physical TOE scope

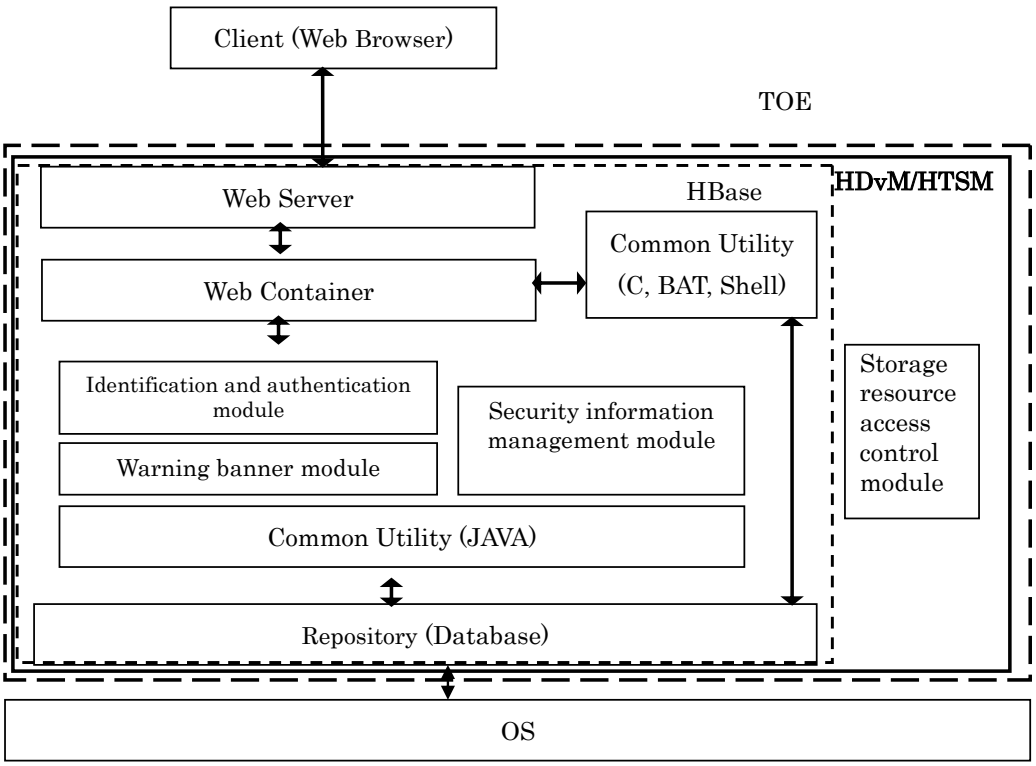


Fig. 1-4 Physical TOE scope (bold dotted line)

In **Fig. 1-4**, the area enclosed in the bold dotted line indicates the physical TOE. All functions are shared throughout the TOE.

1.4.3. Guidance documentation

Guidance documents for the TOE are as follows:

- Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software Security Guide
- Hitachi Command Suite Installation and Configuration Guide (3021-9-006-10)
- Hitachi Command Suite User Guide (3021-9-003-10)
- Hitachi Command Suite Administrator Guide (3021-9-008-10)
- Hitachi Command Suite Messages Guide (3021-9-011-10)

1.4.4. Roles related to the TOE

This ST assumes that the users described below exist for the TOE. Each user performs operations according to the permissions assigned to the individual user. When a process is authenticated and authorized in the TOE, the process is assigned a security role. The process can perform operations within the scope of this role. Security roles can be classified into the following categories: system integrator, account administrator, and storage administrator (including upper-level storage administrators). A user's security role is derived from the ACL table, in which combinations of user IDs and operating permissions for each resource are defined.

A system integrator, who is authorized as the TOE system account, has all TOE permissions. The system integrator can modify, update, or delete the ACL table from which the account administrator's and storage administrator's security roles are defined.

An account administrator has user management permissions in the TOE and can update (modify, delete, etc.) the ACL table from which the account administrator's and storage administrator's security roles are defined.

A storage administrator has a combination of permissions for each resource that is specified by a system integrator or an account administrator, and can perform all tasks associated with those permissions. (For details about the access control management model for the storage administrator and the storage administrator security role, refer to sections 1.4.4.1 and 1.4.4.2.)

An upper-level storage administrator can register, edit, update, and delete storage systems, can delete resource groups, and can assign and unassign storage resources.

An external authentication server administrator can configure settings related to an external authentication server or an external authorization server, if such servers are used.

(1) System integrator (server and network administrator)

Role: Maintains and manages the system by performing operations such as backing up server data.

Permissions:

- Allowed to determine and set parameters required for building and running the system. Accordingly, the system integrator can update (change and delete) security roles.
- The system integrator's security role cannot be changed.
- TOE security roles other than the system administrator security role cannot be added to the system integrator's account.
- The system integrator's account is built-in account as the system account in the TOE, and has all permissions for the TOE.

Level of trust: Has responsibility for the entire system and is trusted.

(2) Account administrator

Role: Manages the accounts of system users and specifies settings for the system.

Permissions:

- The source information for an account, including whether an account is to be created for an individual and the permissions to be granted to that individual's account, is derived from organizational information such as the organizational hierarchy. An account administrator is granted permissions based on this source information and can perform the operations corresponding to these permissions.
- Accordingly, an account administrator can update (change and delete) the account administrator and storage administrator security roles.
- An account administrator can assign the upper-level storage administrator security role to the account administrator's own account and therefore obtain upper-level storage administrator permissions. If this Security Role is assigned to the account administrator's account, the account administrator then has all permissions related to managing the ACL table and can assign resource groups and roles for a user group, update (change, delete and modify) storage systems, delete resource groups, and assign or unassign storage resource information.
- The account administrator has User Management permissions in the TOE.

Level of trust: Has responsibility for the account administrator's own work and is trusted within the scope of that work.

(3) Storage administrator

Role: Manages storage systems by performing operations such as managing storage resources.

Permissions:

- An upper-level storage administrator can register, delete, update, or edit storage systems, delete resource groups, and control the assignment and unassignment of storage resource information.
- A storage administrator can specify resource settings, such as the settings for allocating volumes, for storage systems installed by the system integrator. Accordingly, the storage administrator can view permissions information in order to understand the security role granted to the storage administrator's own account.
- A storage administrator has a combination of operating permissions for resources derived from the ACL table specified by a system integrator or by an account administrator in the TOE.
- The ACL table, from which the storage administrator's security role is derived, defines the following information: the relationship between roles and user groups and resource groups (which group users and resources, respectively), and the details regarding the combination of operating permissions and the resources for which such operations can be performed.
- In the TOE, the storage administrator has permissions related to storage system operations, including the Admin, Modify, View, and CUSTOM permissions.

Level of trust: Has responsibility for the storage administrator's own work and is trusted within the scope of that work.

(4) External authentication server administrator

Role: Manages the external authentication server and the external authorization server

Permissions:

- The external authentication server administrator sets up the external authentication server and the external authorization server in the business area.
- If the TOE is to use the external authentication server and the external authorization server, the external authentication server administrator sets up the authorization and authentication information from the TOE on the external servers.

Level of trust: Has responsibility for the external authentication server administrator's own work and is trusted within the scope of that work.

1.4.4.1. Access control Management Model for Storage administrator

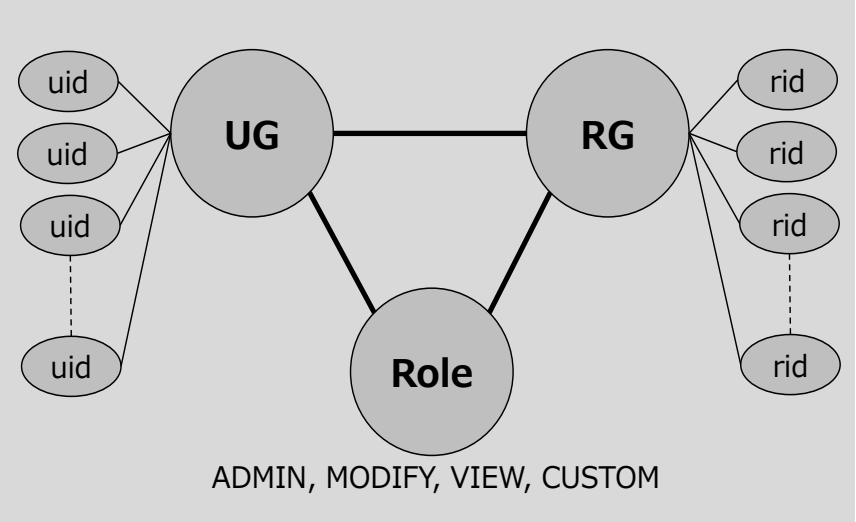
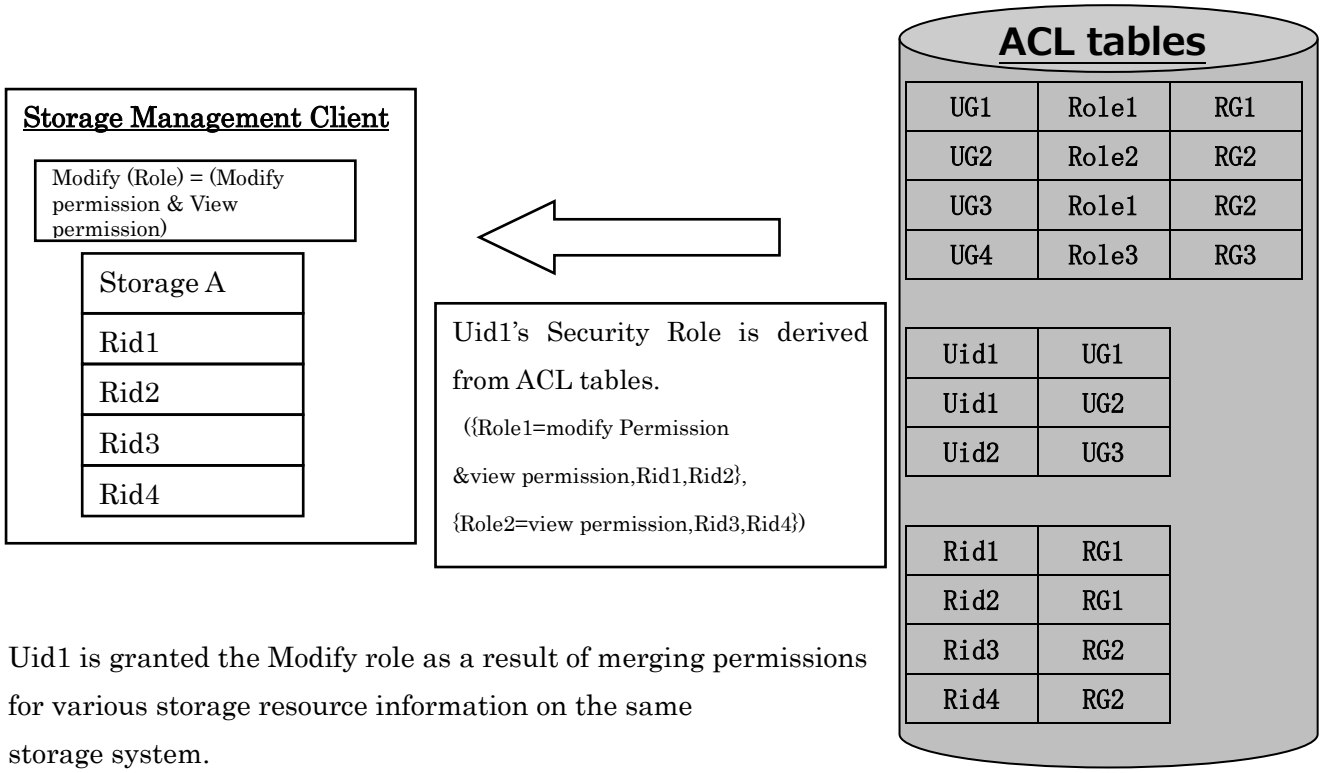


Fig. 1-5 Access control Management Model for Storage administrator

uid: An identifier assigned to each storage administrator.
rid: An identifier assigned to each storage resource.
Role: A combination of operating permissions
Admin (Role): A combination of the Admin, Modify, and View permissions
Modify (Role): A combination of the Modify and View permissions
View (Role): View permissions
Custom (Role): A combination of operating permissions more detailed than the Admin, Modify, and View roles
UG: Abbreviation for user group. User groups represent the relationship between a group of uids and a combination of roles and resource groups.
RG: Abbreviation for resource group. Resource groups represent the relationship between storage resources and a combination of roles and user groups.

1.4.4.2. Security Role for Storage administrator

The storage administrator's security role is derived from the ACL tables configured in the access control management model. Storage resource information is controlled by each storage syste, and the storage administrator's security role is a role in which various permissions for each storage resource are merged. The following example shows that if Uid1 (a storage administrator account belonging to the user groups UG1 and UG2) opens a window related to Storage A (a storage system), Uid1 has the role Modify (Role) for rid1, rid2, rid3, and rid4 (storage resource information).



Uid1 is granted the Modify role as a result of merging permissions for various storage resource information on the same storage system.

2. Conformance claims

2.1. CC conformance claim

This ST conforms to the CC versions below.

2.1.1. CC versions to which the ST claims conformance

Part 1: Introduction and general model Version 3.1 Revision 4 (CCMB-2012-09-001)

Part 2: Security functional components Version 3.1 Revision 4 (CCMB-2012-09-002)

Part 3: Security assurance components Version 3.1 Revision 4 (CCMB-2012-09-003)

2.1.2. Conformance to CC Part 2

CC Part 2 conformant

2.1.3. Conformance to CC Part 3

CC Part 3 conformant

2.2. Protection Profile (PP) claims and package claims

2.2.1. PP claim

No Protection Profile claims apply to this ST.

2.2.2. Package claim

EAL2 and ALC_FLR.1 are added as evaluation assurance levels of the ST.

3. Security problem definition

This section describes threats, assumptions, and organizational security policies.

3.1. Threats

3.1.1. Assets to be protected

The TOE manages access to storage resource information and banner information based on security roles. The following assets are protected by the TOE:

- Banner information
- Storage resource information

3.1.2. Threats

T.ILLEGAL_ACCESS (illegal connection)

If an illegal user (a user who does not have an account in the TOE) accesses the TOE from a management client, this user might delete, modify, or reveal storage resource information or delete or modify banner information. In addition, a user who has an account in the TOE might be misrecognized as having permissions that the user does not really have, and might delete or modify the TOE's storage resource information or banner information.

T.UNAUTHORISED_ACCESS (unauthorized access)

An authenticated storage administrator or account administrator might delete or modify the TOE's storage resource information or banner information by performing an unauthorized operation from a management client.

3.2. Assumptions

A.PHYSICAL (hardware management)

The management server on which the TOE runs, peripheral devices, the external authentication server and external authorization server that the TOE uses, the internal network, and the firewall at the boundary of the internal network is assumed to be installed in a physically isolated business server area. Only the administrators of the hardware and software in that area are permitted to enter this area. The administrators is assumed to be trusted persons who will not perform malicious acts in that area.

A.NETWORKS (networks)

The internal network, located in the business server area that houses the management network

connected to the management server, is assumed to be restricted only to communication from storage management client terminals by means of a firewall.

A.ADMINISTRATORS (administrators)

The system integrator is assumed to be a trusted person. Account administrators, storage administrators, and external authentication server administrators are assumed not to, in the course of the work associated with their own permissions, perform malicious acts related to the management of accounts and permissions of TOE users, and the management of storage systems. Other server administrators are assumed not to perform malicious acts with regard to their own work.

A.SECURE_CHANNEL (communications security)

The network between the management server on which the TOE runs, and management clients, and the network between the TOE and the external authentication server and external authorization server that the TOE uses are assumed to be secure with regard to the confidentiality and integrity of communications.

A.PASSWORD (setting and updating passwords)

The system integrator,the account administrators and the administrator of the external authentication server are assumed to determine an appropriate level of password complexity, as well as the number of login attempts to be permitted before an account is to be locked, and to configure accordingly. Each administrator is assumed toupdate their passwords regularly and avoid actions that might lead to passwords being stolen or revealed via physical actions (for example, writing a password on a sticky note and sticking it on a PC monitor, or allowing the shoulder hacking) or human causes (for example, failing to update passwords, updating a password by using the same password again, using a password consisting of personal information, using a password that is used in other applications, or leaving password information in the cache).

A.CLIENTS (management of storage management clients)

It is assumed that malicious software dose not exist on the storage management client.

A.SRV_MGMT (server management)

The settings for services that run on the server, server settings, and accounts registered on the server is assumed to be managed to prevent management clients from bypassing the TOE and directly accessing the internal network.

3.3. Organisational security policies

P.BANNER (warning banners)

The storage management software must have functionality that displays advisory warning messages related to illegal use before identification and authentication.

4. Security objectives

This section describes the security objectives for the TOE and for the operating environment, and the rationale for these security objectives.

4.1. Security objectives for the TOE

O.I&A

The TOE must identify and authenticate users of storage management client terminals for whom internal authentication is specified, so that only authorized users are able to access the permissions information and storage resource information managed by the TOE.
If an authentication attempt for a user for whom internal authentication has been specified fails the number of times defined by the TOE, the TOE must automatically lock that user's account.

O.MGMT

The TOE must provide methods for viewing and specifying the authentication method, the permissions information and storage resource information and the banner information for each user, and must control access to these methods so that only users of storage management client terminals who have the appropriate permissions can use them.

O.BANNER

The TOE must display advisory warning messages about illegal use before identification and authentication.

O.PASSWORD

The TOE must limit the types of passwords that can be registered by users for whom internal authentication is specified, in accordance with the specified security parameter values.

4.2. Security objectives for the operational environment

4.2.1. Security objectives achieved during operations

OM.SECURE_CHANNEL

By using protected channels for which measures such as encryption are in place, the following networks must maintain the confidentiality and integrity of communications: the network between the management server on which the TOE runs and the management clients, and the network between the TOE and any external authentication and authorization server used by the TOE.

OM.I&A

An external authentication server administrator must ensure that the external authentication server has identification and authentication functionality, and functionality to limit the number of login attempts for users for whom external authentication is specified.

OM.PASSWORD_EX

An external authentication server administrator must ensure that the external authentication server has functionality to ensure password complexity for users for whom external authentication is specified.

OM.PASSWORD

A system integrator and account administrators and an external authentication server administrator must determine an appropriate level of password complexity, as well as the number of login attempts to be permitted before an account is to be locked, and must specify password settings accordingly. Administrators must update their passwords regularly and avoid actions that might lead to passwords being stolen or revealed via physical actions (for example, writing a password on a sticky note and sticking it on a PC monitor, or allowing the shoulder hacking) or human causes (for example, failing to update passwords, updating a password by using the same password again, using a password consisting of personal information, using a password that is used in other applications, or leaving password information in the cache).

OM.PHYSICAL

The following must be installed in a physically isolated business server area: the management server on which the TOE runs, peripheral devices, the external authentication and authorization server that the TOE uses, the internal network, and the firewall at the boundary of the internal network. Only the administrators of the hardware and software in that area are permitted to enter this area. Personnel control must be used so that only trusted persons who will not perform

malicious acts in regard to either the hardware or software in the area are designated as administrators.

OM.FIREWALL

A firewall must be installed between the internal network in the business server area, which houses the management network connected to the management server, and the external network. The firewall must be configured so that only storage management client terminals are allowed to communicate with the internal network. This prevents unnecessary communications from the external network from entering the internal network in the business server area.

OM.ADMINISTRATORS

The head of the organization must select appropriate personnel in order to guarantee that the system integrator can be trusted and that account administrators, storage administrators, external authentication server administrators, and administrators of other servers shall not perform malicious acts with regard to their own work. Work includes the management of the accounts and permissions of storage management software users, the management of storage systems, and the management of other servers.

OM.TOE_ACCOUNT

The system integrator, account administrators, and external authentication server administrators must not reveal the passwords that they set for creating users. And the system integrator, account administrators, external authentication server administrators, and storage administrators must set difficult-to-guess passwords on the basis of the combination of password length and character types.

OM.CLIENTS

The system integrator, account administrators, and storage administrators must monitor the storage management client terminals to ensure that malicious software is not installed on any of the client terminals that are used to access the TOE.

OM.SRV_MGMT

The settings of services that run on the server, server settings, and accounts registered on the server must be managed to prevent storage management clients from bypassing the TOE and directly accessing the internal network by system integrator.

4.3. Security objectives rationale

The security objectives counter the threats specified in the definitions of security problems, and satisfy the assumptions and organizational security policies. **Table 4-1** describes the correspondence between the security objectives and the following: the threats to be countered, the assumptions to be satisfied, and the organizational security policies to be satisfied.

Table 4-1 Correspondence among security objectives, assumptions, threats, and organizational security policies

Security problem definition / Security objectives	A.PHYSICAL	A.NETWORKS	A.ADMINISTRATORS	A.SECURE_CHANNEL	A.PASSWORD	A.CLIENTS	A.SRV_MGMT	T.ILLEGAL_ACCESS	T.UNAUTHORISED_ACCESS	P.BANNER
O.I&A								X		
O.MGMT								X	X	
O.BANNER										X
O.PASSWORD								X		
OM.I&A								X		
OM.PASSWORD_EX								X		
OM.PHYSICAL	X									
OM.FIREWALL		X								
OM.ADMINISTRATORS			X							
OM.SECURE_CHANNEL				X						
OM.PASSWORD					X					
OM.CLIENTS						X				
OM.SRV_MGMT							X			
OM.TOE_ACCOUNT								X		

As shown in **Table 4-1**, each security objective corresponds to at least one assumption, threat, or organizational security policy.

The following describes how these security objectives counter threats, uphold assumptions, and enforce organizational security policies.

(1) Threats

T.ILLEGAL_ACCESS (illegal connection)

O.I&A, **O.MGMT**, and **OM.I&A** ensure that users of storage management client terminals who attempt to access the TOE are identified, authenticated, and verified as authorized users. At this point, the TOE identifies and authenticates those users for whom internal authentication is specified, and the external authentication server identifies and authenticates those users for whom external authentication is specified. **O.PASSWORD** and **OM.PASSWORD_EX** ensure that the TOE and the external authentication server limit the types of passwords that can be registered so that difficult-to-guess passwords must be set. **OM.TOE_ACCOUNT** ensures that users set passwords that are difficult to guess because of password length and character types used. This process ensures safe password management. In addition, **O.I&A** and **OM.I&A** ensure that the TOE automatically locks the account of a user for whom an authentication attempt fails the defined number of times, to defend against brute-force password attacks.

T.ILLEGAL_ACCESS is therefore countered by **O.I&A**, **O.MGMT**, **O.PASSWORD**, **OM.I&A**, **OM.PASSWORD_EX**, and **OM.TOE_ACCOUNT**.

T.UNAUTHORISED_ACCESS (unauthorized access)

O.MGMT ensures that the TOE controls access to permissions information and banner information by storage management client terminal users, in accordance with the permissions information provided for the TOE users.

T.UNAUTHORISED_ACCESS is therefore countered by **O.MGMT**.

(2) Assumptions

A.PHYSICAL (hardware management)

OM.PHYSICAL ensures that the following are installed in a physically isolated business server area: the management server on which the TOE runs, peripheral devices, the external authentication server and the external authorization server, the internal network, and the firewall at the boundary of the internal network. Entry and exit are controlled so that only the administrators of the servers installed in the business server area can enter. These administrators are trusted persons who will not perform malicious acts in regard to the servers in the business server area.

A.PHYSICAL can therefore be handled by **OM.PHYSICAL**.

A.NETWORKS (networks)

OM.FIREWALL ensures that a firewall is installed between the internal network in the business server area, which houses the management network connected to the management server, and the external network, so that the internal network and the external network are logically separated. As a result, communication from sources other than storage management client terminals does not enter the internal network.

A.NETWORKS can therefore be handled by **OM.FIREWALL**.

A.ADMINISTRATORS (administrators)

OM.ADMINISTRATORS ensures that those with the highest level of responsibility in an organization select appropriate personnel to serve as the system integrator, account administrators, storage administrators, external authentication server administrators, and administrators of other servers. Therefore, the system integrator can be trusted. In addition, account administrators, storage administrators, external authentication server administrators and the administrators of other servers can be trusted not to perform malicious acts regarding the work for which they are responsible. Work includes the management of the accounts and permissions of users, the management of storage systems, and the management of other servers.

A.ADMINISTRATORS can therefore be handled by **OM.ADMINISTRATORS**.

A.SECURE_CHANNEL (communications security)

OM.SECURE_CHANNEL ensures that the network between the management server and management clients, as well as the network between the management server and the external authentication server/external authorization server in case of different business server area, uses communication paths protected by encryption or other methods, to ensure the confidentiality and integrity of communications.

A.SECURE_CHANNEL can therefore be handled by **OM.SECURE_CHANNEL**.

A.PASSWORD (setting and updating passwords)

OM.PASSWORD ensures that the system integrator,the account administrators and the administrator of the external authentication server must determine an appropriate level of password complexity, as well as the number of login attempts to be permitted before an account is to be locked, and must specify password settings accordingly. Each administrator must update their passwords regularly and avoid actions that might lead to passwords being stolen or revealed via physical actions (for example, writing a password on a sticky note and sticking it on a PC monitor, or allowing the shoulder hacking) or human causes (for example, failing to update passwords, updating a password by using the same password again, using a password consisting of personal information,

using a password that is used in other applications, or leaving password information in the cache).

A.PASSWORD can therefore be handled by **OM.PASSWORD**.

A.CLIENTS (management of storage clients)

OM.CLIENTS ensures that the system integrator and account administrators monitor client terminals in order to prevent malicious software from being installed on the client terminals that are used to access the storage management software.

A.CLIENTS can therefore be handled by **OM.CLIENTS**.

A.SRV_MGMT (management of accounts registered on the server)

OM. SRV_MGMT ensures that the settings for services that run on the server, server settings, and the accounts registered on the server are managed to prevent management clients from bypassing the TOE and directly accessing the internal network.

A.SRV_MGMT can therefore be handled by **OM. SRV_MGMT**.

(3) Organisational security policies

P.BANNER (warning banners)

O.BANNER ensures that the storage management software displays the advisory warning messages regarding illegal use of it before identification and authentication.

P.BANNER can therefore be handled by **O.BANNER**.

5. Extended components definition

This ST does not define any extended components.

6. Security requirements

6.1. Security functional requirements

This section describes the TOE security functional requirements. All the functional requirement components that will be used are specified in CC Part 2.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].**

[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

subjects: Process acting on behalf of the user of the storage management client terminal

objects: banner information file

operations: Viewing, modification, creation, or deletion

subjects: Process acting on behalf of the user of the storage management client terminal

objects: storage resource information

operations: modification

[assignment: *access control SFP*]

ACL access control SFP

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 **The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].**

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation**

among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] and [assignment: access control SFP]

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]	[assignment: access control SFP]
Subject: Process acting on behalf of a user of the storage management client terminal Object: Banner information file Subject attributes: Security role associated with the subject Object attribute: None	ACL access control SFP
Subject: Process acting on behalf of the user of the storage management client terminal Object: Storage resource information Subject attributes: Security role associated with the subject Object attribute: None	ACL access control SFP

[assignment: rules governing access among controlled subjects and controlled objects usingcontrolled operations on controlled objects]

Subject	Object	Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects
Process acting on behalf of a user of the storage management client terminal	Banner information file	If the security role associated with the subject is account administrator or system integrator, the process can create, delete or modify the banner information file.

Process acting on behalf of a user of the storage management client terminal	Storage resource information	If the security role associated with the subject has modify permission of storage resource information, the process can modify storage resource information.

[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

Subject	**Object**	**Rules, based on security attributes, that explicitly authorise access of subjects to objects**
Process acting on behalf of a user of the storage management client terminal	Banner information file	Viewing of banner information is always authorized.

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
None

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 [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].**

The following table describes the assignment and selection items described above.

[assignment: *list of security attributes*]	[selection: *change default, query, modify, delete*, [assignment: *other operations*]]	[assignment: *the authorized identified roles*]	[assignment: *access control SFP(s), information flow control SFP(s)*]
Account administrator's security role (other than the subject user IDs)	Assignment: assign, unassign	Account administrator, system integrator	ACL access control SFP
User group associated with storage administrator (including upper-level storage administrator), security roles	Selection: delete Assignment: assign user IDs, unassign user IDs	Account administrator, system integrator	ACL access control SFP
Combination of user groups, roles, and resource groups associated with a storage administrator's security role	Assignment: assign or unassign resource groups to user groups,modify roles	Account administrators that have the upper-level storage administrator security role, system integrator	ACL access control SFP
Resource groups associated with a storage administrator's security role	Selection: delete Assignment: assign or unassign storage resource information to resource groups	System integrator, upper-level storage administrator	ACL access control SFP

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 [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.**

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]
restrictive.

[assignment: other property]
None

[assignment: *access control SFP, information flow control SFP*]
ACL access control SFP

[assignment: *the authorised identified roles*]
None

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 **The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].**

The following table describes the assignment and selection items listed above.

[*assignment: list of TSF data items*]	[selection: *change the default values of, query, modify, delete, clear,* [assignment: *other operations*]]	[assignment: *the authorized identified roles*]
Password associated with a user ID other than the system integrator user ID	Selection: modify Assignment: register	System integrator, account administrator
	Selection: modify	Storage administrator whose user ID is to be modified
Password associated with the system integrator user ID	Selection: modify	System integrator, account administrator
Lock status of a storage administrator	Selection: query, modify	System integrator, account administrator
Lock status of the system integrator	Selection: query, modify	Account administrator
Lock status of an account administrator	Selection: query, modify	System integrator, account administrator (The modification of the lock status of the account administrator is excluded)
Security parameter	Selection: query, modify, clear	System integrator, account administrator
Value for whether an account is subject to external authentication or internal authentication	Selection: change the default value, query, modify	System integrator, account administrator
User ID other than the system integrator user ID and the subject's user ID	Selection: delete	System integrator, account administrator

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: [assignment: *list of management functions to be provided by the TSF*].**

The following table describes the assignments listed above.

[assignment: list of management functions to be provided by the TSF]

Management function
Deleting a user ID other than the system integrator user ID
Registering passwords to be associated with a user ID other than the system integrator user ID
Modifying passwords associated with a user ID other than the system integrator user ID
Modifying the password associated with the system integrator user ID
Querying the lock status of a storage administrator's account
Modifying the lock status of a storage administrator's account
Querying the lock status of the system integrator's account
Modifying the lock status of the system integrator's account
Querying the lock status of an account administrator's account
Modifying the lock status of an account administrator's account
Querying a security parameter
Modifying a security parameter
Deleting a security parameter
Changing the default value for whether an account is to be subject to external authentication or internal authentication
Inquiring about the specified value for whether an account is to be subject to external authentication or internal authentication
Modifying the specified value for whether an account is to be subject to external authentication or internal authentication
Assigning the account administrator security role
Unassigning the account administrator security role
Deleting user groups associated with the storage administrator security role
Assigning user IDs to a user group associated with the storage administrator security role

Unassigning user IDs from a user group associated with the storage administrator security role
Assigning resource groups to a user group associated with the storage administrator security role
Modifying the roles of user groups as they correspond to resource group associated with the storage administrator security role
Unassigning resource groups from a user group associated with the storage administrator security role
Deleting resource groups associated with the storage administrator security role
Assigning storage resource information to a resource group associated with the storage administrator security role
Unassigning storage resource information from a resource group associated with the storage administrator security role

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 [assignment: *the authorised identified roles*].**

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

[assignment: *the authorised identified roles*]

Storage administrator, account administrator, system integrator

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the [refinement:user] to be performed before the [refinement:user] is authenticated.**

FIA_UAU.1.2 **The TSF shall require [refinement:each user] to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that [refinement:user].**

[assignment: *list of TSF mediated actions*]

Warning banner function, license management function (Product version display function)

[refinement: user]

A user of a storage management client terminal for which use of internal authentication is specified

[refinement: each user]

Each user of a storage management client terminal for which use of internal authentication is specified

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 **The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the [refinement:user] to be performed before the [refinement:user] is identified.**

FIA_UID.1.2 **The TSF shall require [refinement:each user] to be successfully identified before allowing any other TSF-mediated actions on behalf of that [refinement:user].**

[assignment: *list of TSF-mediated actions*]

Warning banner function, license management function (Product version display function)

[refinement: user]

A user of a storage management client terminal

[refinement each user]

Each user of a storage management client terminal

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 [assignment: *a defined quality metric*].**

[assignment: a defined quality metric]

Minimum length (minimum number of characters): The number of characters specified in the corresponding security parameter

Complexity: The level of complexity (the required combination of alphanumeric characters and symbols) specified in the corresponding security parameter

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: [assignment: list of security attributes].**

[assignment: list of security attributes]

User ID, security role

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *list of user security attributes*]

User ID, security role

[assignment: rules for the initial association of attributes]

user	subjects acting on the behalf of that user	user security attributes and the value (attributes:value)
System integrator	Process acting on behalf of the system integrator	User ID: System Security Role: System integrator
Account administrator	Process acting on behalf of an account administrator	User ID: Authenticated user ID Security Role: Registered security role associated with the user ID
Storage administrator	Process acting on behalf of a storage administrator	User ID: Authenticated user ID Security Role: Registered security role associated with the user ID

[assignment:rules for changing attributes]

None

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].**

FIA_AFL.1.2 **When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].**

[assignment: *list of authentication events*]

user accounts to be used since the last successful authentication (except for those user accounts for

which an authentication function external to the TOE is used)

[selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*]

An administrator-configurable positive integer within the following range: *[assignment: range of acceptable values]*]

[assignment: range of acceptable values]

The range of values specified in the security parameters

[selection: *met, surpassed*]

met

[assignment: *list of actions*]

Lock an account (except for those user accounts for which the external authentication function is used).

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 **Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.**

6.2. Security assurance requirements

The evaluation assurance level of this TOE is EAL2, which is augmented with the ALC_FLR.1 assurance component.

All assurance requirement components are directly derived from the assurance components specified in CC Part 3. **Table 6-1** lists the assurance components with EAL2 augmented (EAL2 + ALC_FLR.1).

Table 6-1 Assurance components with EAL2 augmented (EAL2 + ALC_FLR.1)

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

6.3. Security requirements rationale

This section describes the rationale for the TOE security functional requirements. All functional requirement components to be used are specified in CC Part 2.

6.3.1. Security functional requirements rationale

Table 6-2 describes the relationship between the security functional requirements selected for the TOE and the TOE security objectives.

Table 6-2 Relation between TOE security functional requirements and TOE security objectives

TOE security objective / TOE security functional requirement	O.I&A	O.MGMT	O.BANNER	O.PASSWORD
FDP_ACC.1		X	X	
FDP_ACF.1		X	X	
FMT_MSA.1		X		
FMT_MSA.3		X		
FMT_MTD.1	X	X		
FMT_SMF.1		X		
FMT_SMR.1		X		
FIA_UAU.1	X			
FIA_UID.1	X			
FIA_SOS.1				X
FIA_ATD.1	X			
FIA_USB.1	X			
FIA_AFL.1	X			
FTA_TAB.1			X	

As shown in **Table 6-2**, each security functional requirement for the TOE corresponds to at least one TOE security objective.

The following describes how each security objective for the TOE can be achieved by implementing the security functional requirements for the TOE.

O.I&A

When a user of a storage management client terminal for which the use of internal authentication is specified accesses the TOE, the TOE uses **FIA_UID.1** to check whether the user is authorized and uses **FIA_UAU.1** to identify the user. If repeated authentication attempts by the user fail the predefined number of times, the TOE uses **FIA_AFL.1** to lock the user's account. The TOE uses **FIA_ATD.1** to maintain the user ID and the user's role, and uses **FIA_USB.1** to associate the user ID and role of a user who has been successfully identified and authenticated with the process that acts on behalf of the user.

The TOE also uses **FMT_MTD.1** to allow only account administrators and the system integrator to manage user IDs, passwords, and the lock status registered for each user.

O.I&A can therefore be handled by **FIA_UAU.1, FIA_UID.1, FIA_ATD.1**, **FIA_AFL.1**, **FIA_USB.1**, and **FMT_MTD.1**.

O.MGMT

The TOE uses **FDP_ACC.1** and **FDP_ACF.1** to control access to the banner information file and storage resource information. In addition, if the security role associated with the subject includes the Modify permission for a specific storage resource, this access control allows the user to modify the storage resource. Furthermore, if the user's security role is account administrator or system integrator, the user can modify, create, or delete banner information.

The TOE uses **FMT_SMR.1** to maintain the system integrator, account administrator, and storage administrator security roles, and uses **FMT_MSA.1** to prevent general storage administrators from managing the following security attributes: user IDs and security roles. The TOE also uses **FMT_MSA.3** to provide specified user IDs as restricted initial values when a security role is created.

The TOE uses **FMT_MTD.1** to allow only account administrators and the system integrator to manage users' authentication methods (to select whether internal authentication or external authentication is to be used), delete the use ID as well as users' security parameters and lock statuses. The TOE uses **FMT_SMF.1** to enable execution of the management functions indicated by the management items.

O.MGMT can therefore be handled by **FDP_ACC.1**, **FDP_ACF.1, FMT_MSA.1**, **FMT_MSA.3**, **FMT_MTD.1**, **FMT_SMF.1**, and **FMT_SMR.1**.

O.BANNER

The TOE uses **FTA_TAB.1** to display the advisory warning messages regarding illegal use of the TOE before user session establishment (login screen). When providing these messages, the TOE uses **FDP_ACC.1** and **FDP_ACF.1** to control access to the banner information file so that the banner information file containing the warning messages can always be viewed.

O.BANNER can therefore be handled by **FTA_TAB.1**, **FDP_ACC.1**, and **FDP_ACF.1**.

O.PASSWORD

The TOE uses **FIA_SOS.1** to maintain quality standards for secrecy (passwords) for those users for whom internal authentication is used.

O.PASSWORD can therefore be handled by **FIA_SOS.1**.

6.3.2. Security functional requirement dependencies

Table 6-3 describes the dependencies of the security functional requirement components.

Table 6-3 Dependencies of the security functional requirement components

Functional requirement component selected in this ST	Dependent component specified in CC Part 2	Dependent component selected in this ST	Whether achieved
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	○
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	○
	FMT_MSA.3	FMT_MSA.3	○
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1	○
	FMT_SMF.1	FMT_SMF.1	○
	FMT_SMR.1	FMT_SMR.1	○
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	○
	FMT_SMR.1	FMT_SMR.1	○
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	○
	FMT_SMR.1	FMT_SMR.1	○
FMT_SMF.1	None	－	－
FMT_SMR.1	FIA_UID.1	FIA_UID.1	○
FIA_UAU.1	FIA_UID.1	FIA_UID.1	○
FIA_UID.1	None	－	－
FIA_SOS.1	None	－	－
FIA_ATD.1	None	－	－
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	○
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	○
FTA_TAB.1	None	-	-

Each security functional requirement therefore satisfies all necessary dependencies.

6.3.3. Rationale for security assurance requirements

The evaluation assurance level of this TOE is EAL2 augmented by the ALC_FLR.1 assurance component.

It is assumed that the users of this TOE are restricted to storage administrators that each user is registered, and that there are a limited number of users. Therefore, any intent to attack the system can be repressed. EAL2 is the appropriate choice because it includes evaluation from the point of view of structural design, secure delivery procedures, and vulnerability assessment for the TOE with the described characteristics.

Handling problems related to security vulnerabilities has recently become important. This product plays an important part in managing storage systems, and it is crucial to trace security flaws and act quickly when vulnerability problems arise. Because assurance in the face of security flaws is important in providing safety for users, we have selected ALC_FLR.1.

7. TOE summary specification

This section describes the TOE security functions.

7.1. Identification and authentication function (SF.I&A)

When a user of a storage management client terminal uses the TOE, **SF.I&A** identifies and authenticates the user. **SF.I&A** manages the session of a user who has logged in and confirms that the identification and authentication of the user are maintained.

(1) Identifying and authenticating users

SF.I&A compares a user of a storage management client terminal for whom internal authentication is specified against the account information (user ID, password, and lock status (locked or unlocked)) registered for the user, and identifies and authenticates the user based on the result. For a user of a storage management client terminal for whom external authentication is specified, an external authentication server identifies and authenticates the user, and the TOE receives the result from the external authentication server.

If the user of the storage management client is successfully identified and authenticated by the TOE internal authentication function or the external authentication server, **SF.I&A** associates the user ID entered by the user with the process (subject) that acts on behalf of the user. **SF.I&A** then accesses the ACL table to acquire the user's role.

If the acquired role contains a security role for using the TOE, **SF.I&A** proceeds to the session management described in (3) below.

If **SF.I&A** is unable to identify or authenticate a user, if the user account is locked, or if the acquired role does not include a security role for the TOE, **SF.I&A** returns an error and displays an error message in the storage management client terminal's window.

Until **SF.I&A** successfully identifies and authenticates the user, the TOE does not perform any operations other than sending a warning message provided by the warning banner function (**SF.BANNER**) and the license management function (Product version display function).

The TOE ensures that the **SF.I&A** operations are always performed when the TOE accepts a request from a storage management client terminal to identify and authenticate a user.

(2) Automatically locking accounts

When the TOE internal authentication function is used to identify and authenticate a user who attempts to log in to the TOE, if repeated authentication attempts for the same user fail a preset number of times, **SF.I&A** automatically locks the user account. The account is locked indefinitely. **SF.MGMT** unlocks a user account and sets a threshold for the number of consecutive authentication failures to be used as the trigger to automatically lock the account. **SF.I&A** manages the number of consecutive authentication failures for each user who uses the TOE internal authentication function. The number of consecutive failures for an account is reset when the user is successfully authenticated by the TOE internal authentication function, or when the account is locked because the number of consecutive authentication failures occurring when the TOE internal authentication function is used has reached the threshold.

(3) Managing sessions

When **SF.I&A** has successfully identified and authenticated a user and acquired the necessary security role as described above, **SF.I&A** maintains and manages the user ID and security role of the user as session data, and associates the user ID and security role with the process that acts on behalf of the user.

When the GUI issues a request to execute the security information management function provided by **SF.MGMT**, the TOE proceeds to **SF.MGMT** processing. At this time, **SF.I&A** maintains and manages the session data described above while the security information management function is operating.

If the TOE issues a login authentication request for a new user, **SF.I&A** generates and identifies a session for the user who is attempting to log in. If a login authentication request is issued for a user who is already logged in, **SF.I&A** generates and identifies a new session for the user. Because **SF.I&A** generates a separate session for each login, if the same user logs in several times, **SF.I&A** generates and identifies a new session for each of the times the user logs in.

After a session for a user who has successfully logged in to the TOE is established, **SF.I&A** checks the session data to confirm the validity of the session upon receiving a user's session validity confirmation request from the GUI.

If **SF.I&A** determines that the user session is valid, **SF.I&A** returns the user ID and security role of the user in response to the GUI. If **SF.I&A** determines that the user session is not valid, **SF.I&A** returns an error to the GUI.

If **SF.MGMT** deletes or locks an account, **SF.I&A** invalidates any logged-in sessions for that account, and prohibits new sessions from being generated.

7.2. Security information management function (SF.MGMT)

SF.MGMT manages the authentication method, account information, ACL table, banner information, and security parameters, etc, for each user. Before **SF.MGMT** can be used, the security role of a user must be assigned.

(1) Managing accounts

SF.MGMT manages the user ID, password, lock status (locked or unlocked), and authentication method (external or internal authentication) for each user as account information. When a user sends a request, **SF.MGMT** provides methods for registering or deleting the user ID (account), registering or modifying the password, querying or modifying the lock status, or changing the default value for the authentication method (external or internal authentication), or querying or modifying.

SF.MGMT allows account administrators and the system integrator to perform all of the above operations. For storage administrators, **SF.MGMT** only permits an administrator to change the administrator's own password. Note that **SF.MGMT** does not allow any user to register a new account that has the system integrator role or to delete an account that has the system integrator role.

(2) Checking the complexity of passwords

SF.MGMT checks whether a password satisfies the following quality criteria when a new account is created or when a password is registered or changed. **SF.MGMT** does not allow any password that does not satisfy the quality criteria to be set.

- The password must satisfy the minimum number of characters required in a password. This number is determined by a security parameter.
- The password must satisfy the condition for password complexity (a combination of alphanumeric characters and symbols). This complexity is determined by a security parameter.

(3) Managing the ACL table

SF.MGMT manages each user's user ID andthe ACL table. In response to a request from a user, **SF.MGMT** accesses the security role derived from ACL table and provides methods for registering, modifying, or deleting ACL table information according to authorized roles.

When a process that acts on behalf of a user of a storage management client terminal performs any of the above operations, **SF.MGMT** controls access to the ACL table based on the user ID and security role associated with the process (the subject), according to the following rules:

- When the security role associated with the subject is account administrator or system integrator, **SF.MGMT** allows the process to create, delete, and modify the security role for the user (user ID).

  Note that the user ID must be specified when a security role is created, and that the relationship between the user ID and the security role takes effect as soon as the security role is created.

  The system integrator and account administrators can specify a user ID and delete the corresponding security role. They can also delete a security role by deleting the corresponding user ID (account).
- If the security role associated with the subject is account administrator or system integrator, **SF.MGMT** allows the process to assign or unassign security roles for user IDs, to delete user groups associated with a storage administrator's security role, and to assign or unassign user IDs to a user group.
- If the security role associated with the subject is system integrator or account administrator with the upper-level storage administrator security role, **SF.MGMT** allows the process to assign or unassign user groups associated with a storage administrator's security role, and to modify roles.
- If the security role associated with the subject is system integrator or upper-level storage administrator security role, **SF.MGMT** allows the process to delete resource groups, and to assign or unassign storage resource information.

SF.MGMT ensures that the access control described above is always performed.

Only authorized processes can access the information in the ACL table. Accordingly, **SF.MGMT** ensures that information in the ACL table can be changed only by processes acting on behalf of users that have been successfully identified and authenticated, and not by untrusted processes.

(4) Managing security parameters

SF.MGMT manages, as security parameters, the variable parameters related to functions of the automatic locking of accounts and the complexity checking of passwords. **Table 7-1** lists the security parameters. In response to a request from a user, **SF.MGMT** provides methods for querying, modifying, and clearing these parameters.

SF.MGMT permits only account administrators and the system integrator to perform these operations.

Table 7-1 Security parameters

#	Parameter	Description
1	Threshold value for the number of consecutive authentication attempt failures	The threshold value used by the automatic account lock function as the trigger for automatically locking accounts when repeated authentication attempts fail
2	Minimum number of characters in a password	The minimum number of characters to be used in a password
3	Password complexity condition	A condition specifying that a certain number of certain types of characters must be included in a password

(5) Managing banner information

SF.MGMT manages advisory warning messages regarding illegal use of the TOE as banner information.

When a process that acts on behalf of a user of a storage management client terminal performs any of the above operations, **SF.MGMT** controls the ability to generate, delete or change the banner information file based on whether the security role associated with the process (the subject) is account administrator or system integrator.

SF.MGMT ensures that the access control described above is always performed.

(6) Managing storage resource information

When a process that acts on behalf of a user of a storage management client terminal has the Modify permission for storage resource information, **SF.MGMT** controls access to the ability to modify the storage resource information based on the security role associated with the process.

SF.MGMT ensures that the access control described above is always performed.

7.3. Warning banner function (SF.BANNER)

SF.BANNER displays banner information that is set by **SF.MGMT**. The TOE displays this warning message in the login window used for identifying and authenticating the user of the storage management client terminal.

7.4. Relation between the TOE security functional requirements and the TOE security functions

This section describes the TOE security functions. As shown in **Table 7-2**, the security functions described in this section satisfy the TOE security functional requirements described in subsection **6.1**.

Table 7-2 Relation between TOE security functions and TOE security functional requirements

TOE security function \ TOE security functional requirement	FDP_ACC.1	FDP_ACF.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FIA_UAU.1	FIA_UID.1	FIA_SOS.1	FIA_ATD.1	FIA_USB.1	FIA_AFL.1	FTA_TAB.1
SF.I&A								X	X		X	X	X	
SF.MGMT	X	X	X	X	X	X	X			X				
SF.BANNER	X	X												X

FDP_ACC.1:

FDP_ACF.1:

When the process (the subject) that acts on behalf of a user of the storage management client modifies storage resource information (the object) and modifies, creates or deletes the banner information file (the object), the TOE uses **SF.MGMT** to control access to the object according to the security role associated with the subject.

When the process (the subject) that acts on behalf of a user of the storage management client reads the banner information file (the object), the TOE uses **SF.BANNER** to display a warning message.

FDP_ACC.1 and **FDP_ACF.1** can therefore be handled by **SF.MGMT** and **SF.BANNER**.

FMT_MSA.1:

The TOE uses **SF.MGMT** to allow only processes that have the account administrator or the system integrator security role to assign or unassign the account administrator security role, to

assign or unassign the user IDs associated with a storage administrator's security role, or to delete user groups associated with a storage administrator's security role.

The TOE uses **SF.MGMT** to allow only processes that have the system integrator security role or the account administrator security role with the upper-level storage administrator security role to assign or unassign resource groups to user groups associated with a storage administrator's security role, or to modify roles.

The TOE uses **SF.MGMT** to allow only processes that have the system integrator or the upper-level storage administrator security role to delete resource groups, or to assign or unassign storage resource information to a resource group.

FMT_MSA.1 can therefore be handled by **SF.MGMT**.

FMT_MSA.3:

When a security attribute is generated, the TOE uses **SF.MGMT** to provide the user IDs of the users to whom the security attribute is to be assigned as the restricted initial values of the user IDs listed as security attributes in the ACL table.

FMT_MSA.3 can therefore be handled by **SF.MGMT**.

FMT_MTD.1:

The TOE uses **SF.MGMT** to provide a function that manages the user ID (account), password, lock status, selection of internal or external authentication for each user, and security parameters.

Note that the TOE does not allow any user to delete the user's own user ID or the system integrator's user ID.

The TOE allows only account administrators and the system integrator to register and delete user IDs, to register, change, and delete passwords (which deletes entire accounts), to query and change a user's lock status, to query, change, and clear security parameters, and to query, change, and modify the default value for whether internal or external authentication is to be used.

Note that the TOE does not allow any user to modify the user's own lock status or the system integrator's lock status.

Note that the TOE allows storage administrators to change their own passwords.

The TOE cannot register a new system integrator account or delete the user ID for the existing system integrator account.

FMT_MTD.1 can therefore be handled by **SF.MGMT**.

FMT_SMF.1:

Among the requirements specified in CC Part 2 for the functional requirements selected in this ST, **SF.MGMT** manages all items (list of management functions to be provided by the TSF) that are to

be managed by the TOE as described in section **7.2.**

FMT_SMF.1 can therefore be handled by **SF.MGMT**.

FMT_SMR.1:

The TOE uses **SF.MGMT** to maintain the storage administrator, account administrator, and system integrator roles by managing the ACL table.

FMT_SMF.1 can therefore be handled by **SF.MGMT**.

FIA_UAU.1, FIA_UID.1:

Until **SF.I&A** successfully identifies and authenticates the user of a storage management client terminal for whom internal authentication is specified, the TOE does not perform any operation except displaying a warning message provided by the warning banner function (**SF.BANNER**) and carrying out the operations of the license management function (Product version display function).

FIA_UAU.1 and **FIA_UID.1** can therefore be handled by **SF.I&A**.

FIA_SOS.1:

When a new account is created or when a password is registered or modified inside the TOE, the TOE uses **SF.MGMT** to provide mechanisms for verifying that the password satisfies the following quality criteria:

- The password must satisfy the minimum number of characters required in a password. This number is determined by a security parameter.
- The password must satisfy the condition for password complexity (a combination of alphanumeric characters and symbols). This complexity is determined by a security parameter.

FIA_SOS.1 can therefore be handled by **SF.MGMT**.

FIA_ATD.1, **FIA_USB.1:**

The TOE uses **SF.I&A** to maintain and manage user IDs and security roles, and to associate user IDs with security roles if the process that acts on behalf of a storage management client user has been successfully identified and authenticated.

FIA_ATD.1 can therefore be handled by **SF.I&A**.

FIA_AFL.1:

When the TOE performs authentication for a user for whom internal authentication is specified, the TOE uses **SF.I&A** to lock the account of a user whose authentication attempts have repeatedly failed a predefined number of times.

FIA_AFL.1 can therefore be handled by **SF.I&A**.

FTA_TAB.1:

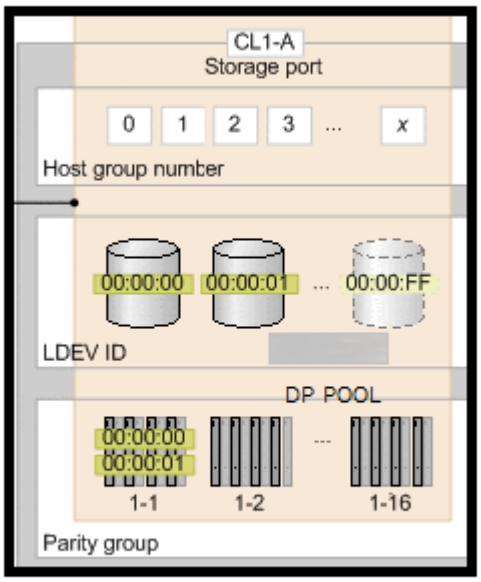
The TOE uses **SF.BANNER** to display an advisory warning message regarding illegal use of TOE in the login window.

FTA_TAB.1 can therefore be handled by **SF.BANNER**.

8. Terms

Table 8-1 describes the terms and abbreviations used for this Security Target.

Table 8-1 Meaning of terms and abbreviations

Term	Meaning
SAN	Abbreviation for storage area network
Banner information	Information used for the warning banner functionality
Storage resource information	Storage resource information (storage ports, host group numbers, LDEV IDs, DP pools, and parity groups), which is managed by the TOE. The following conceptual diagram shows storage resources on a storage system. The parity group represents the location of physical disks. In DP pools and volumes, parity groups are divided into logical access units. LDEV IDs are used as logical identifiers for these divisions. In addition, for physical storage ports, host group numbers are used as identifiers for the groups for which I/O to the volume is permitted.  Storage System

Permissions	Permissions represent the actions that the TOE allows a user to perform for a given resource. Permissions such as User Management permissions, Admin permission, Modify permission, View permission, and CUSTOM (provisioning) permission are necessary for users to view or modify storage information or to perform tasks.
Role	A combination of TOE permissions. The role of the storage administrator, as described in the manuals, is Admin, which is a combination of the Admin, Modify, and View permissions. You can modify the storage administrator access control table by assigning roles that correspond to user groups and resource groups. Admin permissions allow a user to manage resources, Modify permissions allow a user to edit resources, and View permissions allow a user to view resources. Most importantly, you can allow a user to manage resource groups and storage systems by assigning that user the Admin role for all resources.
ACL table	A table used to define access control information for the TOE. This table defines the operating permissions assigned to each user ID for each resource.
Security role	A role classified from a security perspective, and assigned to a process that acts on behalf of a TOE user. There are three possible security roles in the TOE: system integrator, account administrator, and storage administrator. The operations that a process can perform in the TOE are determined based on the assigned role.
User group	User groups facilitate the management of user accounts by grouping storage administrators who have the same operating permissions.
Resource group	Resource groups facilitate the management of access control for storage resource information by grouping resources such as storage systems, parity groups, LDEV IDs, and storage ports.
HBase	HBase is the base module that provides common functions for the storage management software available in Hitachi Command Suite.
HDvM	Hitachi Device Manager Software. HDvM is storage management software. It is part of Hitachi Command Suite, and provides volume management functionality for storage systems.
HRpM	Hitachi Replication Manager Software HRpM is storage management software. It is part of Hitachi Command Suite, and provides functionality for managing copying between volumes in storage systems.

HTSM	Hitachi Tiered Storage Manager Software. HTSM is storage management software. It is part of Hitachi Command Suite, and controls the movement of data between volumes in storage systems.
HTnM	Hitachi Tuning Manager Software. HTnM is storage management software. It is part of Hitachi Command Suite, and provides functionality for managing the efficiency with which the resources in storage systems are used.
HGLM	Hitachi Global Link Manager HGLM is storage management software. It is part of Hitachi Command Suite, and provides integrated path management for large system configurations.
HCSM	Hitachi Compute Systems Manager HCSM is storage management software. It is part of Hitachi Command Suite, and provides functionality for supporting cost-efficient server management and high availability of the target servers.
Security parameter	Parameter information related to TOE security functions. Parameter information includes such information as the number and type of characters permitted in passwords; the number of consecutive login failures and the corresponding threshold; and whether the threshold has been exceeded, in which case the account is locked.
Warning banner	Warning text displayed before users start to use the TOE. Warning banners are mainly used to call attention to the possibility of illegal use.
Internal authentication	An authentication method that uses only the TOE internal authentication functionality.
External authentication	An authentication method that uses an external authentication server (an LDAP directory server, a RADIUS server, or a Kerberos server) from inside the TOE.
External authentication group linkage	A function of the TOE that acquires information about a group registered on an external authorization server and the accounts in that group, and then passes permissions information to the TOE. Because this function requires authentication functionality external to the TOE and because the accounts belong to a group, this function is called *external authentication group linkage*.

Storage management client	A storage management client process acting on behalf of the storage administrator or another user to communicate with storage management software.
Storage management client terminal	The computer on which a storage management client process is being executed.