Hitachi Command Suite Common Component

Security Target

2011/4/19

Version 3.09

Hitachi, Ltd.

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

Hitachi Command Suite Common Component Security Target

Trademarks

- Active Directory is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Linux is a trademark or registered trademark of Linus Torvalds in Japan and other countries.
- Microsoft is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries.
- SUSE is a trademark of Novell, Inc. in Japan.
- Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.
- All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.
- Sun and Sun Microsystems are trademarks or registered trademarks of Oracle Corporation and its affiliates 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 Command Suite Common Component Security Target

- Contents -

1. ST Introduction

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

1.1. ST identification

ST title: Hitachi Command Suite Common Component Security Target

ST version: 3.09

Identification name: HSCC-ST-3.09

Date: April 19, 2011

Author: Hitachi, Ltd., Software Division

1.2. TOE identification

TOE name: Hitachi Command Suite Common Component

TOE version:7.0.1-00

Keyword: Storage management software

Developer: Hitachi, Ltd., Software Division

1.3. TOE Overview

1.3.1. TOE type and security functions

(1) TOE type

The TOE is a software product that provides the basic module that implements common functions for the storage management software in the Hitachi Command Suite series.

The target of evaluation, Hitachi Command Suite Common Component (abbreviated hereafter to *HSCC*), runs as the base module that provides the common functions for storage management software that centrally manages multiple storage devices connected in a SAN environment.

The storage management software includes Hitachi Device Manager Software (abbreviated hereafter to *HDvM*), Hitachi Replication Manager Software (abbreviated hereafter to *HRpM*), and Hitachi Tiered Storage Manager Software (abbreviated hereafter to *HTSM*), Hitachi Tuning Manager Software (abbreviated hereafter to *HTnM*), etc. These products and HSCC are generically referred to as Hitachi Command Suite.

HSCC is bundled with each product package as the base module of Hitachi Command Suite.

A storage system (abbreviated hereafter to *storage*) contains multiple volumes in a frame, and is connected to an application server that runs business applications. These volumes store information required to run the business applications. Because the size of storage tends to increase as the size of the information system increases, operation of the information systems requires storage management software that is able to manage large-scale storage, the capacity of which continually increases. This means that the following operations must be carried out

satisfactorily:

- Volume allocation (For example, HDvM enables an application server to access storage volumes.)
- Copy management (For example, HRpM manages the copying of volumes that contain business data.)
- Data movement (HTSM moves old data to other storage to free up volumes.)
- Performance monitoring (HTnM monitors the SAN or volume usage to ensure that the system operates efficiently.)

In order to perform these operations on many volumes and storage systems, the storage administrator uses storage management software with the appropriate functions, from the management devices connected to the target storage to centrally manage the storage. Hitachi Command Suite provides a group of software products that manage storage in the manner described above. **Figure 1** outlines a system that uses Hitachi Command Suite to manage storage.

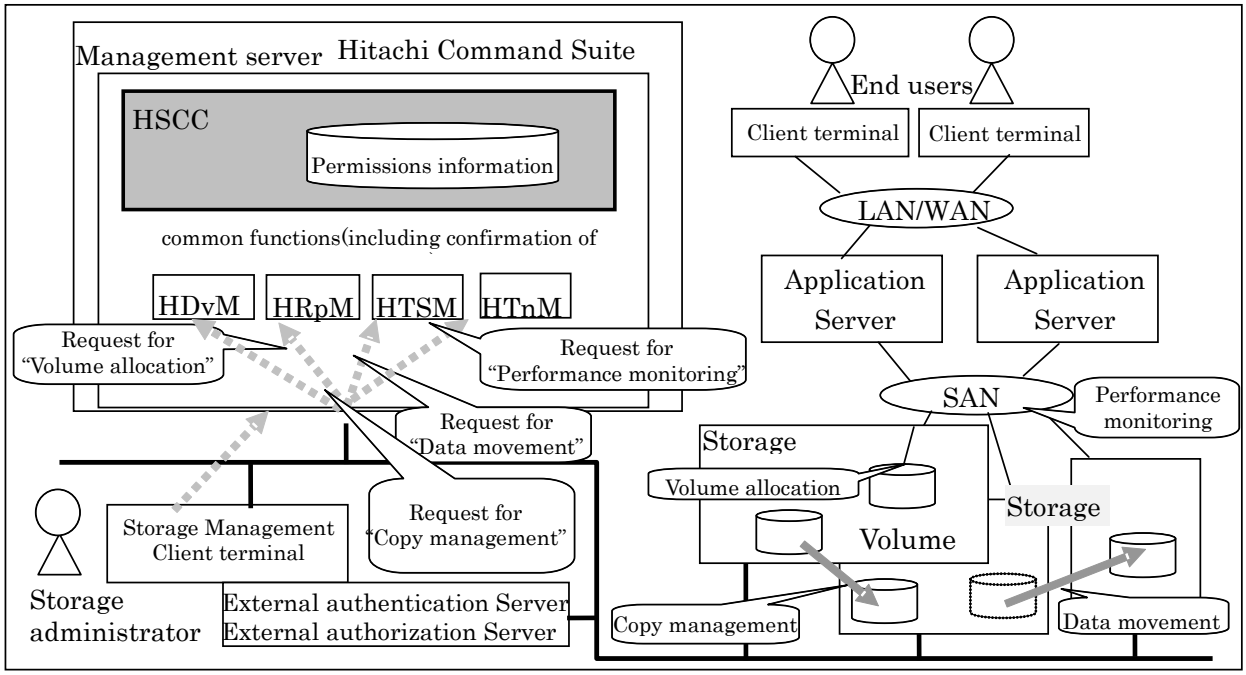

Figure 1: Overview

In **Figure 1**, the storage administrator requests a required operation, such as copying, by accessing the necessary storage management software from a client terminal. The TOE provides common functions for the storage management software, such as authentication, the display of permissions information, and a graphical user interface for displaying information on the client terminal.
The TOE identifies and authenticates the user prior to performing the requested storage management operation. The TOE then controls access to permissions information so that the

storage management operation requested by the storage administrator, such as volume allocation or copy monitoring, can be performed correctly within the authorized scope.

The TOE also provides account information for authentication as well as functions that allow account administrators to set permission information.

(2) Security functions

The TOE security functions are as follows:

- Identification and authentication

  The identification and authentication function uses IDs and corresponding passwords to authenticate users, and generates and maintains sessions based on the result. It also passes permissions information to the requesting user based on the result of authentication.

- Security information management

  The security information management function manages account information, permissions information, and banner information, including the creation, viewing, modification, and deletion of banner information. It also sets security parameters.

- Warning banner

  The warning banner function inputs and displays warning message data to be viewed by those who perform Hitachi Command Suite operations.

1.3.2. TOE configuration

The physical TOE consists of the libraries and programs below.

Figure 2 shows the software configuration that includes the TOE. The TOE is HSCC. The modules implementing the TOE security functions are shaded.

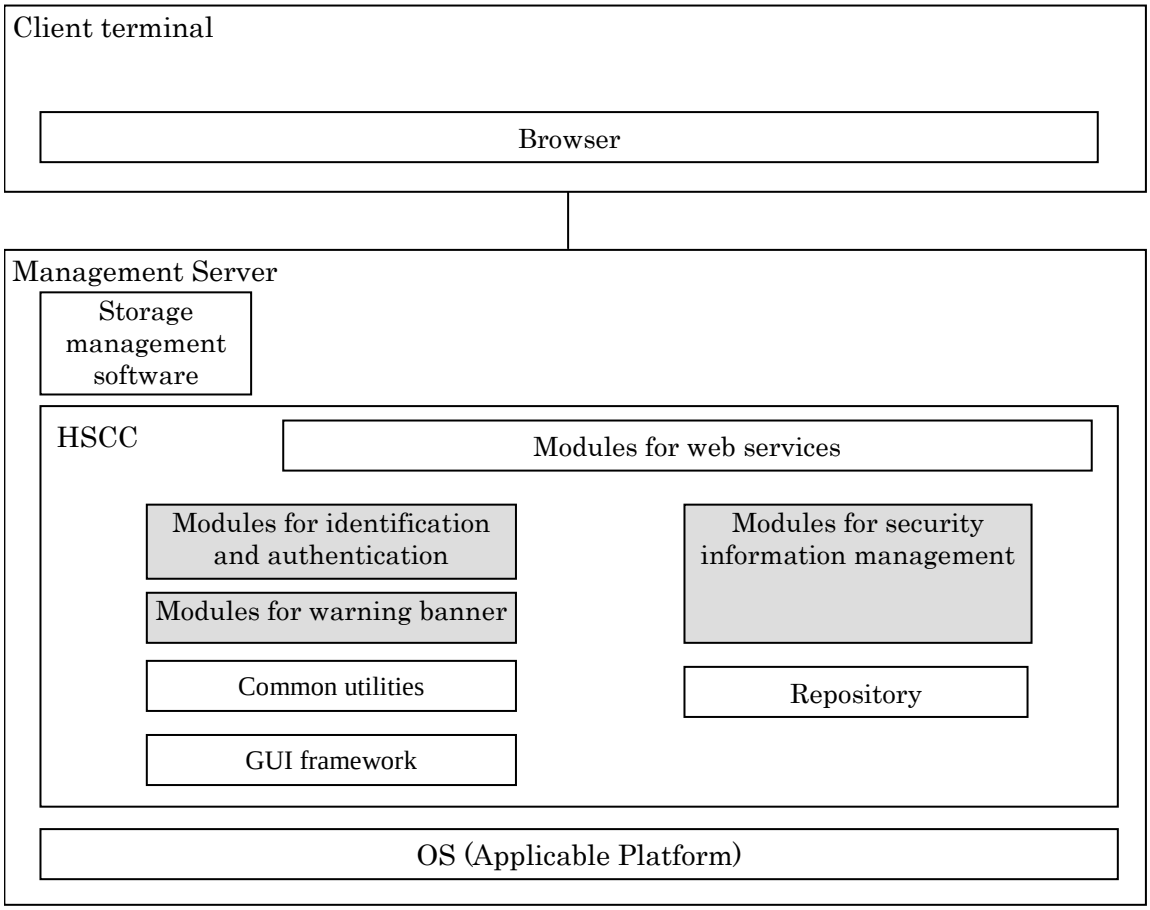

Figure 2: Software configuration including the TOE

Identification and Authentication Module is a module that implements the identification and authentication function of the TOE.

Security Information Management Module is a module that implements the security information management function of the TOE.

Warning Banner Module is a module that implements the warning banner functionality of the TOE.

Common Utility is a module that implements the common functions of the TOE.

Web Service Module is a module that implements the TOE Web service.

GUI Framework is a module that implements the TOE graphical user interface.

Repository is the database that stores data for the TOE.

1.3.3. TOE operational environment

1.3.3.1. Environment in which the TOE is used

Figure 3 shows an example of a system configuration that uses the TOE.

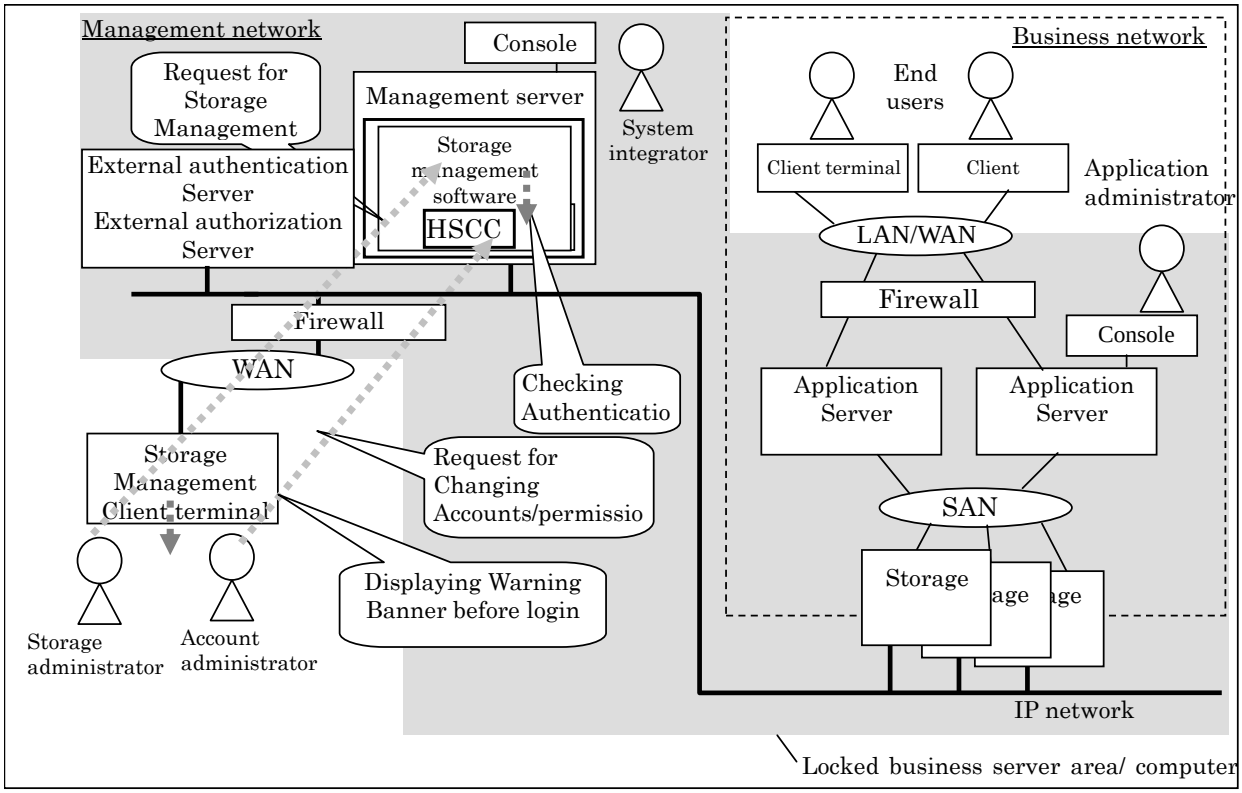

Figure 3: TOE model

In **Figure 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, and peripheral devices are installed in the business server area. Physical entry to and exit from this area are controlled with a lock or similar means.

The management network and the business network within the firewall are called internal networks. The networks outside the firewall are called external networks.
Management servers, storage, and peripheral devices are connected to the management network. Application servers, storage, and peripheral devices are connected to the business network. The internal networks are protected from external networks by a firewall.
Storage that belongs to both an external and an internal network has two, independent NICs, one of which connects to the management network and the other of which 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, the storage administrator and the account administrator use a storage management client terminal to issue operation requests to the storage management software. At this time, the TOE continuously displays a warning banner in the login

window cautioning TOE operators (including users) about illegal use. In addition, the storage administrator and the account administrator use difficult-to-guess passwords to access the TOE. In **Figure 3**, an external authentication server and external authorization server have been set up. The external authentication server can be used in place of the TOE identification and authentication function. The TOE can grant permissions to a group registered on the external authorization server as long as a 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 storage management software within the scope of the permissions granted by the TOE.

The external authentication server and external authorization server are installed in the same business server area as the storage management software server. However, the two servers can be installed in a different business server area from that of the storage management server if the confidentiality and integrity of the channel between the two servers can be guaranteed. If the confidentiality and integrity cannot be guaranteed, the servers must be installed within the same locked business server area. Note that any method can be used to install the external authentication server and external authorization server. For example, any of the following are possible: (1) The external authentication server and the external authorization server are physically different machines, (2) the external authentication server and the external authorization server are physically the same machine but different software is used, and (3) the external authentication server and the external authorization server are physically the same machine and the software is also the same.

1.3.3.2. Software requirements

The TOE software requirements are described below.

(1) Management server

- Platform running Java™ VM (Version 1.5.0_11 or later) that has been installed by Hitachi Command Suite Common Component for Windows
- Platform running Java™ VM (Version 1.5.0_05 or later) that has been installed by Hitachi Command Suite Common Component for Solaris
- Platform running Java™ VM (Version 1.5.0_05 or later) that has been installed by Hitachi Command Suite Common Component for Linux

(2) Storage management client terminal

[When the client OS is Windows]

- Microsoft Internet Explorer 6.0, 7.0, or 8.0

[When the client OS is Linux]

- Firefox 3.6.0 or later

[When the client OS is Solaris]

- Firefox 3.6.0.0 or later

(3) External authentication server and external authorization server

Microsoft Active Directory (supplied with the Windows Server 2003 series or Windows Server 2008 series of operating systems)

1.3.3.3. Hardware requirements

The TOE hardware requirements are described below.

(1) In Windows

Devices in the following series that support the Windows platform described in Section 1.3.3.2

- Hitachi BladeSymphony series
- Hitachi HA8000 series
- Hitachi or Non-Hitachi PC/AT-compatible devices

The minimum requirements are as follows:

CPU clock: 2 GHz

Memory size: 2 GB

Disk size: 5 GB

(2) In Linux

Devices in the following series that support the Linux platform described in Section 1.3.3.2

- Hitachi BladeSymphony series
- Hitachi HA8000 series
- Hitachi or Non-Hitachi PC/AT-compatible devices

The minimum requirements are as follows:

CPU clock: 2 GHz

Memory size: 2 GB

Disk size: 5 GB

(3) In Solaris

Devices in the following series that support the Solaris platform described in Section 1.3.3.2

- Solaris SPARC

The minimum requirements are as follows:

CPU clock: 1.2 GHz

Memory size: 2 GB

Disk size: 5 GB

1.3.4. TOE evaluation configuration

1.3.4.1. Hardware requirements

Windows and Linux

Model name: HP Compaq dc7900SF/CT

CPU: Intel Core2 Quad

RAM: 4 GB

HDD: 1,000 GB

Solaris

Model name: Sun Fire V250

CPU: UltraSPARC-IIIi 1280 MHz *2

RAM: 2 GB

HDD: 64 GB

1.3.4.2. Software requirements

(1) TOE versions

- In Windows
  - Hitachi Command Suite Common Component7.0.1-00(P-2413-6412)
- In Linux
  - Hitachi Command Suite Common Component 7.0.1-00(P-9S13-6412)
  - Hitachi Command Suite Common Component 7.0.1-00(P-9S13-6C12)
- In Solaris
  - Hitachi Command Suite Common Component 7.0.1-00(P-9D13-6412)

(2) Versions of the products containing the TOE

- In Windows
  - Hitachi Command Suite Device Manager 7.0.1-00(P-2Z13-3574)
  - Hitachi Command Suite Replication Manager 7.0.1-00(P-2Z13-3774)

Hitachi Command Suite Tiered Storage Manager 7.0.1-00(P-2Z13-3674)

Hitachi Command Suite Tuning Manager 7.0.0-01(P-2Z13-3874)

- In Linux

  Hitachi Command Suite Device Manager 7.0.1-00(P-2Z13-3574)

  Hitachi Command Suite Replication Manager 7.0.1-00(P-2Z13-3774)

  Hitachi Command Suite Tiered Storage Manager 7.0.1-00(P-2Z13-3674)

- In Solaris

  Hitachi Command Suite Device Manager 7.0.1-00 (P-2Z13-3574)

  Hitachi Command Suite Replication Manager 7.0.1-00 (P-2Z13-3774)

  Hitachi Command Suite Tiered Storage Manager 7.0.1-00(P-2Z13-3674)

  Hitachi Command Suite Tuning Manager 7.0.0-01(P-2Z13-3874)

(3) Installed programs

- In Windows

  Windows Server 2008 R2 Enterprise Edition

- In Linux

  RedHat Enterprise Linux Advanced Edition 5 update 4

  SuSE Linux Enterprise Server 11

- In Solaris

  Solaris 10(SPARC)

- Software common to each OS

  Active Directory (program in Windows 2008)

- Browser

  - In Windows: Internet Explorer 7
  - In Solaris: FireFox 3.6.13
  - In Linux: FireFox 3.6.9

1.4. TOE Description

1.4.1. The logical scope of the TOE

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

Table 1: TOE (HSCC) functions

Function	Overview
Identification and Authentication	Uses user IDs and corresponding passwords to identify and authenticate users, and generates and maintains sessions according to the results. This function also passes permissions information to the requesting user based on the result of authentication.
Security Information Management	Manages account information, permissions information, and banner information (including the creation, viewing, modification, and deletion of banner information). This function also sets security parameters.
Warning Banner	Inputs and displays warning message data to be viewed by those who perform Hitachi Command Suite operations.
Common Utility	Used for setting up and administering Hitachi Command Suite.
Web Service	Provides a Web service so that Hitachi Command Suite can interact with the browsers on client terminals.
GUI Framework	Provides a GUI framework for Hitachi Command Suite.
Repository	Memory area for storing the data used to run Hitachi Command Suite.

(1) Identification and authentication function

This function identifies a TOE user when the user logs on to the storage management software, and passes permissions to the user when the user is authenticated. Permissions information refers to the operation permissions of each storage management software product. For example, a user with Modify permission can set and change resources managed by the storage management software. A user with View permission can only view such resources.

If successive authentication attempts by the user fail for a predefined number of times during the identification and authentication period, the user's account for the TOE is automatically locked. At this point, the identification function uses the identification function in the TOE.

Instead of the TOE's internal authentication function, the TOE can use the external authentication functionality of an external authentication server. When registering accounts, the account administrator sets whether internal authentication or external authentication is used for an account. The internal authentication and the external authentication are independent functions and each account is only authenticated by either internal authentication or external authentication. 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, after which the TOE returns permissions information based on the authentication result.

HSCC 7.0.1-00 provides support for an external authentication group linkage function. This function assigns permissions information managed in the TOE to a group managed on an external authorization server and to the accounts belonging to the group. When the TOE acquires account information about a group and the accounts belonging to that group from the external authorization server, permissions are assigned to the group and accounts in the TOE. Note that when the external authentication group linkage function is used, the external authentication function must be used to identify and authenticate users.

The external authentication group linkage function does not require that the 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. (Accordingly, even if the system integrator's account (System) exists on the external authentication server, the account in the TOE is used as the System account. This means that if a System account is created on the external authentication server, the system integrator's permissions cannot be obtained).

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 needs to be used to prevent threats such as an illegal login through repeated authentication attempts.

(2) Security Information Management function

For the users registered in the TOE, the TOE manages user IDs, passwords, and the lock status

as account information. The TOE stores the variable parameters for automatic account locking and 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. In addition, any permissions information entered for a corresponding user ID is stored in the ACL.

When the external authentication function or 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 needs to be used to protect against threats such as illegal login through repeated authentication attempts.

The TOE manages the warning messages about the illegal use of storage management software as banner information, and provides methods for creating, deleting, and modifying the banner information when so requested by TOE users.

(3) Warning Banner function

This function sets and returns banner information in response to a request from the storage management software.

Banner information is entered by the system integrator or account administrator from a TOE window that allows warning banner messages to be edited. In addition, the system integrator is 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 storage management software operation begins.

Regardless of the method used to set banner information, the TOE returns the set banner information to the storage management software regardless of the permissions and role of the TOE user. Thereafter, the storage management software displays the banner information in the login window.

To send permissions information to the storage management software, the TOE protects the ACL that stores permissions information from changes by unauthorized users. The ACL is associated with user IDs, and has the security attributes of a TOE user role, such as the account administrator role. The ACL contains permissions information about the view and modification processing that is permitted in the storage management software. When the TOE identifies and authenticates a user, it reads the security attributes of the user ID as needed and uses the attributes as access permissions information (session data).

The TOE also provides functions that allow the account administrators to set account information for authenticating users and to set security attributes. Once the account administrator has been identified and authenticated by the TOE (either the internal or external function), the account administrator can access the security information management function of

the TOE from a client terminal and perform account management, such as creating, updating, and deleting user accounts, and setting permissions. Generally, an ACL is TSF data used for access control and is managed by special administrators. However, for the security functions claimed by this TOE, the permissions information in the ACL is treated as user data. The TOE permits access (for example, viewing and updating by a user such as the storage administrator) to the information in the ACL based on the role of the user.

The following explains how to use the TOE.

(1) Preparation by the system integrator

- The system integrator purchases required information system resources, including the TOE.
- The system integrator installs and connects the devices on which the TOE is to be installed, builds the assumption environment for the TOE, installs the TOE, performs setup, and verifies correct operation.
- The system integrator creates an account for the account administrator with the appropriate account management permission 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 the appropriate account and password to access the TOE to be authenticated by the TOE.
- The account administrator creates the accounts for other account administrators and storage administrators in the TOE based on the source information for the accounts to be set. 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 storage administrator

- The storage administrator acquires an appropriate account and password.
- The storage administrator uses the appropriate account and password to access the TOE to obtain authentication by the TOE. After authentication, the storage administrator acquires the permission corresponding to the account.
- After the authentication by the TOE, the storage administrator performs storage management to the extend allowed by the acquired permission.

1.4.2. The physical scope of the TOE

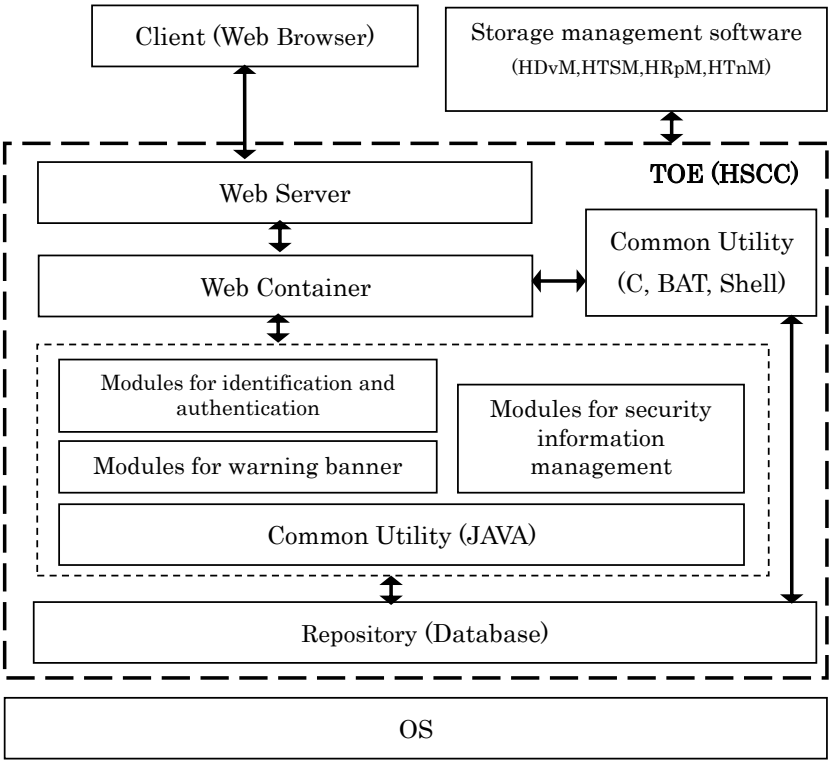

Figure 4: Physical TOE scope (bold dotted line)

In **Figure 4**, the area enclosed in the bold dotted line indicates the physical TOE. This area corresponds to the scope of the logical TOE, and the TOE is HSCC itself.

1.4.3. Guidance documents

The TOE comes with the following guidance document:

- Hitachi Command Suite Common Component Security Guide

1.4.4. TOE user roles

This ST assumes the users described below. Users perform operations according to permissions that have been assigned to them.

(1) System integrator (server / network administrator)

Role Maintains and manages the system by, for example, 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) the permissions of users, which are user data. The system integrator's permissions cannot be changed. Nor can other permissions be added to the system integrator's permissions. The system integrator has already been registered as a system account in the TOE, and has all permissions for the storage management software.

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

(2) Account administrator

Role: Manages the accounts of users who use the system and specify settings for the system.

Permissions: The source information for an account, including whether an account should be created and the permissions that should be granted to the account, is derived from organizational information such as the organizational hierarchy. The account administrator has permissions granted based on the source information, and can perform the corresponding operations. Accordingly, the account administrator can update (change and delete) user permissions, which are user data.

The account administrator has the User Management permissions in the TOE.

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

(3) Storage administrator

Role: Manages storages by, for example, managing the resources in the storages.

Permissions: The storage administrator is allowed to specify resource settings, such as the settings for allocating volumes, in the storage installed by the system integrator. Accordingly, the storage administrator can access the permissions of users, which are user data, to determine the permissions granted to the storage administrator.

In the TOE, the storage administrator has permissions related to storage operations, including the View, Modify, and Execute permissions.

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

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, Release 3

Part 2: Security functional components, Version 3.1, Release 3

Part 3: Security assurance components, Version 3.1, Release 3

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 claims

No Protection Profile claims apply to this ST.

2.2.2. Package claims

The evaluation assurance level of the ST is EAL2 augmented with ALC_FLR.1.

3. Security problem definition

Described here are threats, assumptions, and organizational security policies.

3.1. Threats

3.1.1. Assets to be protected

Since the main purpose of the TOE is to allow storage administrators to acquire an authorized storage management environment by acquiring appropriate permissions through authentication, the following assets are protected by the TOE:

- Permissions

  Permissions are granted to accounts and stored in the ACL together with corresponding user IDs and security attributes.

- Banner information

  Text used by the warning banner function.

3.1.2. Threats

T.ILLEGAL_ACCESS (illegal connection)

From a management client, an illegal user might delete, modify, or reveal the permissions information managed by the TOE for the storage management software functions, or might delete or modify the banner information.

T.UNAUTHORISED_ACCESS (unauthorized access)

From a management client, an authenticated storage administrator or account administrator might delete, modify, or reveal the permissions information managed by the TOE, or delete or modify banner information by performing an unauthorized operation.

3.2. Assumptions

A.PHYSICAL (management of hardware)

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

A.NETWORKS (networks)

The internal network in the business server area housing the management network connected to the management server must be restricted to communication from storage management client terminals by means of a firewall.

A.ADMINISTRATORS (administrators)

The system integrator is trusted. Account administrators, storage administrators, and administrators of other servers, including application servers, do not perform malicious acts with regard to one another's work. Work includes the management of accounts and permissions of storage management software users, the management of storages, and the management of other servers.

A.SECURE_CHANNEL (communication security)

The network between the management server and management clients, on which the TOE and storage management software run, and the management clients, or between the TOE and the external authentication server and the external authorization server that the TOE uses is secure with regard to confidentiality and integrity of communication.

A.VERSION (product versions that can be used with the TOE)

The TOE is to be used in combination with any of the following products:

HDvM version 5.6.0 or later

HTSM version 5.5.0 or later

HRpM version 5.6.0 or later

HTnM version 7.0.0 or later

A.PASSWORD (complex passwords)

Any passwords that are set must be difficult to guess on the basis of password length and character types used in order to prevent unauthorized users from logging in to the system through guesswork. In addition, a function that limits the number of repeated authentication attempts must be used to prevent unlimited authentication attempts.

A.CLIENTS (management of storage management clients)

Harmful software does not exist in the storage management client.

A.SRV_MGMT (server management)

The settings of services that run on the server, server settings, and accounts registered on the server must be managed to prevent management clients from directly accessing the internal network without using the TOE.

3.3. Organizational security policies

P.BANNER (warning banner)

Storage management software must have functions that display advisory warning messages related to its illegal use of the software.

4. Security Objectives

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

4.1. Security Objectives for the TOE

O.I&A

The TOE must identify and authenticate storage management client terminal users for which internal authentication is specified, so that only authorized users are able to access the permissions information managed by the TOE for the storage management software functions. If authentication of a user for which internal authentication has been specified fails more than 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 setting the authentication method, the permissions information, and the banner information for each user, and must control access so that only users of storage management client terminals who have the appropriate permissions can use the methods.

O.BANNER

The TOE must provide the storage management software with advisory warning messages about illegal use of the storage management software.

O.PASSWORD

The TOE must limit the registration patterns of the passwords of users for which internal authentication is specified in accordance with the set security parameter values.

4.2. Security Objectives for the operational environment

4.2.1. Security Objectives for the IT environment

OE.SECURE_CHANNEL

The network between the management server on which the TOE and the storage management software run and management clients, and the network between the external authentication server/external authorization server that the TOE uses and the TOE must maintain the confidentiality and integrity of communications.

OE.BANNER

The storage management software shall have functionality that displays advisory messages

(provided by the TOE) regarding illegal use.

OE.I&A

An external authentication server must identify and authenticate users for which external authentication is specified.

OE.PASSWORD

An external authentication server, for users for which external authentication is specified, must set passwords that are difficult to guess on the basis of password length and character types in accordance with the set security parameter values.

4.2.2. Security Objectives achieved during operations

OM.PHYSICAL

The management server on which the TOE and storage management software run, peripheral devices, the external authentication server and external authorization server that the TOE uses, storage devices, the internal network, and the firewall at the boundary of the internal network must be installed in a physically isolated business server area. Entry to and exit from the business server area must be controlled to permit only the administrators of the hardware and software in that area to enter the 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 where the management network is connected to the management server and the external network. The firewall must be configured to limit communication to the internal network from storage management client terminals to prevent unnecessary communication from the external network from entering the networks within the business server area.

OM.ADMINISTRATORS

The head of the organization shall select appropriate personnel to guarantee that the system integrator can be trusted and that account administrators, storage administrators, and administrators of other servers, including application servers, shall not perform malicious acts with regard to one another's work. Work includes the management of the accounts and permissions of storage management software users, the management of storages, and the management of other servers.

OM.TOE_ACCOUNT

The system integrator, account administrators, and storage administrators must not reveal the passwords that they create for the users of the storage management software. Passwords that are set must be difficult to guess on the basis of password length and character types used, and the passwords must be changed at an appropriate interval.

OM.VERSION

The system integrator must establish an environment that uses a combination of the TOE and any of the following products:

HDvM version 5.6.0 or later

HTSM version 5.5.0 or later

HRpM version 5.6.0 or later

HTnM version 7.0.0 or later

OM.PASSWORD

The system integrator and account administrators must set passwords that are difficult to guess on the basis of password length and character types used, and must limit the number of repeated authentication attempts to prevent unauthorized users from logging in to the system through guesswork.

OM.CLIENTS

The system integrator, the account administrators, and storage administrators monitor the client terminal so that harmful software is not installed to the client terminals that are used to access storage management software.

OM.SRV_MGMT

The settings of services that run on the server, server settings, and the accounts registered on the server must be managed to prevent management clients from directly accessing the internal network without using the TOE.

4.3. Security Objectives Rationale

The security objectives counter the threats specified in the TOE security environment, and satisfy the assumptions and organizational security policies. **Table 2** describes the correspondence between the security objectives and the threats that need to be countered, and the assumptions and organizational security policies that need to be satisfied.

Table 2: Correspondence among security objectives, assumptions, threats, and organizational security policies

Security problem definition / Security objectives	A.PHYSICAL	A.NETWORKS	A.ADMINISTROTORS	A.SECURE_CHANNEL	A.VERSION	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		
OE.SECURE_CHANNEL				X							
OE.BANNER											X
OE.I&A									X		
OE.PASSWORD									X		
OM.PHYSICAL	X										
OM.FIREWALL		X									
OM.ADMINISTROTORS			X								
OM.TOE_ACCOUNT									X		
OM.VERSION					X						
OM.PASSWORD						X					
OM.CLIENTS							X				
OM.SRV_MGMT								X			

As shown in **Table 2**, each security objective corresponds to at least one assumption, threat, or organizational security policy.

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

(1) Threats

T.ILLEGAL_ACCESS (illegal connection)

O.I&A, **O.MGMT**, and **OE.I&A** ensure that users of storage management client terminals who attempt to access the TOE and storage management software are identified, authenticated, and verified as authorized users. At this point, the TOE identifies and authenticates those users for which internal authentication is specified by means of a user possessing the appropriate permissions, and the external authentication server identifies and authenticates those users for which external authentication is specified. **O.PASSWORD** and **OE.PASSWORD** ensure that the TOE and the external authentication server limit the registration patterns of passwords so that difficult-to-guess passwords are set. **OM.TOE_ACCOUNT** ensures that users set passwords that are difficult to guess on the basis of password length and character types used and change them at an appropriate interval, and that passwords are not revealed. This process achieves safe password management. In addition, **O.I&A** ensures that the TOE automatically locks the account of a user for which authentication fails more than 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**, **OE.I&A**, **OE.PASSWORD**, 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 storage management software and TOE users.

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

(2) Assumptions

A.PHYSICAL (hardware management)

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

A.PHYSICAL is therefore satisfied by **OM.PHYSICAL**.

A.NETWORKS (networks)

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

A.NETWORKS is therefore satisfied by **OM.FIREWALL**.

A.ADMINISTRATORS (administrators)

OM.ADMINISTRATORS ensures that those with highest level of responsibility in an organization select appropriate personnel for the system integrator, account administrators, storage administrators, and administrators of other servers, including business servers. Therefore, the system integrator is a trusted person. Also, account administrators, storage administrators, and the administrators of other servers, including business servers, do not perform malicious acts regarding one another's work. Work includes the management of the accounts and permissions of storage management software users, the management of storages, and the management of other servers.

A.ADMINISTRATORS is therefore upheld by **OM.ADMINISTRATORS**.

A.SECURE_CHANNEL (communication security)

OE.SECURE_CHANNEL ensures that the network between the management server and management clients, or the network between the management server and external authentication servers uses communication paths protected by encryption or other methods to ensure the confidentiality and integrity of communication.

A.SECURE_CHANNEL is therefore upheld by **OE.SECURE_CHANNEL**.

A.VERSION (product versions that can be used with the TOE)

OM.VERSION ensures that the system integrator establishes an environment that combines the TOE and the versions of products that can be used.

A.VERSION is therefore satisfied by **OM.VERSION**.

A.PASSWORD (complex passwords)

OM.PASSWORD ensures that administrators set passwords that are difficult to guess on the basis of password length and character types used and that they set a limit on the number of repeated authentication attempts in order to prevent unauthorized users from logging in to the system through guesswork.

A.PASSWORD is therefore satisfied by **OM.PASSWORD**.

A.CLIENTS (management of storage client)

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

A.CLIENTS is therefore satisfied by **OM.CLIENTS**.

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

OM. SRV_MGMT ensures that the settings of services that run on the server, server settings, and the accounts registered on the server are managed to prevent management clients from directly accessing the internal network without using the TOE.

A.SRV_MGMT is therefore satisfied by **OM. SRV_MGMT**.

(3) Organizational security policies

P.BANNER (warning banner)

O.BANNER ensures that the TOE provides the storage management software with advisory warning messages regarding illegal use of the storage management software. **OE.BANNER** ensures that the storage management software has functionality for displaying advisory messages (provided by the TOE) about the illegal use of the storage management software.

P.BANNER is therefore satisfied by **O.BANNER** and **OE.BANNER**.

5. Extended Component 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: ACL table and banner information file

operations: Viewing, modification, creation, or deletion

[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]

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	Access control SFP
Subject: Process acting on behalf of the user of the storage management client terminal Object: ACL table Subject attributes: User ID and role associated with the subject Object attribute: User ID of the object	ACL access control SFP
Subject: Process acting on behalf of the user of the storage management client terminal Object: Banner information file Subject attributes: User ID and role associated with the subject Object attribute: None	ACL access control SFP

[assignment: rules governing access among controlled subjects and controlled objects through controlled 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 the user of the storage management client terminal	ACL table	The process is able to view the user's permissions information only when the user ID associated with the subject matches the user ID of the object.
Process acting on behalf of the user of the storage management client terminal	ACL table	When the role associated with the subject is account administrator or system integrator, the process can create, delete, or modify a user's permissions information.
Process acting on behalf of the user of the storage management client terminal	Banner information file	When the role associated with the subject is account administrator or system integrator, the process can create, delete, or modify the banner information.

[assignment: rules, based on security attributes, that explicitly authorize access to objects by

subjects]

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

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

Subject	Object	Rules, based on security attributes, that explicitly deny access of subjects to objects
Process acting on behalf of the user of the storage management client terminal	ACL table	Even if the role associated with the subject is account administrator, the process cannot delete or modify a user's permissions information.
Process acting on behalf of the user of the storage management client terminal	ACL table	If the object is permissions information corresponding to the system integrator, the process cannot delete or modify the permissions information.

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, information flow control SFP*]
User ID associated with the object (other than the system integrator, and subject user IDs)	Selection: delete Assignment: none	Account administrator, system integrator	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 described above.

[*assignment: list of TSF data*]	[selection: *change_default, query, modify, delete, clear, [*assignment: *other operations]*]	[assignment: *the authorized identified roles*]
User ID other than the system integrator user ID	Selection: delete Assignment: register	System integrator, or an account administrator whose user ID is not to be deleted or registered
Password associated with a user ID other than the system integrator, user ID	Selection: modify Assignment: register	Account administrator System integrator
	Selection: modify	Storage administrator whose user ID is to be modified
Password associated with the system integrator	Selection: modify	Account administrator System integrator
Lock status of the storage administrator	Selection: query, modify	Account administrator System integrator
Lock status of the system integrator	Selection: query, modify	Account administrator

Lock status of the account administrator	Selection: query, modify	System integrator,, or an account administrator whose user ID is not to be queried or modified
Security parameter	Selection: query, modify, clear	Account administrator System integrator
Value selected for external authentication or internal authentication	Selection: change _default, query, modify	Account administrator System integrator

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 described above.

Table 3: List of management functions to be provided by the TSF

Functional requirement	Management requirement	Management item
FDP_ACC.1	None	None
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	a) Management of user IDs and associated permissions
FMT_MSA.1	a) Management of role groups that can affect or be affected by the security attributes b) Management of the rules for inheritance by security attributes of particular values	a) None (there are no role groups that can affect or be affected by security attributes) b) None (there are no rules regarding the inheritance of particular values)

FMT_MSA.3	a) Managing the rule groups that can specify initial values b) Management of the permissive and restrictive setting of the default values for a given access control SFP c) Management of the rules for inheritance by security attributes of particular values	a) None (there are no such role groups) b) None (there is no management of default value settings) c) None (there are no rules regarding the inheritance of particular values)
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	a) None (no groups of roles that may affect TSF data that may affect roles exist)
FMT_SMR.1	a) Management of user groups that are part of a role	a) None (there are no user groups that are part of a role)
FIA_UAU.1	a) Management of the authentication data by an administrator; b) Management of the authentication data by the associated user; c) Managing the list of actions that can be taken before the user is authenticated.	a) Creation and change of passwords b) Change of passwords by users c) None (lists are not changed)
FIA_UID.1	a) The management of the user identities; b) If an authorised administrator can change the actions allowed before identification, the managing of the action lists.	a) Creation and deletion of user IDs for accounts b) None (lists are not changed)
FIA_SOS.1	a) The management of the metric used to verify the secrets.	a) Specification of the required number of characters and types of characters in passwords when passwords are set

FIA_ATD.1	a) If so indicated in the assignment, the authorized administrator is able to define additional security attributes for users.	a) None (no additional security attributes are defined)
FIA_USB.1	a) An authorized administrator can define the default security attributes of the subject. b) An authorized administrator can change the security attributes of the subject.	a) None (no security attributes are assigned by default) b) None (security attributes cannot be changed)
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts b) Management of the actions to be taken in the event of an authentication failure	a) Setting and modification of threshold values by administrators b) None (the only action to be performed is account locking)
FTA_TAB.1	a) Maintenance of banners by the authorized administrator	a) Setting of the banner contents by the administrator

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 [refienment: *user*].

[assignment: *list of TSF mediated actions*]

Warning banner function

[refinement: *user*]

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

[refinement: *each user*]

each user of a storage management client terminal for which the 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

[refinement: *user*]

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]

Password generation condition written in a security parameter (when the internal TOE authentication function is used)

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, 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, 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 Role: Storage administrator
Account administrator	Process acting on behalf of the account administrator	User ID: Authenticated user ID Role: Role associated with the user ID when registered
Storage administrator	Process acting on behalf of the storage administrator	User ID: Authenticated user ID Role: Role associated with the user ID when registered

[assignment: rules for the 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*]

Authenticated account of the user after the last successful authentication (except when 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 *[assignment: range of acceptable values]*

[assignment: range of acceptable values]

the range of values specified in security parameters

[selection: *met, surpassed*]

met

[assignment: *list of actions*]

lock the account (except for when you use the external authentication function).

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 the assurance requirement components are directly derived from the assurance components specified in CC Part 3. **Table 4** lists the assurance components with EAL2 augmented (EAL2+ALC_FLR.1).

Table 4: Assurance components with EAL2 augmented (EAL2 + ALC_FLR.1)

Assurance Class	Assurance components	
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 that will be used are specified in CC Part 2.

6.3.1. Security functional requirements rationale

Table 5 describes the relation between the security functional requirements selected for the TOE and the TOE security objectives.

Table 5: 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 5**, 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 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 and the storage management software, the TOE uses **FIA_UID.1** to check whether the user is authorized and uses **FIA_UAU.1** to identify the user. At this time, the TOE uses **FIA_AFL.1** for this user to lock the user's account if authentication attempts by the user repeatedly fail the predefined number of times. 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 the role of the 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 is therefore achieved with **FIA_UAU.1**, **FIA_UID.1**, **FIA_ATD.1**, **FIA_AFL.1**, **FIA_USB.1**, and **FMT_MTD.1**.

O.MGMT

The TOE uses **FMT_MSA.1** to allow only account administrators and the system integrator to manage user IDs, which are the security attributes of the ACL table. The TOE also uses **FMT_MSA.3** to provide, as restrictive initial values, the user IDs specified when permissions information was created.

The TOE also uses **FMT_MTD.1** to allow only account administrators and the system integrator to manage the authentication method (selection of internal authentication or external authentication) and users' security parameters.

When the TOE acquires the role (permissions information) of a successfully authenticated user of a storage management client terminal from the ACL table, the TOE uses **FDP_ACC.1** and **FDP_ACF.1** to control access to the ACL table based on the user's user ID. If the user performs operations on the ACL table and banner information file, the TOE also uses **FDP_ACC.1** and **FDP_ACF.1** to control access to the ACL table and banner information file based on the user's user ID and the role (permissions information) determined through the access control described above.

The TOE uses **FMT_SMR.1** to maintain the storage administrator, account administrator, and system integrator roles.

The TOE uses **FMT_SMF.1** to enable execution of the management functions indicated by the management items.

O.MGMT is therefore achieved with **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 provide the storage management software with an advisory warning message regarding illegal use of the storage management software. At this time, 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 is therefore achieved with **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

who use internal authentication.

O.PASSWORD is therefore achieved with **FIA_SOS.1**.

6.3.2. Security functional requirement dependencies

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

Table 6: 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 with ALC_FLR.1.

The users assumed by this TOE are storage administrators. Their number is limited, and each is registered. Therefore, intent to attack is suppressed. 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.

Recently, finding means to handle problems related to security vulnerability has become important. This product plays an important part in managing storages, and is required 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, ALC_FLR.1 is selected.

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 storage management software and the TOE, **SF.I&A** identifies and authenticates the user. In response to a request from the storage management software, **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

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

If the user 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 (permissions information). At this point, **SF.I&A** controls access to the ACL table (object) based on the user ID associated with the process (subject) acting on behalf of the user and the following rule:

- The role (permissions information) of the user is able to be acquired only when the user ID associated with the subject matches a user ID in the object.

When the acquired role (permissions information) contains the role (permissions information) necessary for using the storage management software, **SF.I&A** proceeds to the session management described in (3) below.

When **SF.I&A** is unable to identify or authenticate a user, or when the user account is locked, or when the acquired role and permission do not allow the use of the target storage management software, **SF.I&A** returns an error to the storage management software.

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**).

The TOE guarantees that the **SF.I&A** operation is always performed when it accepts a request

from the storage management software to identify and authenticate a user.

SF.I&A guarantees that the access control described above is always performed when the process acting on behalf of the user accesses the ACL table.

(2) Automatically locking accounts

When the TOE internal authentication function is used to identify and authenticate a user who logs in to the storage management software, **SF.I&A** automatically locks the account of the user if the user's authentication attempts repeatedly fail the preset number of times. When locked, the account is locked indefinitely. **SF.MGMT** unlocks a user account and sets a threshold for number of consecutive authentication failures 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 cleared 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. When an account is automatically locked, if another session with the same account has already logged in to the storage management software, automatic locking of the account does not affect the successfully authenticated session.

(3) Managing sessions

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

When the storage management software 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.

When the storage management software issues a login authentication request for a new user, **SF.I&A** generates and identifies a session for the login user. If a login authentication request is issued for a user already logged in, **SF.I&A** generates and identifies a new session for the user. That is, because **SF.I&A** generates a separate session for each login by a user, if the same user logs in several times, **SF.I&A** generates and identifies a session for each of the times the user logs in. Next, in response to a request from the storage management software, **SF.I&A** returns the user ID and role (permissions information) associated with the user that has successfully logged in.

After a session for a user who has successfully logged on to the storage management software is established, **SF.I&A** checks the session data to confirm the validity of the user session.

If **SF.I&A** determines that the user session is valid, **SF.I&A** returns the user ID, role, and permission of the user in response to the request from storage management software.

If **SF.I&A** determines that the user session is not valid, **SF.I&A** returns an error to the storage management software or another TOE security function.

Even if **SF.MGMT** has changed permissions information in the ACL table for a user while the user is logged in, **SF.I&A** does not change the permissions information in the session data for that user. Accordingly, the permissions information used when the user logged in remains in effect as long as the user is logged in to the storage management software and until the user logs out.

When **SF.I&A** receives a logout request from a user, **SF.I&A** deletes the information related to the user session from the session data and ends the session.

The user ID and role (permissions information) associated with each process that acts on behalf of a user who has successfully logged in cannot be changed by an access from any other process. Therefore, **SF.I&A** guarantees that the user IDs and roles described above are not changed by untrusted processes that do not operate on behalf of users who are successfully logged in.

7.2. Security information management function (SF.MGMT)

SF.MGMT manages the authentication method, account information, ACL table, banner information, and security parameters for each user. Before **SF.MGMT** can be used, the role (permissions information) of a user who wants to use **SF.MGMT** must be assigned.

(1) Managing accounts

SF.MGMT manages the correspondence among 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 of, querying, or modifying the selected value for external or internal authentication.

SF.MGMT permits 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 a password is registered or changed. **SF.MGMT** does not allow a password that does not satisfy the quality criteria to be set.

- The number of characters in a password must meet a minimum number of characters, which is set in a security parameter.
- The types of characters that can be used in passwords must be alphabetic and numeric characters and symbols, and the password complexity conditions set in security parameters must be met.

(3) Managing the ACL

SF.MGMT manages the correspondence among the user ID, role, and permission for each user account as the ACL. In response to a request from a user, **SF.MGMT** accesses the ACL table and provides methods for registering, modifying, or deleting permissions 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 access to the ACL table (object) based on the user ID and role associated with the process (subject) and the following rules:

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

  Note that the user ID must be specified when permissions information is created, and the correspondence between them begins as soon as the permissions information is created.

  The account administrator and system integrator can specify a user ID and delete the corresponding permissions information. They can also delete permissions information by deleting the corresponding user ID (account).
- Even when the role associated with the subject is account administrator, **SF.MGMT** does not allow the process to delete or modify permissions information for the user ID associated with the subject.
- When the object is permissions information for the system integrator (System), **SF.MGMT** does not allow any user to delete or modify the permissions information.

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

Only authorized processes can access the information in the ACL table. Accordingly, **SF.MGMT** guarantees 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 the automatic locking of accounts and the complexity checking of passwords. **Table 7 エラー! 参照元が見つかりません。** lists the security parameters. In response to a request from a user, **SF.MGMT** provides methods for querying, modifying, and clearing the parameters.

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

Table 7: Security parameters

#	Parameter	Description
1	Threshold value for the number of consecutive authentication attempt failures	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	Minimum number of characters in a password
3	Password complexity condition	Condition specifying that the specified number of the specified types of characters must be included in a password

(5) Managing banner information

SF.MGMT manages advisory warning messages regarding illegal use of storage management software as banner information. In response to a request from a user, **SF.MGMT** accesses the banner information file and provides operations for generating, deleting, and changing 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 access to the banner information file (object) based on the user ID and role associated with the process (subject) and the following rule:

- When the role associated with the subject is account administrator or system integrator, banner information can be generated, deleted, or changed.

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

Only processes that are authorized to use the function for editing banner information files can access banner information. Accordingly, **SF.MGMT** guarantees that banner information can only be changed by processes acting on behalf of the users who have been successfully identified and authenticated, and not by untrusted processes.

7.3. Warning banner function (SF.BANNER)

SF.BANNER returns banner information that is set by **SF.MGMT** in response to a request from the storage management software. At this time, **SF.BANNER** controls access so that viewing of banner information is always allowed. The banner information contains the text of an advisory warning message regarding illegal use of the storage management software. The storage management software displays the warning message returned as described above in the login window used for identifying and authenticating the user of the storage management client terminal.

SF.BANNER guarantees that the access control described above is always performed.

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 8**, the security functions described in this section satisfy the TOE security functional requirements described in subsection 5.1.1.

Table 8: Relation between TOE security functions and TOE security functional requirements

TOE security functional requirement / TOE security function	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	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 (subject) that identifies and authenticates a user on behalf of the user reads the ACL table (object) to obtain the role and permission granted to the user, the TOE uses **SF.I&A** to control access to the object based on the user ID associated with the subject and the user ID in the object.

When the process (subject) that acts on behalf of a user reads, changes, creates, or deletes the ACL table or the banner information file (object), the TOE uses **SF.MGMT** to control access to the object based on the user ID and the role associated with the subject and the user ID in the object.

When the process (subject) that acts on behalf of a user reads the banner information file (object) to acquire a warning message, the TOE uses **SF.BANNER** to control access to permit only read accesses.

FDP_ACC.1 and **FDP_ACF.1** are therefore achieved for **SF.I&A**, **SF.MGMT**, and **SF.BANNER**.

FMT_MSA.1:

The TOE uses **SF.MGMT** to allow only account administrators and the system integrator to change and delete the user ID and role that are associated with the object (ACL table) and that are security attributes. However, account administrators are not allowed to change their own role and the role for the system integrator account.

FMT_MSA.1 is therefore achieved for **SF.MGMT**.

FMT_MSA.3:

When permissions information is created, the TOE uses **SF.MGMT** to provide, as the restrictive initial values of the user IDs that are security attributes of the ACL table, the user IDs of the users to which the permissions information is to be assigned.

FMT_MSA.3 is therefore achieved for **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 and security parameters of each user. 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 the lock status, and to query, change, and clear security parameters, and to query, change, and modify the default value of the internal or external authentication selection value.

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

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

FMT_MTD.1 is therefore achieved for **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 that are to be managed by the TOE (**Table 3**:) as described in section 7.2.

FMT_SMF.1 is therefore achieved for **SF.MGMT**.

FMT_SMR.1:
The TOE uses **SF.MGMT** to maintain roles associated with users as permissions information in the ACL table in order to manage the roles of storage administrator, account administrator, and system integrator.
FMT_SMF.1 is therefore achieved for **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 which internal authentication is specified, the TOE does not perform any operation except for sending a warning message provided by the warning banner function (**SF.BANNER**).
FIA_UAU.1 and **FIA_UID.1** are therefore achieved for **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 satisfies the minimum number of characters required in a password as determined in a security parameter.
- The types of characters allowed in a password are alphanumeric characters and symbols, and the complex password condition determined by a security parameter is satisfied.

FIA_SOS.1 is therefore achieved for **SF.MGMT**.

FIA_ATD.1, FIA_USB.1:
The TOE uses **SF.I&A** to maintain and manage the user IDs and roles (permissions information) of users, and to associate the user ID and role (permissions information) of a user of a storage management client terminal who has been successfully identified and authenticated with the process acting on behalf of that user.
FIA_ATD.1 is therefore achieved for **SF.I&A**.

FIA_AFL.1:
When the TOE authenticates a user for which internal authentication is specified, the TOE uses **SF.I&A** to lock the account of a user whose authentication attempts have repeatedly failed the predefined number of times.
FIA_AFL.1 is therefore achieved for **SF.I&A**.

FTA_TAB.1:

The TOE uses **SF.BANNER** to send an advisory warning message regarding illegal use of storage management software to the storage management software, and the storage management software displays the warning message in the login window used to identify and authenticate users.

FTA_TAB.1 is therefore achieved for **SF.BANNER**.

8. Terms

Table 9 describes the terms and abbreviations used in this ST.

Table 9: Meaning of terms and abbreviations

Term	Meaning
SAN	Abbreviation for Storage Area Network.
Permissions (permissions information)	Indicates the type of operation that the TOE allows storage management software to perform. Permissions include User Management permissions for managing user information, View permissions for viewing storage, Modify permissions for modifying storage, and Execute permissions for executing tasks. Each user is assigned a permission or a combination of permissions as permissions information.
ACL table	Table used for managing permissions information for account and storage management.
HSCC	Hitachi Command Suite Common Component. HSCC is a part of Hitachi Command Suite, and 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.
HRpM	Hitachi Replication Manager Software (formerly HiCommand Replication Monitor). HRpM is storage management software. It is part of Hitachi Command Suite, and provides functionality for managing the copying between volumes in storage.
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.
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 are used.

Security parameter	Parameter information related to HSCC security functions. Parameter information includes such information as number and type of characters permitted in passwords; 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 use storage management software. A warning banner is mainly used to call attention to the possibility of illegal use.
Internal authentication	An authentication method that uses only the TOE internal authentication function. This is the same authentication method that is used in HSCC 6.0.0-01.
External authentication	Authentication method that uses an external authentication server (LDAP directory server, RADIUS server, or Kerberos server) external to the TOE 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 the group, and then passes permissions information to the TOE. Because this function requires authentication functionality external to the TOE and the accounts belong to a group, this function is called *external authentication group linkage*.