HITACHI
DATA SYSTEMS

Hitachi TagmaStore®
Adaptable Modular Storage
and Workgroup Modular Storage
Account Authentication User's Guide

MK-96DF797-00

Trademarks

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

TagmaStore is a registered trademark of Hitachi Data Systems Corporation.

Linux is a registered trademark of Linus Torvalds.

Windows and Windows NT are registered trademarks, and Windows Server is a trademark of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

All other brand or product names are or may be trademarks or service marks of and are used to identify products or services of their respective owners.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-96DF797-00	May 2007	Initial Release

Source Documents for this Revision

Hitachi TagmaStore™ Adaptable Modular Storage Account Authentication User's Guide, RSD-96DF797-00, 09/25/06

Preface

Before using Account Authentication, read the operating procedures and notices included in this guide.

The Account Authentication *User's Guide* assumes that:

- The user has a background in data processing and understands direct-access storage device subsystems and their basic functions.
- The user is familiar with the Hitachi Disk array subsystem.
- The user is familiar with the *Storage Navigator Modular (for GUI) User's Guide*.

Software Version

This document revision applies to Hitachi TagmaStore™ Adaptable Modular Storage products version 6.0 and higher.

Convention for Storage Capacity Values

Storage capacity values for logical units (LUs) on the AMS/WMS are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes

1 MB (megabyte) = $1{,}024^2$ bytes

1 GB (gigabyte) = $1{,}024^3$ bytes

1 TB (terabyte) = $1{,}024^4$ bytes

Storage capacity values for hard disk drives (HDDs) on the AMS/WMS are calculated based on the following values:

1 KB (kilobyte) = 1,000 bytes

1 MB (megabyte) = $1{,}000^2$ bytes

1 GB (gigabyte) = $1{,}000^3$ bytes

1 TB (terabyte) = $1{,}000^4$ bytes

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

E-mail: doc.comments@hds.com

Fax: 858-695-1186

- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

List of Figures

List of Tables

Chapter 1 Overview of Account Authentication

This chapter discusses storage security concepts and business requirements. It also provides an overview of Hitachi's Account Authentication feature, which addresses these security requirements. This chapter includes the following sections:

- Storage Security (section 1.1)
- Hitachi's Security Solutions (section 1.2)
- Overview of Account Authentication (section 1.3)
- Account Authentication Management Software (section 1.4)

1.1 Storage Security

Storage security had long been an overlooked area of IT investment. However, storage subsystems have evolved to support strong security features that preserve data integrity and protect system access. Until recently, most organizations focused their spending on other information security technologies and relied on host-based security services to protect data in storage servers. However government regulations, such as the Sarbanes-Oxley Act of 2002, demand that organizations adopt formal audit processes and adhere to compliance standards for controlled role-based administration and transaction logging. Organizations are now held accountable for protecting data integrity and confidential data transfer.

In today's business environments, networked storage systems reside on insecure switched Fibre Channel or IP interfaces and are shared by multiple hosts. In spite of improvements in performance, storage utilization, and data availability resulting from storage becoming a networked service, critical business data in subsystems are exposed to many security threats and vulnerabilities. Disregarding storage security is no longer an acceptable alternative for businesses that move data between remote geographic locations. Adopting information lifecycle management (ILM) policies requires that information security must be guaranteed to meet the associated regulatory requirements.

All the above considerations have led to improved security features such as user account authentication, role-based access authorization, and audit logging in today's storage subsystems. The following critical business drivers have led to enhanced storage security features in today's storage products:

- Deter or eliminate theft of sensitive data by perpetrators
- Penalties associated with unauthorized disclosure of regulated data
- Prevent unauthorized modification of sensitive data that affects data integrity
- Avoid human errors that could result in accidental data corruption
- Establish better accountability for transactions through defined allocation of responsibilities and audit logging
- Demonstrate data authenticity at all times
- Need for detail procedures for verifying responsibilities for transactions
- Importance of ensuring business and service continuity as well as data availability
- Ability to demonstrate compliance to regulatory requirements and legal necessities

1.2 Hitachi's Security Solutions

Hitachi has long been a storage security pioneer providing an array of compliance-ready products with enhanced security capabilities, even before other competitors recognized this necessity. The company has always identified and included security requirements when designing storage solutions by reviewing and mapping current regulatory requirements to security frameworks like ISO 17799 and COSO. In keeping with the regulatory focus on accountability, Hitachi's new product offerings have been enhanced with security functionality such as authentication, authorization, and event logging. Security best practices have been implemented in product planning and development by adopting the ISO/IEC 21827:2002 Systems Security Engineering – Capability Maturity Model (SSE-CCM).

The company's dedication to storage security has resulted in the implementation of many notable security provisions such as the following:

- Separation of device management interfaces from storage data
- Secure password management, authentication, authorization, and auditing (AAA)
- Role-based access control to the subsystem resources
- Interoperability with existing authentication infrastructures based on standards such as RADIUS, Kerberos, and two-factor tokens and transaction-based logging standard Syslog
- Management platform support for SMI-S to enable secure communications between devices and management servers via SSL v3, and secure management of multiple storage domains
- IP-based secure remote management and support for secure communications using HTTPS over SSL
- Fibre Channel Security Protocol (FC-SP) compliance

By implementing data protection and security measures with features such as Account Authentication, Audit Logging, and Password Protection in its product line, the company has responded to multiple business drivers in addition to regulatory compliance.

1.3 Overview of Account Authentication

The Account Authentication function ensures the security of disk subsystems and authenticates system users using role-based accounts with predetermined authorizations. By restricting unauthorized access to subsystem resources, this function eliminates the risks associated with an illegal break-in to the subsystem via the management LAN interfaces. Figure 1.1 shows a typical Account Authentication scenario.

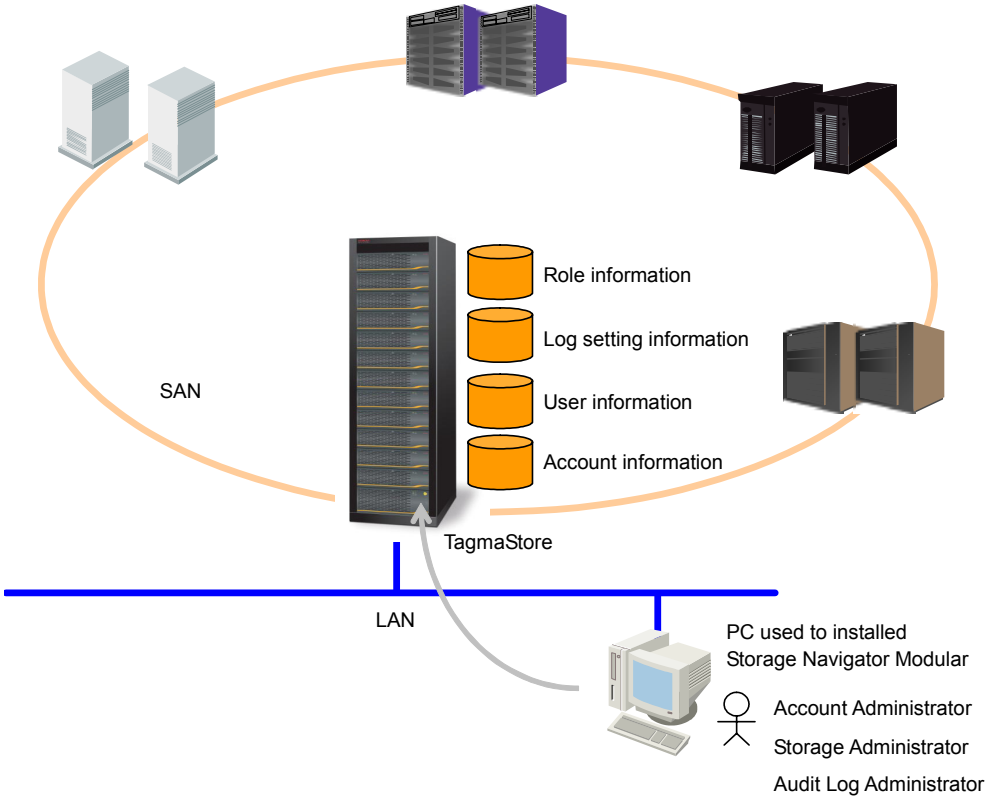


Figure 1.1 Account Authentication Outline

Every user requiring access to the disk subsystem is registered as an account by the User Management function. Account information includes a unique user ID, password, and role identification information. When a user logs in to the disk subsystem, the User Authentication function verifies the user's credentials. The users are permitted access and rights that are based upon their predetermined role-based authorizations. The Access Control function determines the role-based authorizations for each user. Specific users who are registered as administrative accounts with system management permissions can view and modify the disk subsystem resources. Other users can access disk subsystem resources within the range of their authority.

The Account Authentication feature provides the following benefits and protection:

- Secure management of user sessions by predetermined timeout capabilities
- Transaction traceability and accountability by interoperability with the Audit Logging function
- Role-based authorizations that prevent unauthorized access to sensitive data and subsystem resources

1.3.1 Account Authentication Feature Functions

Account Authentication is implemented with the following three functions:

- **User management function:** This function manages registration of user account information (user ID, password, role etc.) and provides the ability to change this information. Users with management and administration privileges are allowed to perform functions like creating or deleting accounts, allocating roles to other users, changing passwords, enabling and disabling accounts, etc.
- **User authentication function:** This function performs user (or account) authentication at the time of access (login) to the disk subsystem based on the previously registered account information. When a user logs in using a preregistered userid and password, this function validates the user information and creates a session for validated users by assigning an appropriate type of session ID.
- **Access control function:** This function controls access to the disk subsystem resources allowing users to view or modify resources based on their assigned roles and associated authorities.

Figure 1.2 shows the interoperability of the three account authentication functions

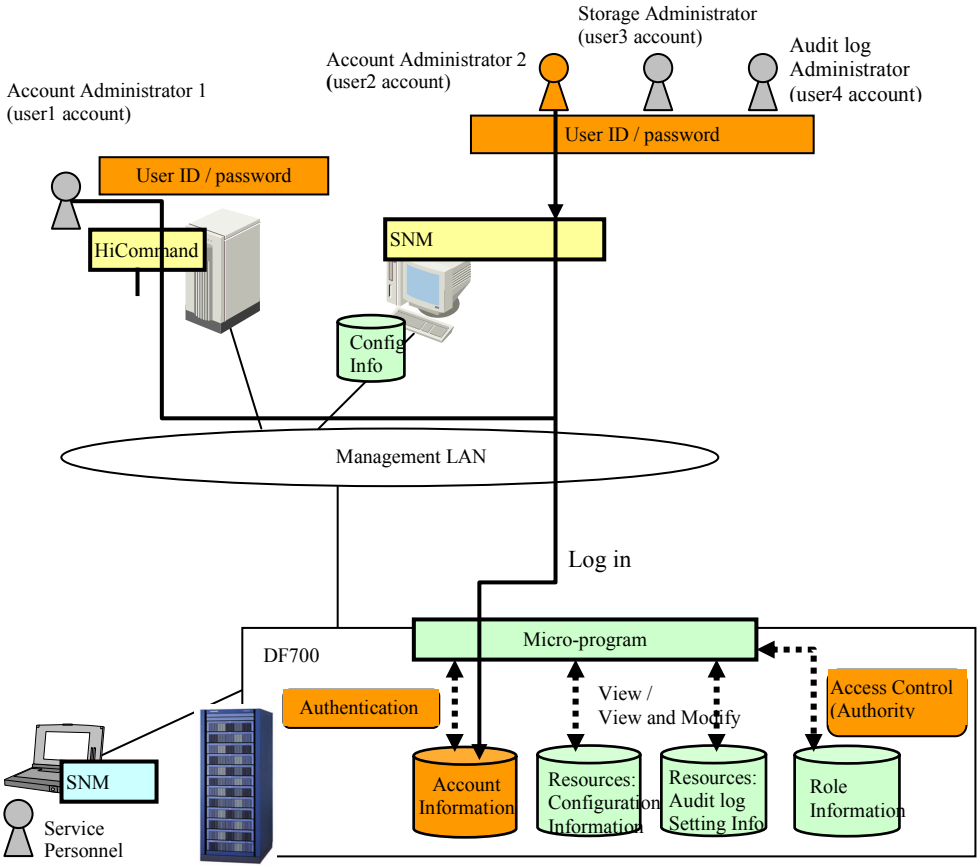


Figure 1.2 Account Authentication Functions

1.3.2 Differentiation from Password Protection Function

The Account Authentication feature is similar to the Password Protection feature but offers higher security capabilities and advanced protection for business data and configuration information.

The primary difference between the two security functions is that the Account Authentication feature allows role-based access control with the facility to create and manage multiple accounts using unique user IDs and passwords. The Password Protection feature supports user authentication with user ID and password. However, it assigns the same permissions to all users, and does not allow more than one user to be authenticated and logged in at any instant in time. Table 1.1 summarizes other differences between the two security features.

Table 1.1 Security Feature Differentiation

Item	Password Protection	Account Authentication
User authentication (with UserID, Password)	Supported (only one user can login at a time)	Supported (duplicated login is available)
Role Base Access Control (RBAC)(*1)	Not supported	Supported
Interaction with Audit Logging	Not supported	Supported (UserID that modified the setting is issued in Logged Data)
Limitation of effective time for login(session timeout function)	Not supported (Sessions continue endlessly if logout operation is not executed by the user.)	Supported (If 20 minutes elapses without any operation, the user account is logged out forcibly.)

(*1) The RBAC function assigns the management authorities to an account based on the user's role

Because the Account Authentication feature provides the capabilities of Password Protection and additional enhanced security functions, you cannot use both functions concurrently. Either of the features must be uninstalled or disabled before using the other.

To install or upgrade to the Account Authentication feature on a disk subsystem that already has the Password Protection feature installed, it is necessary to upgrade the microprogram to 0760/A or later. Then Password Protection must be uninstalled or disabled before Account Authentication is installed.

1.4 Account Authentication Management Software

The Account Authentication feature can be installed and enabled using Storage Navigator Modular management software.

The Account Authentication feature is used in HiCommand Products, for example, when adding a TagmaStore AMS/WMS storage subsystem via the Web Client of Device Manager. For more information about HiCommand products, see the HiCommand V5.5 or later documentation.

Chapter 2 Specifications and Authentication Entities

This chapter provides specifications and operational requirements for the Account Authentication feature. This chapter also describes the various functional entities used to implement the Account Authentication function. This chapter includes the following sections:

- Specifications (section 2.1)
- Accounts (section 2.2)
- Roles and Resources (section 2.3)
- Login Controls (section 2.4)

2.1 Specifications

Table 2.1 shows the Account Authentication specifications and required operating environment.

Table 2.1 Account Authentication Specifications

Items	Contents
Environment required	▪ Micro program: Version 0760/A or more is required for disk subsystem. ▪ Storage Navigator Modular (hereafter called Navigator): Version 6.00 or more is required for management PC.
Concurrent use of Password Protection	Not available
Concurrent use of NAS	Not available.
Account numbers that can be registered	Up to 20 accounts can be registered with the disk subsystem. (Navigator is used for the registration.)
Maximum login numbers	Up to 256 users can log in (including duplicate logins by the same user).
Session time-out	20 minutes (fixed). When 20 minutes elapses without any operation, the logged in user is forcibly logged out. (See Note 1 below.)
Assignable role numbers	Up to 6 roles can be assigned to an account.

Note 1: For information on sessions, see section 2.4.1.

Note on concurrent usage with NAS: Account Authentication cannot be simultaneously used with NAS. NAS options must be uninstalled and the NAS I/F must be detached from DF subsystems, before installing the Account Authentication feature.

Note on concurrent usage with Password Protection: Account Authentication cannot be simultaneously used with Password Protection. Password Protection must be uninstalled or disabled, before installing the Account Authentication feature.

2.2 Accounts

2.2.1 Definition of Accounts

Accounts are basic functional components used by the Account Authentication function to register user information on the disk subsystem. Each unique account includes a user ID, a password, a role identification number, and a flag for enabling or disabling the account. Every user that requires access to the disk subsystem must be registered as a unique role-based account. The disk subsystem authenticates individual users during login and controls access to view or modify the resources based on the predetermined role-based permissions. A maximum of up to 20 accounts can be registered within a disk subsystem. Storage Navigator Modular software is used to perform account registration.

Table 2.2 provides the specifications of all account authentication parameters recorded for each user.

Table 2.2 Account Specifications

Items	Contents	Specifications	Automatic Setting (by Micro Program)	Manual Setting (by Account Administrator
Account type	An identifier for the account type	Account type is set to: 1: Public account 2:Built-in account	Yes	No
User ID	An identifier for identifying the account concerned	Length: 1 to 256 Valid characters: ASCII code (0-9, A-Z, a-z, "! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~	No	Yes
Password	Authentication information for identifying the user account concerned	Length: 6 to 256, see Note 1. Valid characters: ASCII code (0-9, A-Z, a-z, "! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~	No	Yes (Initial setting only. Setting cannot be changed)
Role	A role to be assigned to the account concerned	Predefined role numbers: 1 to 6 For more details, see section 2.3.	No	Yes
Account Status	Information on enabling/disabling the authenticating function for the account concerned.	Account status: Enable or Disable. See Note 2	.No	Yes

Note 1: The password length should be a minimum of six characters.

Note 2: The default status of new accounts is "Disable".

2.2.2 Account Types

The Account Authentication function supports two categories of accounts:

- Built–in Accounts
- Public Accounts

Built-in accounts are accounts originally registered with the subsystem and used to initially login to the subsystem. The initial user ID, initial password, and initially assigned role of the built-in account are predetermined. **Public accounts** are optional accounts created by the user after installation of the Account Authentication function. If the *Public Account(Account Administrator (View and Modify))* is created by the *Built-in Account*, the *Public Account* can create another new Public Account.

Built-in accounts are meant to be used as *super user* accounts. Hence these accounts have some restrictions on configuration, operations and naming conventions. For example, the use of fixed user id *root*. Table 2.3 and Table 2.4 summarize the naming and configuration restrictions for both accounts

Table 2.3 Fixed Information for Account Types

Type	Initial User ID	Initial Password	Initial Assigned role	Contents
Built-in account	root (not changeable)	storage (changeable)	Account Administrator (View and Modify)	An account that has been registered with the Account Authentication function beforehand. Having more than one person use the root id will cause problems. To prevent loss of modification privileges, create a different user ID for managing Storage Navigator Modular.
Public account	Optional	Optional	Optional	An optional account that can be created after Account Authentication is installed.

Note on resetting passwords: It is recommended that the initial password on built-in accounts be changed after installation, because they are very predictable.

Note on retrieving lost passwords: It is necessary to manage built-in account passwords carefully. An account password cannot be reset to the initial password, if its password is lost.

Table 2.4 Configuration Restrictions for Account Types

Type	Deleting Account	Deleting Account Administrator Role	Invalidating Account
Built-in account	Not available	Not available	Not available
Public account	Available	Available	Available

2.3 Roles and Resources

This section describes additional functional entities used by the Account Authentication feature.

2.3.1 Definition of Roles

A role is a designated “part” that is assigned to the account when it is created. It defines the administrative authority assigned to the account, and determines the user’s rights or permissions to view, modify, or operate on each disk subsystem resource. For example, an account assigned the role of **Storage Administrator (View and Modify)** has the authority to view and modify the disk subsystem configuration. This designation allows the user to display and create an LU. However this designation does not have the authority to set up new accounts or modify audit log settings.

Role allocations can also be changed after the account is created. Some roles are preconfigured and used to perform common management operations such as installing and initiating account authentication operations.

Table 2.5 summarizes the supported role types and briefly explains their purpose.

Table 2.5 Role Type

Role Type	Contents	Usage
Storage Administrator (View and Modify)	Authority that enables a user to view and modify the resource, and perform storage configuration such as creation of RAID group and LU.	This is assigned to a user who manages the storage.
Storage Administrator (View Only)	Authority that enables a user to only view the resource such as RAID group and LU.	This is assigned to a user who views the storage information. Also automatically assigned to a user who cannot log in with the Storage Administrator (View and Modify) in the modify mode.
Account Administrator (View and Modify)	Authority that enables a user to view and modify the resource, and perform account operations such as creation, setting, and deletion.	This is assigned to a user who authenticates the account information.
Account Administrator (View Only)	Authority that enables a user to only view the resource of the account.	This is assigned to a user who views the account information. Also automatically assigned to a user who cannot log in as the Account Administrator (View and Modify) in the modify mode.
Audit Log Administrator (View and Modify)	Authority that enables a user to view and modify the resource, and perform audit log operations such as configuring settings for sending, etc.)	This is assigned to a user who manages the audit log function.
Audit Log Administrator (View Only)	Authority that enables a user to view the audit log resource. The internal output of Audit logging can execute by Audit Log Administrator (View only) too.	This is assigned to a user who views the audit log. Also automatically assigned to a user who cannot log in as the Audit Log Administrator (View and Modify) in the modify mode.

Note: It is strongly recommended that each account be assigned only a single role. This prevents the risks and dependencies associated with concentrating multiple role authorizations on a single user.

2.3.2 Resources

From the account authentication perspective, a resource refers to a classified repository of system information or a category of physical subsystem components, to which role-based authorities can be assigned. Role definitions are based upon permissions an account has on target resources. Resources are further consolidated into resource groups to facilitate simpler allocation of functional authorities.

Table 2.6 summarizes the various resource groups used by the Account Authentication function.

Table 2.6 Definition of Resource Groups

Resource Groups	Repositories	Contents
Storage management resource group	Role definition repository	A repository that stores information on the definition of the role, that is, what access right each role has concerning each resource (role type, resource, whether or not having the authority to operate)
	Key repository	A repository that stores information on the device authentication (an authentication name for the CHAP authentication of the iSCSI and the secret (a password))
	Storage resource repository	A repository that stores information for the storage management such as that on the hosts, switches, volumes, and ports and settings of functions concerning the storage management
Account management resource group	Account repository	A repository that stores information on a user ID, a password, etc. of each account
	Role mapping repository	A repository that stores information on the correspondence of each account to a role to be assigned to the account
	Account setting repository	A repository that stores information on a function concerning an account (a time limit until the session time-out, the minimum number of characters of a password, etc)
Audit log management resource group	Audit log setting repository	A repository for setting Audit Logging (IP address of the transfer destination log server, etc.)
	Audit log	A file that stores the audit log in the disk subsystem

Table 2.7 shows authorities of various roles in relation to available resource groups.

Table 2.7 Relation between Roles and Resource Groups

Resource Group Name	Role Definition	Key	Storage Resource	Account	Role Mapping	Account Setting	Audit Log Setting	Audit Log
Storage Administrator (View and Modify)	–	V/M	V/M	×	×	×	×	×
Storage Administrator (View Only)	–	V	V	×	×	×	×	×
Account Administrator (View and Modify)	–	×	×	V/M	V/M	V/M	×	×
Account Administrator (View Only)	–	×	×	V	V	V	×	×
Audit Log Administrator (View and Modify)	–	×	×	×	×	×	V/M	V
Audit Log Administrator (View Only)	–	×	×	×	×	×	V	V
Legend: V: View, M: Modify, V/M: View and modify, ×: Impossible of view and modify, –: Not available								

2.3.3 Operational Authority of Roles and Resources

Roles	Storage Administrator				Account Administrator						Audit Log Administrator			
Repositories	**Key**		**Storage Resource**		**Account**		**Role Mapping**		**Account Setting**		**Audit Log Setting**		**Audit Log**	
Resources	**V/M**	**V**	**V/M**	**V**	**V/M**	**V**	**V/M**	**V**	**V/M**	**V**	**V/M**	**V**	**V/M**	**V**
Setting of the license key														
Install			O								O			
Uninstall			O						O		O			
Enable/Disable			O						O		O			
Setting of the storage														
Setting up RAID group/LU Formatting the LU, etc			O	O										
Setting of an account														
Forced logout					O		O							
Adding account					O		O							
Modifying account					O		O							
Deleting account					O		O							
Changing owner password	O	O	O	O	O	O	O	O	O	O	O	O	O	O
Displaying account					O	O	O	O						
Setting of Audit log														
Initializing internal storing log													O	
Exporting internal storing log													O	O
Setting Syslog server											O	O		
Enable/Disable of internal log											O	O		
Legend: V/M: View and Modify, V: View Only, O: Available														

Note: When Account Authentication has been installed, the following restrictions are placed on the setting of the license key for each role.

- Storage Administrator can set the license keys other than Account Authentication and Audit Logging.
- Account Administrator can set the license key for Account Authentication only. However, it cannot install Account Authentication (because Account Authentication is not installed yet).
- Audit Log Administrator can set the license key for Audit Logging only.

2.4 Login Controls

2.4.1 Sessions

A session refers to the elapsed time period between the time the user logged in and logged out of the disk subsystem. A maximum of 256 sessions can be concurrently open on a single disk subsystem allowing up to 256 accounts to simultaneously use the same system. A single user may also open multiple sessions by duplicating logins.

Note on Session timeouts: Sessions are preconfigured to timeout after fixed periods of user inactivity. The default time interval after which a user session times out is fixed at 20 minutes. The user account is forcibly logged out if 20 minutes have elapsed since the last user operation.

Note: When a login is done with the built-in account, the login is always made on the condition of the session of the modify mode.

2.4.2 Session IDs

A Session ID is an internal ID issued by the subsystem to an application program from which the user completes a successful login. This internal ID is not available to the user.

2.4.2.1 Types of Session IDs

Session IDs can be of two different types, depending on the permitted operational mode:

- Modify mode
- View mode

Table 2.8 summarizes information about the types of Session IDs.

Table 2.8 Session ID Type

Type	Permitted Operation	Maximum Number of Session IDs
Modify mode	View and modify (setting) operations of the disk subsystem	3
View mode	View only of the disk subsystem setting information	256

The **Modify mode** is the default Session ID mode for sessions initiated during the first login from a *Public Account* (View and Modify) and for all logins from any *Built-in Account*.

The **View mode** is the default Session ID mode for sessions initiated by logins from a *Public Account* (View and Modify) that has previously logged in. Session IDs in this mode are also created when a *Public Account* (View and Modify) changes to *Public Account* (View) and when the *Built-in Account* logs in.

2.4.2.2 Deletion of Session IDs

Session IDs are deleted under the following circumstances:

- When a user logs out
- When a user is forced to logout
- When the session times out (see Note 1)
- When a planned shutdown is executed

The disk subsystem is not operational after Session IDs are deleted.

Note: If 20 minutes elapse without any operation, the session times out, and the user account is logged out forcibly.

2.4.3 Resource Operation Authorities

Transitions of resource operation authorities occur when different accounts log in to the disk subsystem. Authority transitions depend on the type of accounts logging in and also on similarities or dissimilarities in their role authorities. The changes to resource operational authorities are effective (valid) only in the particular session in which the transition occurs and are not permanent role changes for the concerned account.

When two or more Public accounts with **View and Modify** authority log in to the disk subsystem, a **Modify** mode Session ID is given to the account that logs in first. The account that logs in second is given a **View** mode session ID. The authority to operate the resource is transferred, even though the account retains its **View and Modify** role. Figure 2.1 illustrates the transition of authority for Public Accounts.

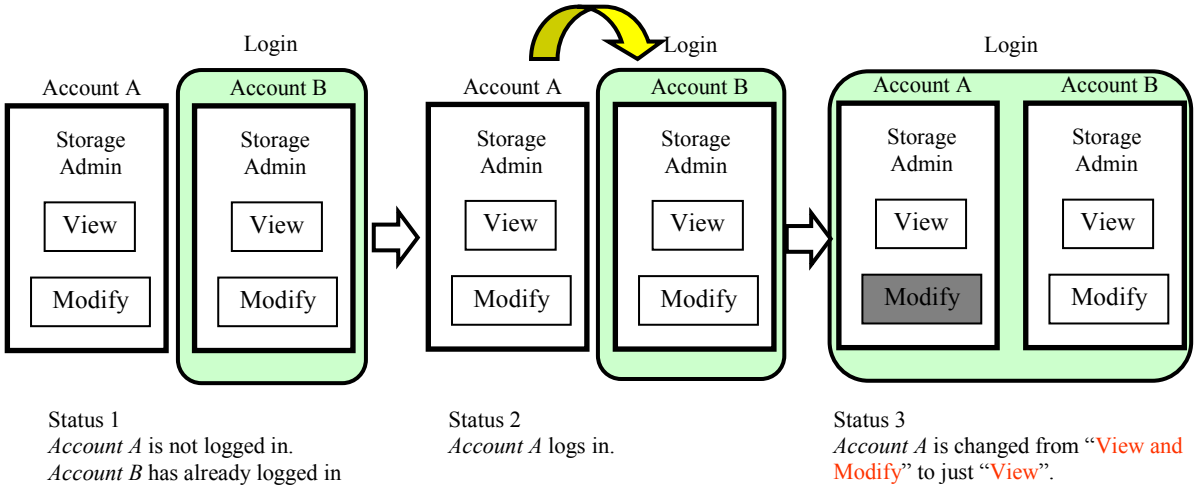


Figure 2.1 Transition of Authority for Public Accounts

Note 1: The Built-in Account has strong authority and a lot of attentions for other users are required to use Built-in Account. The user that is assigned the role of Account Administrator (View and Modify) or Account Administrator (View Only) can display the account information including which users have the MODIFICATION authority.

When any account with View and Modify authority logs in and there is no previously logged in account with the same View and Modify authority, a Modify mode Session ID is assigned to the most recently logged in account. A maximum of three such Modify mode Session IDs can be assigned simultaneously at any point in time. This allows the three predefined View and Modify roles (Storage Administrator, Account Administrator and Audit Log Administrator) to be logged in to the subsystem simultaneously.

Built-in Accounts always log in with **Modify** mode Session IDs. When a built-in account logs in, any previously logged in Public account with a **Modify** mode Session ID and having a **View and Modify** role (same as the Built-in account) is forced to be placed in the **View** mode. The **View and Modify** role assigned to the Built-in account always takes precedence over any previously logged in Public account with the same role authorization.

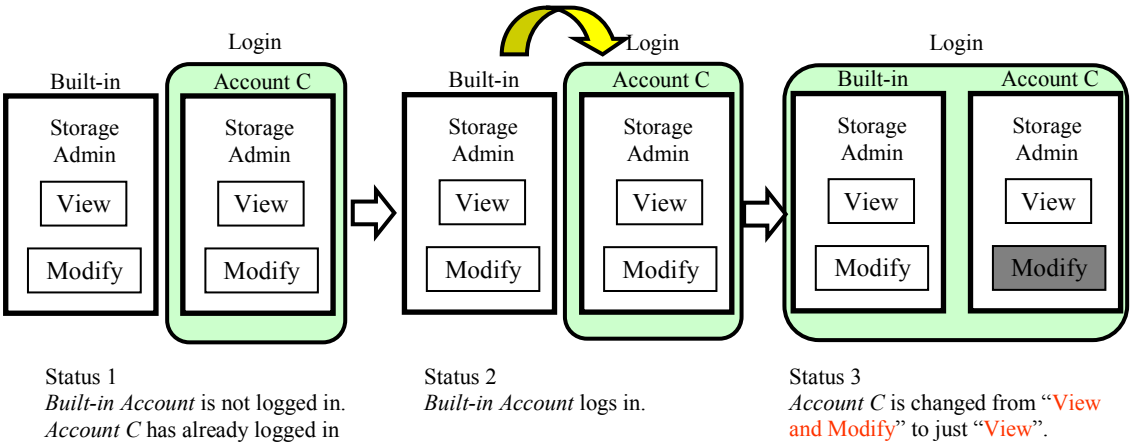


Figure 2.2 Transition of Authority for Built-in Accounts

Chapter 3 Preparing for Account Authentication Operations

This chapter provides instructions for installing, uninstalling , enabling and disabling the Account Authentication function using Storage Navigator Modular. This chapter includes the following sections:

- Installing (section 3.1)
- Uninstalling (section 3.2)
- Enabling or Disabling (section 3.3)

3.1 Installing

The Account Authentication function is an optional feature that is usually inactive (locked). It must be installed, uninstalled, enabled or disabled for each disk array subsystem using Storage Navigator Modular. It must be installed and activated (unlocked) using a key code or key file. Before installation or uninstallation, it is essential to make sure that the subsystem is in normal operating condition. Installation and uninstallation of this feature cannot be performed if there are failures such as a controller blockade.

Prior to installing the Account Authentication feature, it is necessary to determine the following:

- User for *Built-in Account* (The administrator who can execute the registration of *Public Account*)
- Users for *Public Account* (Recommended to have more than 3 persons)
- Management authority responsible for each user (Storage Administrator, Account Administrator, Audit Log Administrator)
- User ID and Password for the *Public Account*
- User ID and Password for the *Public Account* that maintenance personnel use. These should not be managed by the maintenance Personnel but by the User).
- Another new Password for *Built-in Account*. (This is strictly confidential to the Maintenance Personnel.)

The following restrictions apply when installing the Account Authentication feature:

- Installation of the Account Authentication feature can be performed only by an account with the Account Administrator (View and Modify) role.
- Account Authentication cannot be used concurrently with Password Protection. Before installing Account Authentication, Password Protection must be uninstalled or disabled.
- Account Authentication cannot be used concurrently with NAS Manager Modular. Account Authentication cannot be installed on NAS Manager Modular.
- Account Authentication cannot be used with NAS. When installing **Account Authentication**, NAS options must be uninstalled, and the NAS I/F must be detached from the AMS subsystem.

The following instructions describe how to install Account Authentication, using Storage Navigator Modular:

1. Start Navigator and change the mode of operation to **Management Mode**.
2. Register the subsystem in which you will install Account Authentication. Connect to this subsystem; the following window is displayed.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.

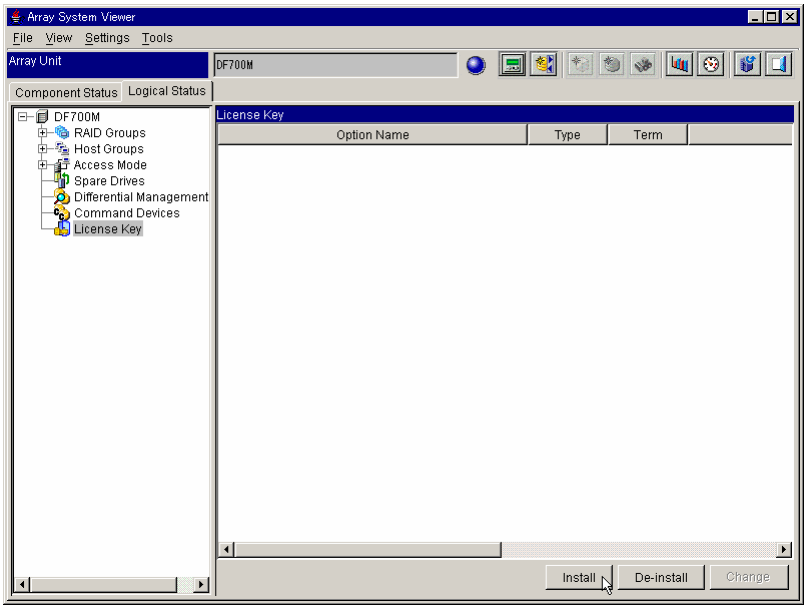


Figure 3.1 Array System Viewer Panel (Logical Status Page)

5. Click the **Install** button.

   The **Install Options** dialog is displayed.

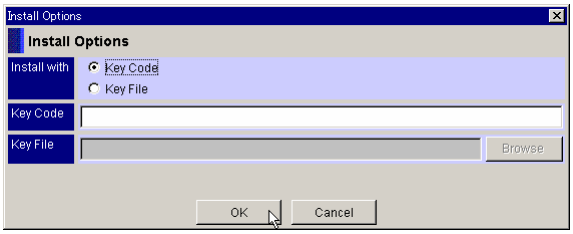


Figure 3.2 Install Options Dialog

6. When you install the option using the key code, click the **Key Code** radio button, then set up the key code. When you install the options using the key file, click the **Key File** radio button, and then set up the path for the key file. The **Browse** button can be used to set the correct path to a key file. Click **OK**.

7. When you install the options using the key file, the options selection dialog is displayed. Verify the **Option Name** and click **OK**.

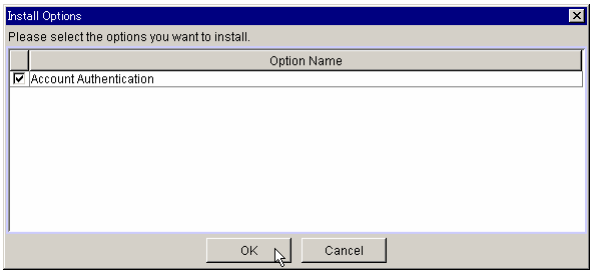
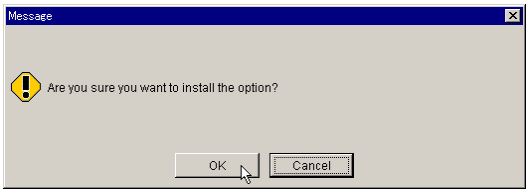
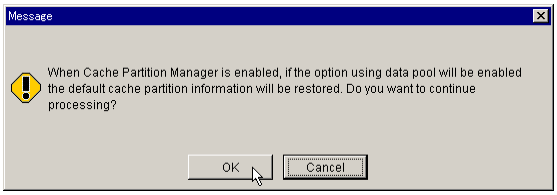


Figure 3.3 Options Selection Dialog

8. A screen appears, requesting a confirmation to install the Account Authentication option. Click **OK**.

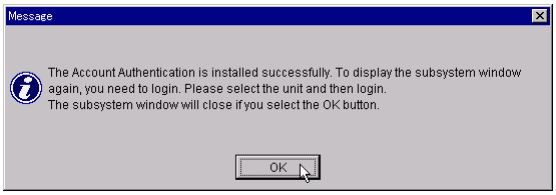


9. When Cache Partition Manager is enabled, the following message is displayed. Because Account Authentication does not use the data pool, click **OK** and do not do anything else.



10. When you install the options using the key file, the result dialog is displayed. Click the **Close** button.
11. Select **OK** on the confirmation message.

    The Array System Viewer panel closes.



12. Open the subsystem (Array System Viewer panel).

    The Login panel is displayed.

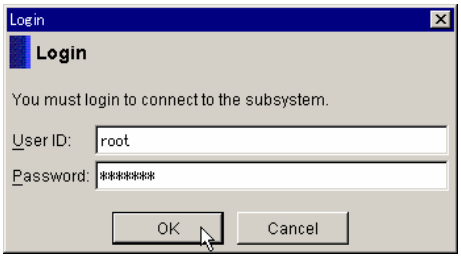


Figure 3.4 Login Panel

13. Enter the **User ID** and **Password**, and then click **OK**.

    User ID: root, **Password**: storage

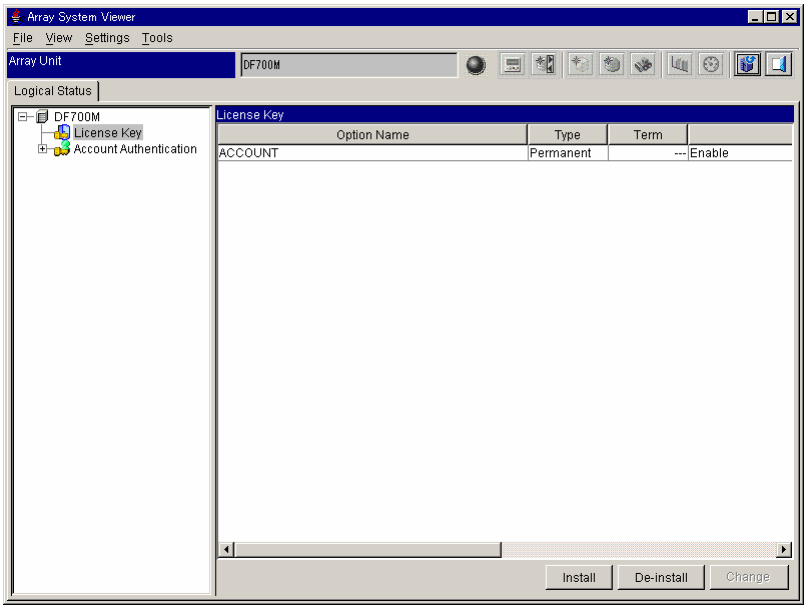


Figure 3.5 Array System Viewer Panel (Logical Status Page: Option Enable)

After the **Account Authentication** feature is installed, the user associated with the *Built-in Account* can create a new *Public Account*.

Note 1: It is important to change the initial password of a Built-in account after installation, because the initial password can be easily deciphered.

Note on retrieving lost passwords: You must carefully manage the Built-in account passwords. A Built-in account password cannot be reset to the initial password, if its current password is lost.

3.2 Uninstalling

To uninstall Account Authentication, the key code provided with the Account Authentication feature is required. When the Account Authentication function is uninstalled, it is no longer available (locked) until it is reinstalled using the key code or key file.

The following restrictions apply when uninstalling the Account Authentication feature:

- Uninstallation operations can be performed only by the account assigned the role of an **Account Administrator (View and Modify)**.
- During uninstallation, all the accounts that have been logged in (excluding the own account) are forced to logout. Uninstallation operation cannot be performed successfully until all users are logged out.
- After uninstallation, information regarding all user accounts (excluding the initial password of the Built-in account) is deleted.

Follow the instructions below to uninstall Account Authentication.

1. Start Navigator.
2. Register the subsystem in which you will uninstall Account Authentication. Connect to this subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Click the **Logical Status** tab.
5. Click the **License Key** icon. See Figure 3.5.
6. Click the **De-install** button.

   The **De-install Options** dialog is displayed.

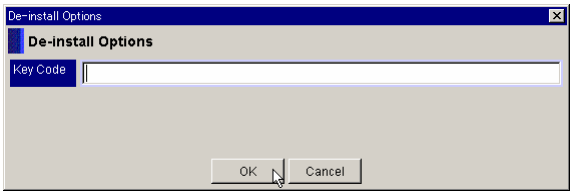
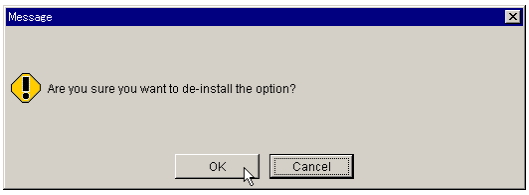


Figure 3.6 De-install Options Dialog

7. Enter a key code in the text box. Click **OK**.

8. A screen appears, requesting a confirmation to uninstall the Account Authentication option. Click **OK**.



9. A message appears, confirming that this feature has been uninstalled. Click **OK**.

3.3 Enabling or Disabling

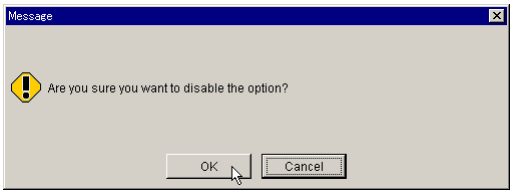
The Account Authentication function can be enabled or disabled depending on the conditions under which the feature has been installed.

The following restrictions apply when enabling or disabling the Account Authentication feature:

- Enable or Disable operations can be performed only by the account assigned the role of an **Account Administrator (View and Modify)**.
- When the Account Authentication function is enabled or disabled, all the accounts that are currently logged in (excluding the own account) are forced to logout. Enable or Disable operations cannot be performed successfully until all users are logged out.
- Account Authentication operations can no longer be performed after the function is disabled.
- Disabling the Account Authentication function does not result in the deletion of user account information. All account information remains in the disk subsystem.

The following procedure describes steps for enabling or disabling the Account Authentication function after it has been installed:

1. Start Navigator and change the mode of operating to **Management Mode**.
2. Register the subsystem in which you will set Account Authentication. Connect to this registered subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Click the **Logical Status** tab.
5. Click the **License Key** icon. See Figure 3.5.
6. Click on **ACCOUNT** in the **Option List** text box, and then click the **Change** button.



7. A message appears, confirming that this option is set. Click **OK**.

Chapter 4 Performing Account Authentication Operations

This chapter provides instructions for performing Account Authentication operations using Navigator. This chapter includes the following:

- Logging In (section 4.1)
- Logging Out (section 4.2)
- Displaying Account Information (section 4.3)
- Adding Account Information (section 4.4)
- Modifying Account Information (section 4.5)
- Changing Owner Account Password Information (section 4.6
- Deleting Account Information (section 4.7)

4.1 Logging In

1. Start Navigator.

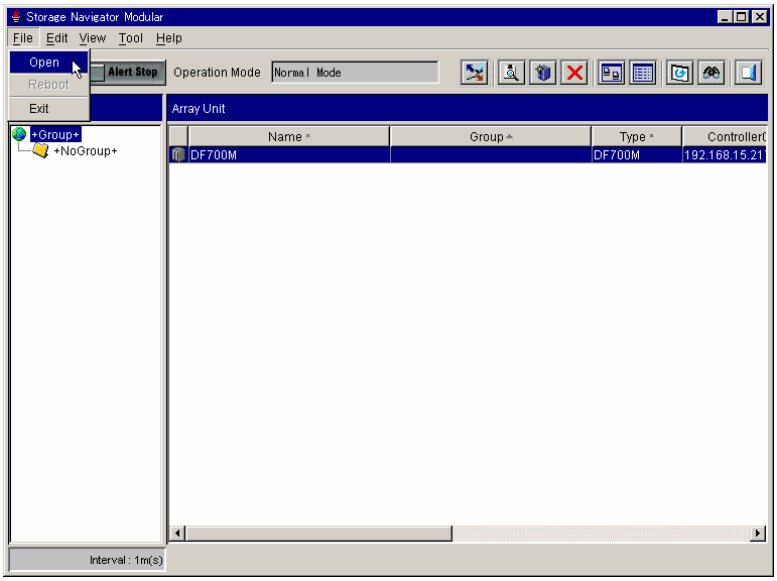


Figure 4.1 Main Screen of Navigator

2. Select the array unit you want to login, select **Open** on the **File** menu.
3. The **Login** panel is displayed. Enter the registered **User ID** and **Password**, and then click **OK**.

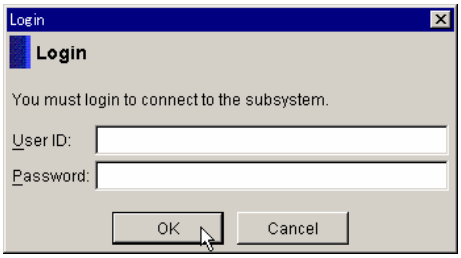


Figure 4.2 Login Panel

When you have successfully logged in, the Array System Viewer Panel is displayed.

Note: When a login cannot be performed after following the procedure explained in this section, although the account has been registered, contact a user who manages the account of the **Account Administrator (View and Modify)** role. (It is possible that the user ID or password is incorrect or the account has been invalidated through a forced logout.)

4.2 Logging Out

From the **File** menu, select **Exit**. Alternatively, from the tool bar, select **Exit**  on the Array System Viewer Panel.

4.2.1 Forcibly Logging Out

The forced logout forcibly logs out other users except the built-in account that logs in the disk subsystem.

Note 1: When a failure occurs in the controller of the disk subsystem during a login of an account, a session ID being logged in may remain in the disk subsystem. Therefore, when a controller failure occurs, log out by force all the accounts with the remaining session IDs among the accounts to which the roles of the **Account Administrator (View and Modify)** are assigned.

Note 2: The account that has been forced into logout becomes invalid. The account concerned cannot be logged in again unless the account is validated using the account to which the **Account Administrator (View and Modify)** role is assigned.

1. Start Navigator.
2. Register the subsystem in which you will forcibly logout. Connect to this registered subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.

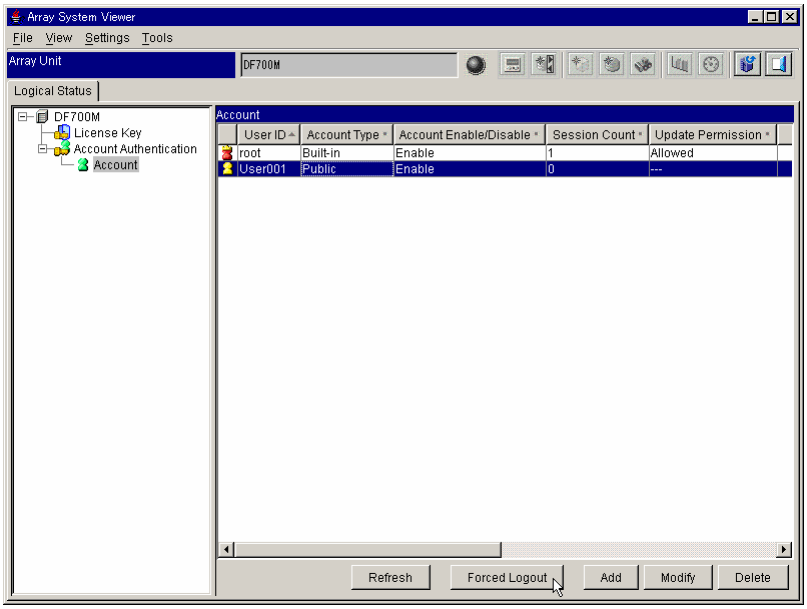


Figure 4.3 Forcibly Logout

6. Select the account you want to forcibly logout from **Account** list, and then select **Forced Logout**.

7. Observe any messages that appear and click **OK** to continue.

4.3 Displaying Account Information

To display the account information:

Note: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)** or an **Account Administrator (View Only)**.

1. Start Navigator.
2. Register the subsystem in which you will display account information. Connect to this subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)** or an **Account Administrator (View Only)**.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.

   The registered account information is displayed.

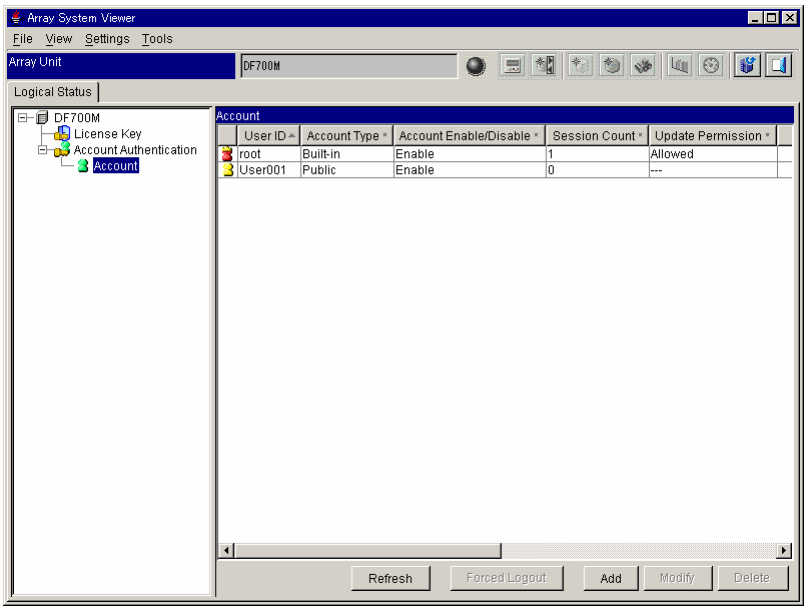


Figure 4.4 Displaying the Account Information

Table 4.1 Displaying Contents of Account Information

Item	Contents
Icon	 : Built-in account  : Public account
User ID	The user ID is displayed.
Account Type	The account type is displayed.
Account Enable/Disable	Enable or Disable is displayed.
Session Count	The session ID is displayed.
Update Permission	Allowed: The session ID is Modify mode. ---: The session ID is View mode.

4.3.1 Account Properties

To display account every user:

1. Select account from the **Account** list, and then select **Property** (right-click pop-up) menu.

   The **Property** panel is displayed.

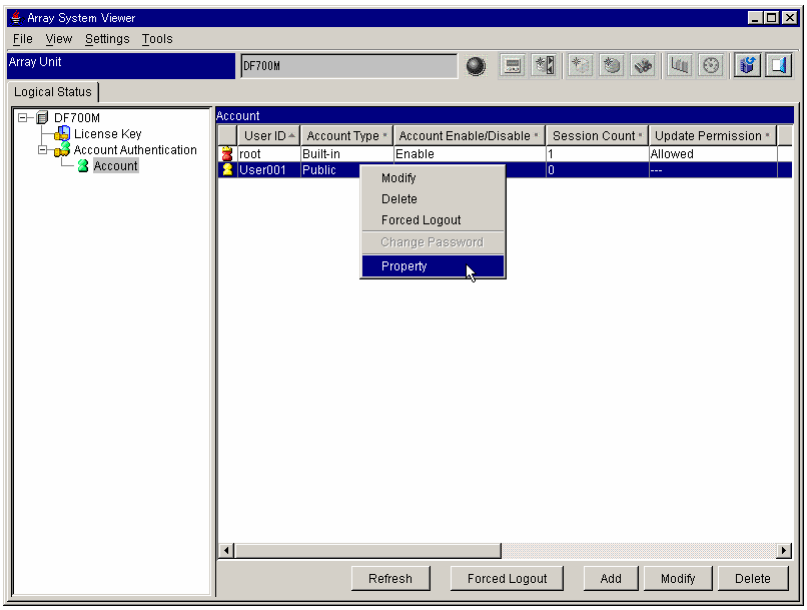
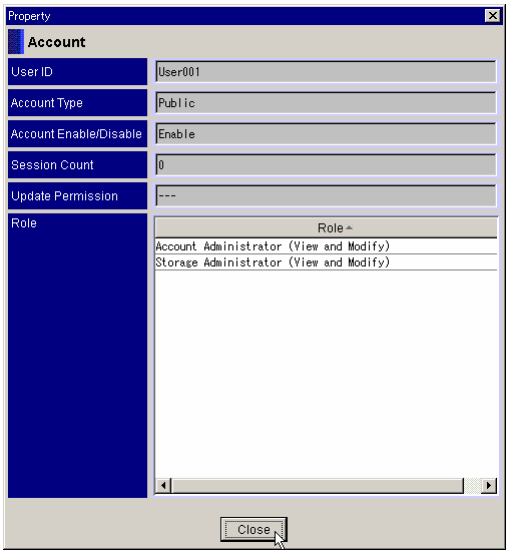


Figure 4.5 Account Property

2. Click **Close** to close this panel.



4.4 Adding Account Information

To add the account information:

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**. Immediately after the installation of the Account Authentication function, log in with the built-in account and add the account information.

Note 2: When adding the account information, you must register an optional user ID and a password. It is recommended to register character strings that are difficult to be assumed as the user ID and the password.

It is prescribed in the standard ISO/IEC 17799 (BS 7799) to avoid the following character strings because they are especially easy to be assumed.

Built_in_user, *Admin*, *Administrator*, *Administrators*, *root*, *Authentication*, *Authentications*, *Guest*, *Guests*, *Anyone*, *Everyone*, *System*, *Maintenance*, *Developer*, and *Supervisor*.

Note 3: It is recommended that a user who uses an account should log in and change the password immediately after creation of the account (that is because it is possible that an account creator remembers the initial password and logs in illegally).

Note 4: When monitoring the failure via Navigator, because the failure monitoring cannot be applied to the disk subsystem that is a target of the Account Authentication unless it is logged in, register the common user ID and the password for the monitoring to be used at the time of the failure monitoring. It is required to create the user ID and the password for the failure monitoring beforehand for each disk subsystem for which the Account Authentication has been validated.

Note 1: It is not recommended to setup more than one account for a single user.

Note 2: Service personnel use the Navigator for maintenance of subsystems as well. When creating an account, register the user ID for service personnel. Assign the **Storage Administrator (View and Modify)** for service personnel account.

1. Start Navigator.
2. Register the subsystem in which you will add Account Information. Connect to this registered subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.

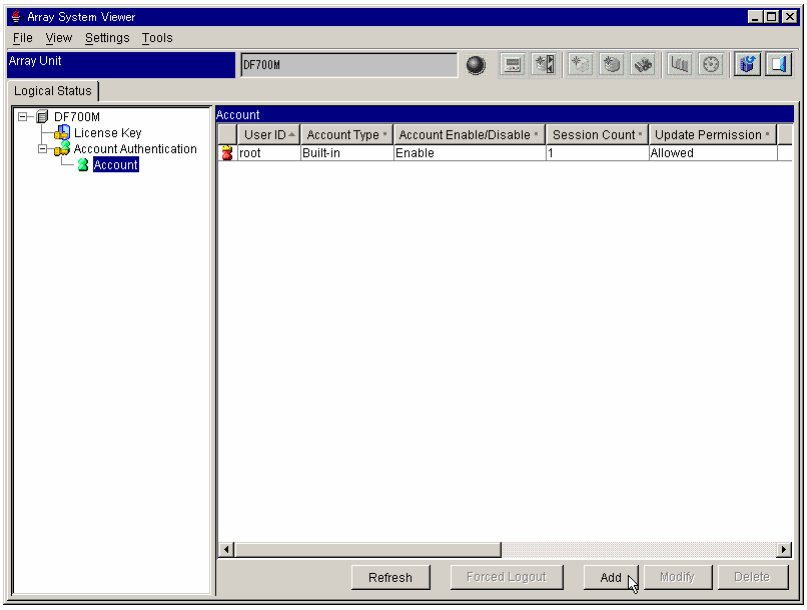


Figure 4.6 Adding an Account Information

6. Select **Add**.

   The **Add Account** dialog is displayed.

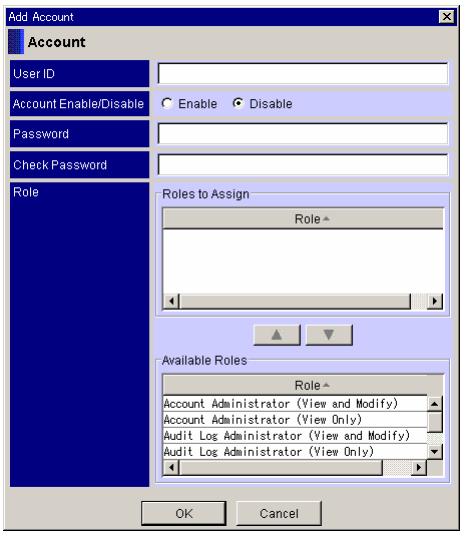


Figure 4.7 Add Account Dialog (Before Setting)

7. Input or select the **User ID**, **Account Enable/Disable**, **Password**, and **Check Password**.
8. Select **Role** to be added, and then click the ▲ button.

   The added contents are displayed in the **Roles to Assign** list.

   An assignable role is 1 to 6 per user.

   To delete, click the line to be deleted in the **Roles to Assign** list and click the ▼ button. The deleted contents disappear from the display of **Available Roles** list.

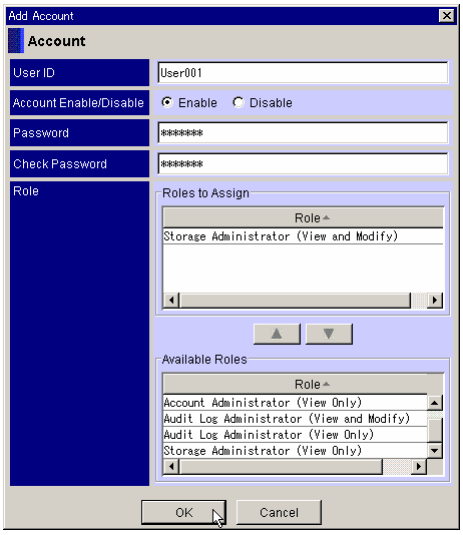


Figure 4.8 Add Account Dialog (After Setting)

9. Click **OK**.
10. Observe any messages that appear, and click **OK** to continue.

4.5 Modifying Account Information

To modify the account information:

You can modify following information:

- Password
- Role assignment
- Account enable/disable

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: The procedure for modifying the account information to be explained here can be executed for an account of the other user. The own account information cannot be modified. However, the built-in account can modify the own account information.

Note 3: The account information that has been modified is applied to the following logins of the account concerned.

Note 4: The public account cannot modify the built-in account information.

Note 5: Either user ID of the public account and the built-in account cannot be changed.

To modify the account information:

1. Start Navigator.
2. Register the subsystem in which you will modify Account Information. Connect to this registered subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.

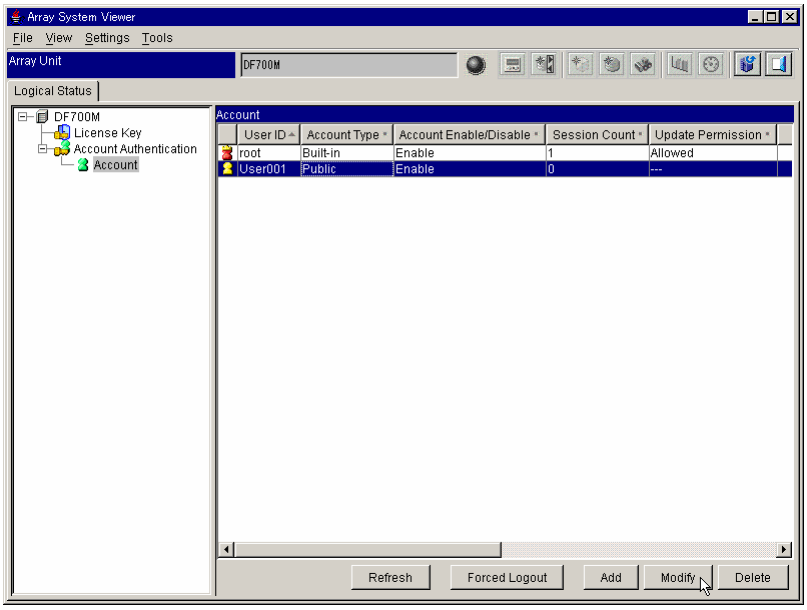


Figure 4.9 Modifying the Account Information

6. Select account from the **Account** list that must be modified, and then select **Modify**. The **Modify Account** dialog is displayed.

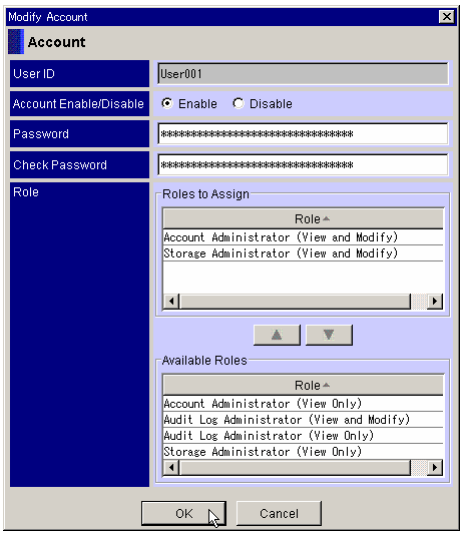


Figure 4.10 Modify Account Dialog

7. Input or select the **Account Enable/Disable** or **Password** and **Check Password**.
8. Select **Role** to be modified, and then click the ▲ button.

   The added contents are displayed in **Roles to Assign** list.

   An assignable role is 1 to 6 per a user.

   To delete, click the line to be deleted in the **Roles to Assign** list and click the ▼ button. The deleted contents disappear from the display of **Available Roles** list.
9. Click **OK**.
10. Observe any messages that appear and click **OK** to continue.

4.6 Changing Owner Account Password Information

To change the password with Navigator:

1. Start Navigator.
2. Register the subsystem in which you will change Account Information. Connect to this registered subsystem.
3. Login with the account in which you will change Account Information.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.
6. Select account from the **Account** list that will be changed, and then select **Change Password** (right-click pop-up menu).

   The **Change Password** dialog is displayed.

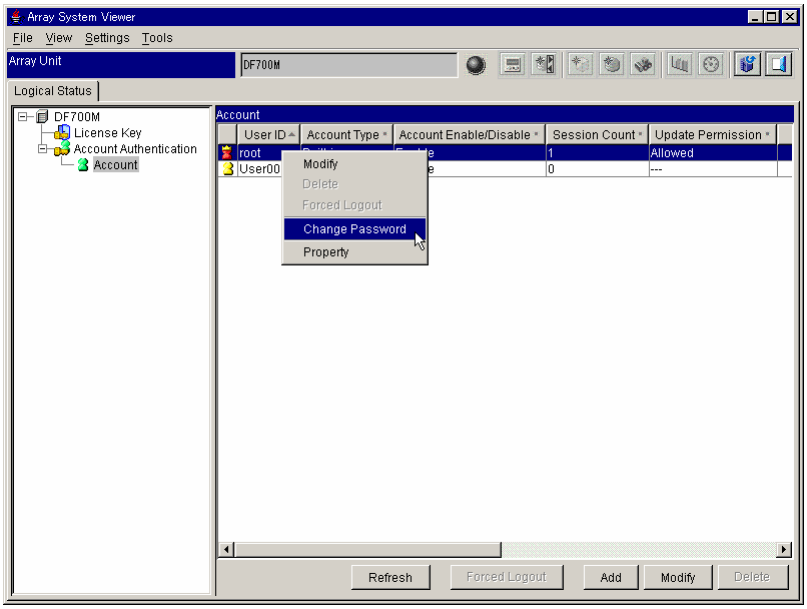
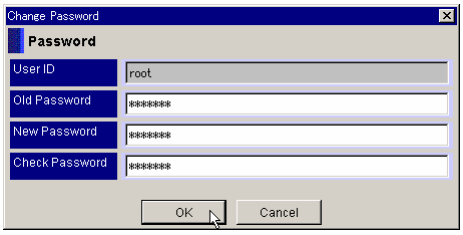


Figure 4.11 Changing Password

7. Input the **Old Password**, **New Password**, and **Check Password**, then select **OK**.

   You must input the same contents **New Password** and **Check Password**.



8. Observe any messages that appear and click **OK** to continue.

4.7 Deleting Account Information

To delete the account information:

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: The own and built-in account information cannot be deleted.

Note 3: When a user account that has been logged in is deleted, the user is immediately forced into logout.

1. Start Navigator.
2. Register the subsystem in which you will delete Account Information. Connect to this registered subsystem.
3. Login with the account assigned to the role of an **Account Administrator (View and Modify)**.
4. Select the **Logical Status** tab.
5. Click **Account** in the **Account Authentication** icon.

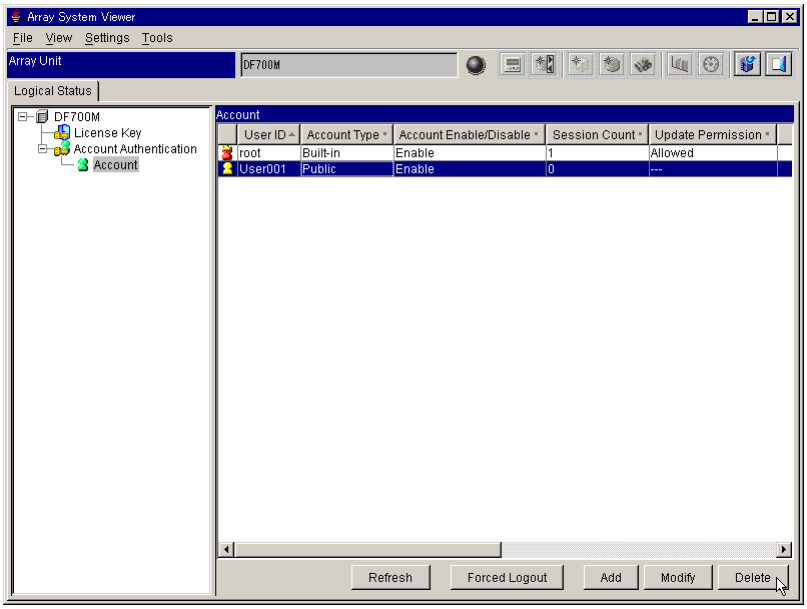


Figure 4.12 Deleting the Account Information

6. Select the account to delete from the **Account** list, and then select **Delete**.
7. Observe any messages that appear and click **OK** to continue.

Chapter 5 Operations Using CLI

This chapter describes the following operation procedure for Account Authentication using the CLI of the Navigator. The following sections are included:

- Installing
- Uninstalling
- Adding Account Information
- Modifying Account Information
- Changing Password of the Owner Account Information
- Deleting Account Information
- Logging in
- Forcibly Logging out
- Setting/Deleting the Account Information for the Script

5.1 Installing

The Account Authentication feature is usually unselectable (locked). To make it available, you must install the Account Authentication feature and make its functions selectable (unlocked). **To install this function, the key code or key file provided with the optional feature is required.**

Follow the instructions below to install the Account Authentication feature. Account Authentication is installed and uninstalled using Navigator.

Note 1: Before installing and uninstalling, make sure that the subsystem is in normal operating condition. If a failure such as a controller blockade has occurred, installation and uninstallation operations cannot be performed.

Note 2: Account Authentication cannot be used with Password Protection at the same time. When installing Account Authentication, Password Protection must be uninstalled or disabled.

Note 3: Account Authentication cannot be used with NAS Manager Modular at the same time. Account Authentication cannot be installed on NAS Manager Modular.

The following instructions describe how to install Account Authentication, using the CLI version of Navigator:

1. From the command prompt, register the subsystem in which you will install the Account Authentication feature. Connect to the subsystem.
2. Install the optional features by using the following:

   Example: The gray part is displayed when the Cache Partition Manager is enabled.

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to install the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

   Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name                    Type      Term     Status
ACCOUNT                        Permanent ---      Enable
%
```

Note 1: Because the initial password of a built-in account can be assumed easily, be sure to change it after the installation.

Note 2: When a password of a built-in account is lost, it cannot be returned to the initial password. Therefore, take enough care to manage the password of the built-in account.

Account Authentication is installed and the status is “Enable”. Installation of Account Authentication is now complete.

5.2 Uninstalling

Follow the instructions below to uninstall Account Authentication. When it is uninstalled, the Account Authentication is not available (locked) until it is installed by the key code or key file.

To uninstall Account Authentication, the key code provided with the Account Authentication feature is required.

Note 1: The uninstallation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: When the uninstallation is executed, all the accounts that have been logged in excluding the own account are forced into logout. The un-installation cannot be executed when the forced logout of all users is not completed.

Note 3: After the uninstallation is executed, all the account information excluding the initial password of the built-in account is deleted.

1. From the command prompt, register the subsystem in which you will uninstall the Account Authentication feature. Connect to the subsystem.
2. Uninstall the optional features by using the following:

   Example:

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to de-install the option? (y/n [n]): y
The option is de-installed successfully.
%
```

   Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
DMEC002015: No information displayed.
%
```

Uninstalling Account Authentication is now complete.

5.2.1 Enabling/Disabling

The Account Authentication function can be set to Disable or Enable depending on the conditions in which the feature has been installed.

The following paragraphs describe a GUI procedure for setting the function to Disable or Enable while the Account Authentication feature stays in an installed state.

Note 1: Setting the function to disable or enable can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: When the function to disable or enable is executed, all the accounts that have been logged in excluding the own account are forced into logout. The uninstallation cannot be executed when the forced logout of all users is not completed.

Note 3: When the Account Authentication function is disabled, the authentication becomes unable to be done.

Note 4: Even when the Account Authentication function is disabled, the whole account information is not deleted and remains in the disk subsystem as it is.

Note 5: Account Authentication cannot be used with Password Protection at the same time. When installing Account Authentication, Password Protection must be uninstalled or disabled.

1. From the command prompt, register the subsystem in which you will change the status of the Account Authentication feature. Connect to the subsystem.
2. Execute the **auopt** command to change the status (enable or disable) of the Account Authentication feature.

   The following is an example of how to change the status from enable to disable. To change the status from disable to enable, enter **enable** after the **-st** option.

   Example:

```
% auopt -unit subsystem-name -option ACCOUNT -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n [n]): y
The option has been set successfully.
%
```

3. Execute the **auopt** command to verify that the Account Authentication feature status has changed.

   Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name                  Type      Term     Status
ACCOUNT                      Permanent ---      Disable
%
```

Enabling or disabling Account Authentication is now complete.

5.2.1.1 Displaying Account Information

Note: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)** or an **Account Administrator (View Only)**.

To display the account information:

1. From the command prompt, register the subsystem in which you will display the Account Authentication information. Connect to the subsystem.
2. Execute the **auaccount** command to display the Account Authentication information. The example is shown below.

   Example:

```
% auaccount –unit subsystem-name –refer
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
User ID                 : root
Account Type            : Built-in
Account Enable/Disable  : Enable
Session Count           : 1
Update Permission       : Allowed
Role                    : Storage Administrator (View and Modify)
                          Storage Administrator (View Only)
                          Account Administrator (View and Modify)
                          Account Administrator (View Only)
                          Audit Log Administrator (View and Modify)
                          Audit Log Administrator (View Only)

User ID                 : User001
Account Type            : Public
Account Enable/Disable  : Disable
Session Count           : 0
Update Permission       : None
Role                    : Storage Administrator (View and Modify)
%
```

5.3 Adding Account Information

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**. Immediately after the installation of the Account Authentication function, log in with the built-in account and add the account information.

Note 2: When adding the account information, you must register an optional user ID and a password. It is recommended to register character strings that are difficult to be assumed as the user ID and the password.

It is prescribed in the standard ISO/IEC 17799 (BS 7799) to avoid the following character strings because they are easy to be assumed.

Built_in_user, *Admin*, *Administrator*, *Administrators*, *root*, *Authentication*, *Authentications*, *Guest*, *Guests*, *Anyone*, *Everyone*, *System*, *Maintenance*, *Developer*, and *Supervisor*.

Note 3: It is recommended that a user who uses an account should log in and change the password immediately after creation of the account (because it is possible that an account creator remembers the initial password and logs in illegally).

Note 4: When monitoring the failure via Navigator, because the failure monitoring cannot be applied to the disk subsystem that is a target of the Account Authentication unless it is logged in, register the common user ID and the password for the monitoring to be used at the time of the failure monitoring. It is required to create the user ID and the password for the failure monitoring beforehand for each of the disk subsystem for which the Account Authentication has been validated.

To add the account information:

1. From the command prompt, register the subsystem in which you will add the Account Authentication information. Connect to the subsystem.
2. Execute the **auaccount** command to add the Account Authentication information. The example is shown below.

   Example:

```
% auaccount –unit subsystem-name –add –uid User001 –account disable –rolepattern 000001
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
Assigned role
  Storage Administrator (View and Modify)
Are you sure you want to add the account? (y/n [n]): y
Please input password.
Password: User001-password
Re-enter Password: User001-password
The account has been added.
%
```

The role pattern value (-rolepattern) is as follows.
100000: Audit Log Administrator (View Only)
010000: Audit Log Administrator (View and Modify)
001000: Account Administrator (View Only)
000100: Account Administrator (View and Modify)
000010: Storage Administrator (View Only)
000001: Storage Administrator (View and Modify)

Example: When the role pattern is assigned **Account Administrator (View and Modify)** and **Storage Administrator (View and Modify)**, specify 000101.

Note: When using “!”, “#”, “$”, “&”, “’”, “*”, “?”, “`”, “{”, “|”, or “~” for the –uid option, set the file by using the –uidfile option. When “!”, “#”, “$”, “&”, “’”, “*”, “?”, “`”, “{”, “|”, or “~” is used for the –uid option, the command may terminate abnormally or the illegal user ID may be set.

5.4 Modifying Account Information

You can modify following information:

- Password
- Role assignment
- Account enable/disable

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: The following procedure for modifying the account information can be executed for an account of the other user. The own account information cannot be modified. However, the built-in account can modify the own account information.

Note 3: The account information that has been modified is applied to the following logins of the account concerned.

Note 4: The public account cannot modify the built-in account information.

Note 5: Either user ID of the public account and the built-in account cannot be changed.

Note 6: When using "!", "#", "$", "&", "'", "*", "?", "`", "{", "|", or "~" for the –uid option, set the file by using the –uidfile option.

To modify the account information:

1. From the command prompt, register the subsystem in which you will modify the Account Authentication information. Connect to the subsystem.
2. Execute the **auaccount** command to modify the Account Authentication information. The example is shown below.

   Example:

```
% auaccount –unit subsystem-name –chg –uid User001 –account enable –rolepattern 000101
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
Assigned role before a change
  Storage Administrator (View and Modify)
Assigned role after a change
  Storage Administrator (View and Modify)
  Account Administrator (View and Modify)
Are you sure you want to change the account? (y/n [n]): y
The account information has been changed.
%
```

5.5 Changing Password of the Owner Account Information

To change the owner password:

1. From the command prompt, register the subsystem in which you will change the owner password. Connect to the subsystem.
2. Execute the **auaccount** command to change the owner password. The example is shown below.

   Example:

```
% auaccount –unit subsystem-name –chgownpwd
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
Are you sure you want to change the password? (y/n [n]): y
Please input password.
Old Password: old-root-password
New Password: new-root-password
Re-enter Password: new-root-password
The password has been changed.
%
```

5.6 Deleting Account Information

Note 1: This operation can be operated only with the account assigned to the role of an **Account Administrator (View and Modify)**.

Note 2: The own and built-in account information cannot be deleted.

Note 3: When a user account that has been logged in is deleted, the user is immediately forced into logout.

Note 4: When using "!", "#", "$", "&", "'", "*", "?", "`", "{", "|", or "~" for the -uid option, set the file by using the -uidfile option.

To delete the account information:

1. From the command prompt, register the subsystem in which you will delete the Account Authentication information. Connect to the subsystem.
2. Execute the **auaccount** command to delete the Account Authentication information. The example is shown below.

   Example:

```
% auaccount -unit subsystem-name -rm -uid User001
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
Are you sure you want to delete [User001]? (y/n [n]): y
If you will delete the logged in user account, user is logged out. Do you want t
o continue processing?
 (y/n [n]): y
The account has been deleted.
%
```

5.7 Logging in

Note: When a login cannot be performed following the procedure in this section even though the account has been registered, contact a user who manages the account of the **Account Administrator (View and Modify)** role. It is possible that the user ID or password is incorrect or the account has been invalidated through a forced logout.

1. For example, you specify the **aurgref** command. The subsystem requires the User ID and its password. Enter the User ID and its password. The example is shown below.

   Example:

```
% aurgref -unit subsystem-name
The Account Authentication is enabled. Please login.
User ID: User001
Password: User001-password
RAID   RAID         Parity        Total Capacity          Free Capacity
Group  Level        Groups  Type         [block]               [block]
    0    0( 2D)          1  FC        1123549184      944930816( 84.1%)
    1    0( 2D)          1  FC         559788032      391778304( 70.0%)
    2    5( 2D+1P)       1  FC         559788032      528330752( 94.4%)
    3    0( 2D)          1  FC         559788032      538816512( 96.3%)
%
```

5.8 Forcibly Logging out

The forced logout forcibly logs out other users except the built-in account that logs in the disk subsystem.

Note 1: When a failure occurs in the controller of the disk subsystem during a login of an account, a session ID being logged in may remain in the disk subsystem. Therefore, when a controller failure occurs, log out by force all of the accounts with the remaining session IDs among the accounts to which the roles of the **Account Administrator (View and Modify)** are assigned.

Note 2: The account that has been forced into logout becomes invalid. The account concerned cannot be logged in again unless the account is validated using the account to which the **Account Administrator (View and Modify)** role is assigned.

Note 3: When using "!", "#", "$", "&", "'", "*", "?", "`", "{", "|", or "~" for the –uid option, set the file by using the –uidfile option.

1. From the command prompt, register the subsystem in which you will log out forcibly. Connect to the subsystem.
2. Execute the **auaccount** command to log out forcibly. The example is shown below.

   Example:

```
% auaccount –unit subsystem-name –forcelogout –uid User001
The Account Authentication is enabled. Please login.
User ID: root
Password: root-password
Are you sure you want to force logout of [User001]? (y/n [n]): y
When the user is using the subsystem, the user cannot continue the operation.
The account is disabled and cannot login from the next time.
Do you want to continue processing? (y/n [n]): y
The force logout of [User001] has been completed.
%
```

5.9 Setting/Deleting the Account Information for the Script

Note: When using “!”, “#”, “$”, “&”, “’”, “*”, “?”, “`”, “{”, “|”, or “~” for the –uid option, set the file by using the –uidfile option. When “!”, “#”, “$”, “&”, “’”, “*”, “?”, “`”, “{”, “|”, or “~” is used for the –uid option, the command may terminate abnormally or the illegal user ID may be set.

1. From the command prompt, register the subsystem in which you will set or delete the Account Authentication information. Connect to the subsystem.
2. Execute the **auaccountenv** command to set or delete the Account Authentication information. The example is shown below.

   Example:

```
% auaccountenv –set –uid User001
Are you sure you want to set the account information? (y/n [n]): y
Please input password.
Password: User001-password
The account information has been set successfully.
%
% auaccountenv –rm
Are you sure you want to delete the account information? (y/n [n]): y
The account information has been deleted successfully.
%
```

3. Set the Navigator environment variable (file name: startsnm.bat). By setting the environment variable here, the script operation that uses the set account information becomes possible.

   When making it valid by the limitation in the script to be executed, it is defined at the head of the script.

   STONAVM_ACT=on

   The input request for the user ID and password of Account Authentication is executed with the user ID and password set with the **auaccountenv** command by setting the STONAVM_ACT environment variable to “on”.

   STONAVM_RSP_PASS=on

   All the input requests for checking a command are responded with “y” by setting the STONAVM_RSP_PASS environment variable to “on”.

   Example:

```
% set STONAVM_ACT=on
% set STONAVM_RSP_PASS=on
```

Chapter 6 Troubleshooting

This chapter discusses the following topics:

- General Troubleshooting (see section 6.1)
- Contacting the Hitachi Data Systems Support Center (see section 6.2)

6.1 General Troubleshooting Tips

The user is responsible for operation and normal maintenance of the computer(s) that host Storage Navigator software. Following are guidelines for troubleshooting Storage Navigator software operations:

- **Check the cabling and the LAN.** Verify that both the computer and LAN cabling are firmly attached, and that the LAN is operating properly.
- **Reboot the computer.** Close any programs that are not responding. If necessary, reboot the computer.
- If Storage Navigator does not succeed in connecting to the array unit, the following message may display:

  An invalid response was received from the subsystem

  This indicates that Storage Navigator may have been connected to the array unit while the array unit automatically rebooted. Connect to the array unit again after approximately 3 minutes.
- Storage Navigator may hang up in the following cases:
  - The communication with the connected array unit fails due to controller blockage, array unit failure, or disconnected LAN connection, etc., or the array unit receives a Reset/LIP from the host.
  - Other applications are working concurrently and memory utilization or a CPU use rate is high.
- If Storage Navigator hangs up, terminate it forcibly and check the array unit status and the connection status of the LAN. Reboot Storage Navigator once again.
- The Storage Navigator can open multiple **Array System Viewer** windows for one array unit. When multiple **Array System Viewer** windows are open, a shortage of memory may occur, depending on the configuration of the system in which the Storage Navigator has been installed; this results in program hang-ups. When opening **Array System Viewer** windows, open only one window to operate an array unit.

6.2 Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure you can provide as much information about the problem as possible. Include the circumstances surrounding the error or failure, the Storage Navigator configuration information, and the exact content of messages displayed on the Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours a day, 7 days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

Acronym	Expansion
A	Ampere
AL-PA	arbitrated loop-physical address
AMS	Adaptable Modular Storage
API	application programming interface
ASTM	American Society for Testing Materials
ATA	Advanced Technology Attachment standard
ATM	asynchronous transfer mode
BC	business continuity
BS	Basic (power) supply
BSA	bus adapter
BTU	British thermal unit
CCI	command control interface
CEC	Canadian Electroacoustic Community
CFW	cache fast write
CHAP	challenge handshake authentication protocol
CIFS	common internet file system
CKD	count-key data
CLI	command line interface
CSA	Canadian Standards Association
CSV	comma separated value
CTG	consistency group
CTL	controller
CU	controller unit
CUDG	control unit diagnosis
dB(A)	decibel (A-weighted)
D-CNT	default (owner) controller
DAMP	Disk Array Management Program
DDL	data definition language
DHCP	dynamic host configuration protocol
DKC	disk controller unit
DLM	data lifecycle management
DM-LU	differential management logical unit
DRAM	dynamic random access memory
DWDM	dense wavelength division multiplexer
EMI	electromagnetic interference
EPO	emergency power-off
FC	fibre channel
FC-AL	fibre channel-arbitrated loop
FCC	Federal Communications Commission
FCP	fibre-channel protocol

Gbps	gigabit per second
HA	high availability
HACMP	high availability cluster multi-processing
HBA	host bus adapter
HDLM	Hitachi Dynamic Link Manager
HORCM	Hitachi Open Remote Copy Manager
H-LUN	host logical unit
H-RAIN	heterogeneous redundant array of independent nodes
HSN	hierarchical star network
HWM	high water mark
IDE	integrated drive electronics; see also ATA.
IIS	Internet Information Service
IOPS	input output operations per second
IOS	internet work operating system
iSCSI	internet small computer system interface
JRE	Java 2 runtime environment
LCP	local control port
LD	logical device
LDEV	logical device
LDM	logical device manager
LIP	loop initialization primitive
LRU	least recently used
LUN	logical unit number
LUSE	LU size expansion
LVI	logical volume image
LVM	logical volume manager
MCU	main control unit
NDMP	Network Data Management Protocol
MDB	master directory block
MIB	message information block
μP	microprocessor
MR	magneto-resistive
MU	mirror unit
MVS	multiple virtual storage
MVS/ESA	multiple virtual storage /enterprise systems architecture
MVS/XA	multiple virtual storage /extended architecture
NAS	network attached storage
NBU	NetBackup (a Symantec product)
NEC	National Electrical Code
NFS	network file system
NIC	network interface card
NIS	network information service
NNC	network node controller
NSC	network storage controller

NTP	network time protocol
NVS	nonvolatile storage
OCI	Oracle Call Interface
ODM	object data manager
OFC	open fibre control
ORM	online read margin
OSI	open systems interconnection
PCI	power control interface
PDL	product documentation library
PFUS	pool full status
POSIX	portable operating system interface
PPRC	peer-to-peer remote copy
PSUE	pair suspended-error status
PSUS	pair suspended-split
PSUS(N)	pair suspended – not restored status
PV	physical volume
P-VOL	primary volume
RAID	redundant array of independent disks
RC	reference code
RCU	remote control unit
RPO	recovery point objective
RTC	real-time clock
RTO	recovery time objective
SAN	storage-area network
SATA	serial ATA
SCSI	small computer system interface
SIM	service information message
SM	shared memory module
SMB	server message block
SMTP	simple mail transfer protocol
SNIA	Storage Networking Industry Association
SNMP	simple network management protocol
SONET	synchronous optical network
SSL	secure socket layer
SSWS	suspend for swapping S-VOL
S-VOL	secondary volume
TID	target identifier
TPOF	tolerable points of failure
UDP	user diagram protocol
UL	Underwriters' Laboratories
USP	Universal Storage Platform
VCS	Veritas Cluster Server™
VDE	Verband Deutscher Elektrotechniker
VIB	volume information block

VOLID	volume identifier
V-VOL	virtual volume (Snapshot Image)
VxVM	Veritas Volume Manager
WDM	wavelength division multiplexing

Index