HITACHI
DATA SYSTEMS

Hitachi TagmaStore®
Adaptable Modular Storage
and Workgroup Modular Storage

Password Protection User's Guide

MK-95DF704-03

Document Revision Level

Revision	Date	Description
MK-95DF704-00	June 2005	Initial Release
MK-95DF704-01	August 2005	Revision 1, supersedes and replaces MK-95DF704-00
MK-95DF704-02	May 2006	Revision 2, supersedes and replaces MK-95DF704-01
MK-95DF704-03	July 2006	Revision 3, supersedes and replaces MK-95DF704-02

Source Documents for this Revision

Not applicable

Changes in this Revision

- Editorial changes only, no technical changes

Preface

This document describes and provides instructions for installing and using the Password Protection support function for the Hitachi TagmaStore® Adaptable Modular Storage (AMS) and Workgroup Modular Storage (WMS) storage subsystems (hereafter referred to as the AMS/WMS subsystems). Before using the TagmaStore AMS/WMS Password Protection function, please read the operating procedures and notices included in this document.

This document assumes the following:

- 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 TagmaStore AMS and/or WMS subsystem.
- The user is familiar with the Storage Navigator Modular software for the Hitachi TagmaStore AMS/WMS subsystem.

Notice: The use of Password Protection and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Microcode Level

This document revision applies to TagmaStore AMS/WMS microcode 0750/A and higher.

Convention for Storage Capacity Values

Storage capacity values for logical devices (LDEVs) 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

Referenced Documents

- *Hitachi TagmaStore® Adaptable Modular Storage and Workgroup Modular Storage Storage Navigator Modular (for GUI) User's Guide* (MK-95DF711)

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 Password Protection

This chapter covers the following topics:

- Overview (section 1.1)
- Specifications (section 1.2)

1.1 Overview

Password Protection enables the user to restrict access to the Hitachi TagmaStore® AMS/WMS subsystem. Access to the subsystem is restricted to registered users only, and only one user at a time can be logged in to the subsystem to prevent concurrent access.

Storage Navigator Modular is used to register users and specify a user ID and password for each user. When a user logs in, the TagmaStore AMS/WMS refers to the registered user IDs and passwords and rejects a login attempt by an unregistered user. When a registered user is logged in, the TagmaStore AMS/WMS rejects login attempts by other users.

Figure 1.1 illustrates the Password Protection function:

- User X is a registered user for TagmaStore AMS/WMS subsystems A and B. An attempt by User X to log in to TagmaStore AMS/WMS subsystem C, D, or E will be rejected.
- User Y is a registered user for TagmaStore AMS/WMS subsystems C and D. An attempt by User Y to log in to TagmaStore AMS/WMS subsystem A, B, or E will be rejected.
- User Z is a registered user for TagmaStore AMS/WMS subsystem E. An attempt by User Z to log in to TagmaStore AMS/WMS subsystem A, B, or C will be rejected.

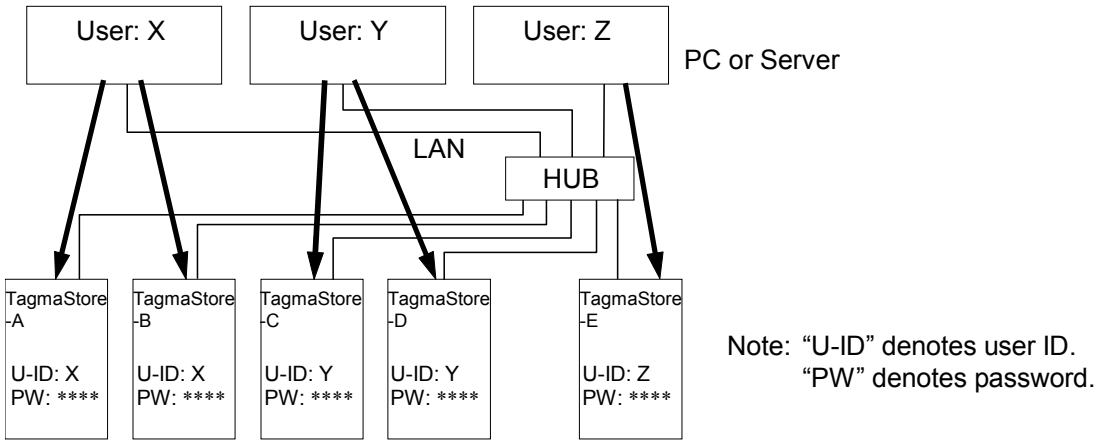


Figure 1.1 Password Protection Control Feature

1.2 Specifications

Table 1.1 lists and describes the Password Protection specifications.

Note: Be sure to assign user IDs and passwords for any service personnel who may need to work on the subsystems.

Table 1.1 Password Protection Specifications

Function	Specification
Register user IDs and passwords to prevent unauthorized access.	Up to 20 sets of user IDs and passwords can be registered for one Hitachi TagmaStore™ from the Navigator. Login attempts by a user of Navigator whose user ID and password are not registered are rejected. (See ***Note***)
Reject concurrent access by users.	The Hitachi TagmaStore AMS/WMS will reject any concurrent login attempted by other users, if a Navigator user whose user ID and password have been registered, is logged in. Even if the concurrent user's ID and password have been registered, that user will not be able to log in until the first user has logged out. An error message issued by Navigator will clarify whether the login is rejected due to non-registration of a user ID and password, or is due to a concurrent login attempt.

Chapter 2 Installing and Uninstalling Password Protection Using Storage Navigator

This chapter provides instructions for installing and uninstalling Password Protection using the GUI version of the Storage Navigator Modular. This chapter includes the following:

- Installation (section 2.1)
- Uninstalling Password Protection (section 2.2)
- Enabling and Disabling Password Protection Using the GUI (section 2.3)

The Password Protection feature is usually unselectable (locked); to make it available, you must install the Password Protection 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 in section 2.1to install the Password Protection feature. Password Protection is installed and uninstalled using Navigator.

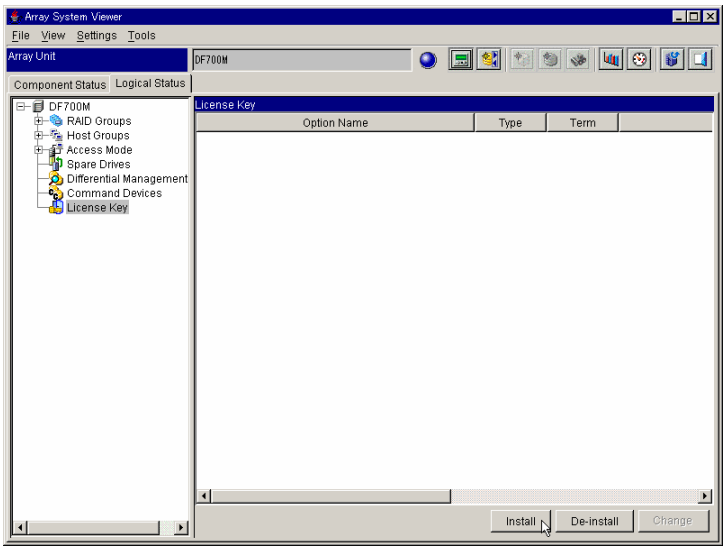
Note: Installing, uninstalling, enabling, and disabling of the Password Protection feature are set for each disk array subsystem.

Note: 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.

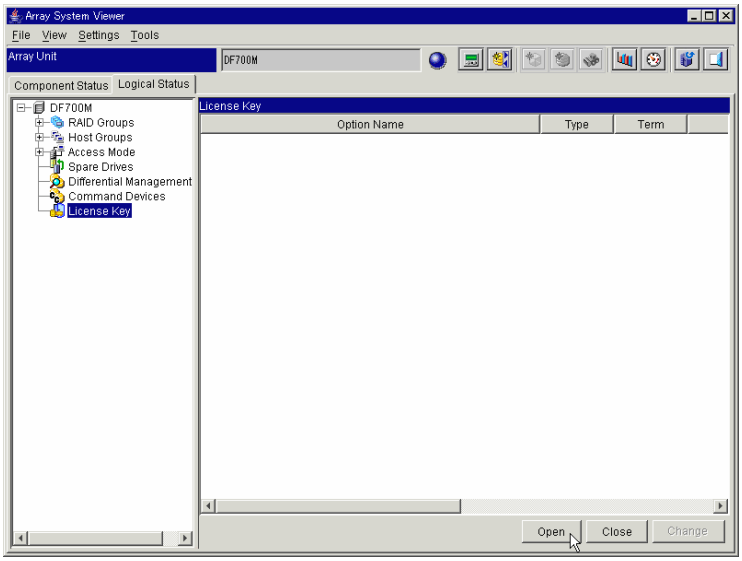
2.1 Installation

To install Password Protection using Navigator (GUI):

1. Start Navigator and change the mode of operation to **Management Mode**. For details on this procedure, please refer to the *Hitachi TagmaStore AMS/WMS Storage Navigator Modular (for GUI) User's Guide* (MK-95DF711).
2. Register the subsystem in which you will install Password Protection. Connect to this subsystem to access the **Array System Viewer** window as shown in Figure 2.1.



Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0

Figure 2.1 Array System Viewer Window (Logical Status Page)

3. Click the **Logical Status** tab.

Click the **License Key** icon, and then click **Install**. The **Install Options** dialog box is displayed. (version 5.00 or later)

Click the **License Key** icon, and then click **Open**. The **Unlock Options** dialog box is displayed. (versions earlier than 5.0)

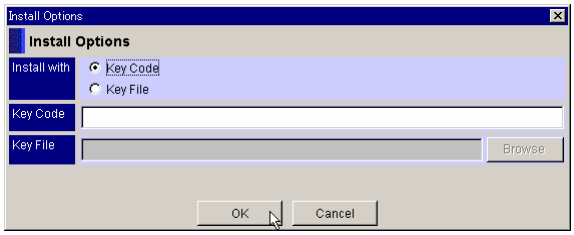


Figure 2.2 Install Options Dialog Storage Navigator

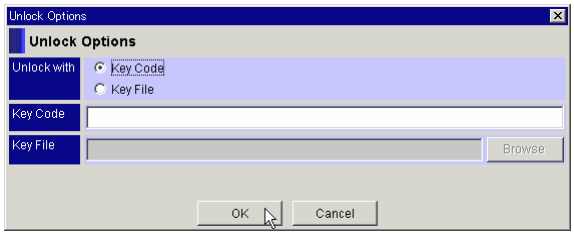
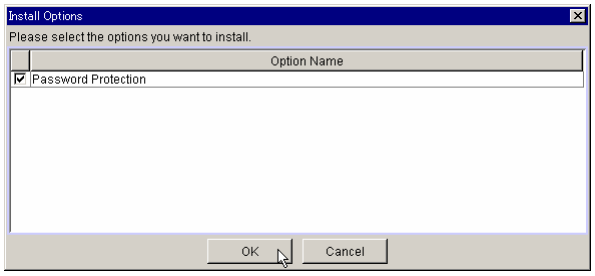


Figure 2.3 Unlock Options Dialog Storage Navigator

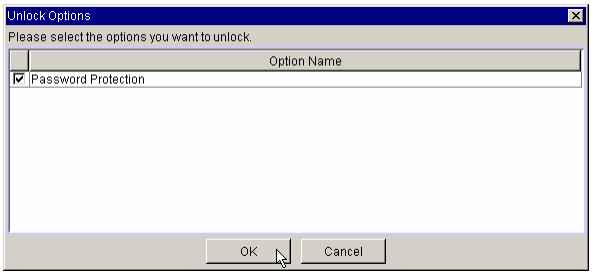
4. When you install the option using the key code, click the **Key Code** radio button, and then set up the key code. When you install the options using the key file, click the **Key File** radio button, then set up the path for the key file and click **OK**.

   Browse can be used to set the path to a key file correctly.

5. Use the file key to install the options. The options selection dialog is displayed make sure the **Option Name** is selected and click **OK**.



Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0

Figure 2.4 Options Selection Dialog

6. A message appears, confirming that this feature is installed. Click **OK**.

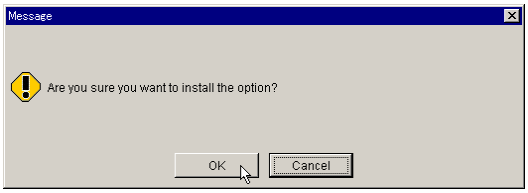
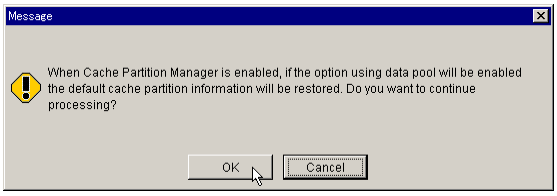
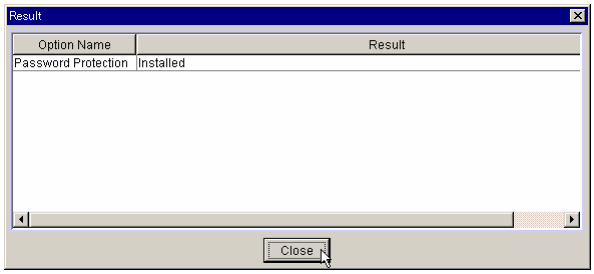


Figure 2.5 Confirmation

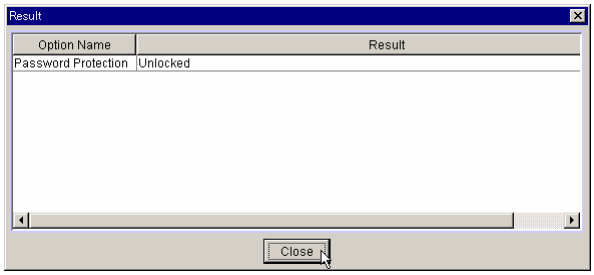
When Navigator version is 3.00 or later and Cache Partition Manager is enabled, the following message is displayed. Since Password Protection does not use the data pool, click the OK button at this point without doing anything else.



7. Use the key file to install the options. The **Result** dialog box is displayed. Click **Close**. The window is updated and then displayed.

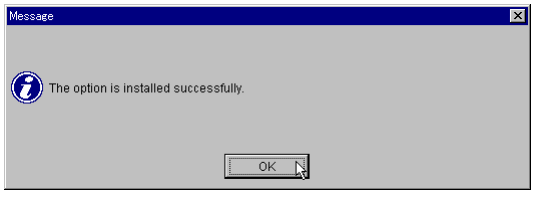


Storage Navigator version 5.00 or later

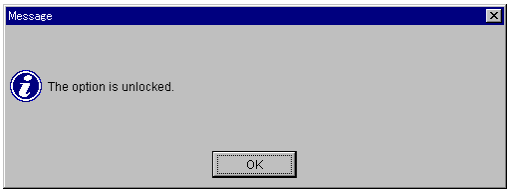


Storage Navigator versions earlier than 5.0

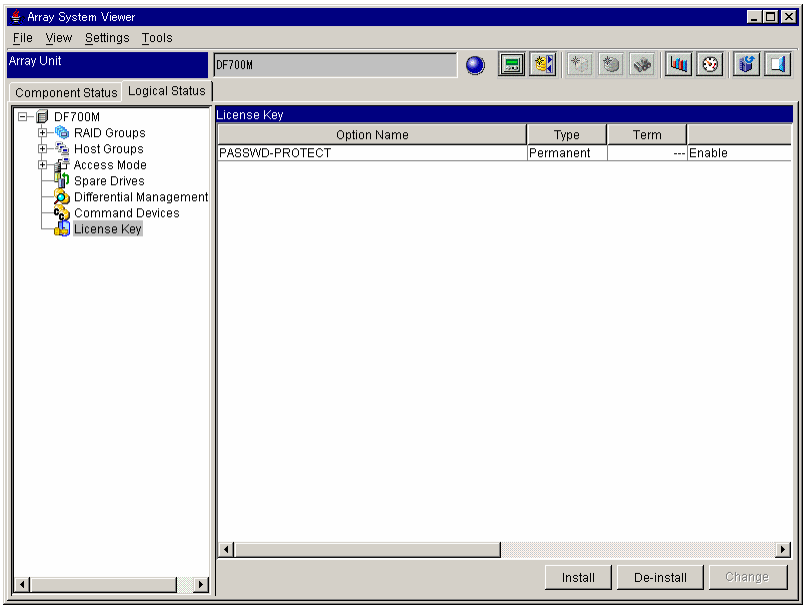
Figure 2.6 Result Dialog Box



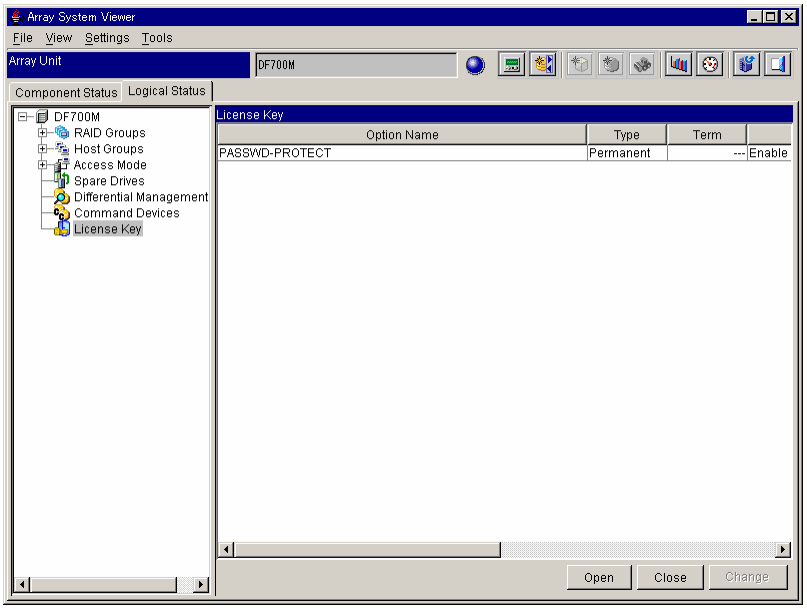
Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0



Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0

Figure 2.7 Array System Viewer Window (Logical Status Page: Option Enable)

2.2 Uninstalling Password Protection

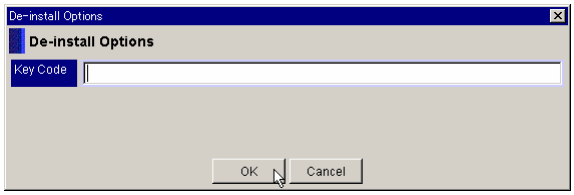
Follow the instructions below to uninstall Password Protection. When it is uninstalled, the Password Protection is not available (locked) until it is installed by the key code or key file.

To uninstall Password Protection, the key code or key file provided with the Password Protection feature is required.

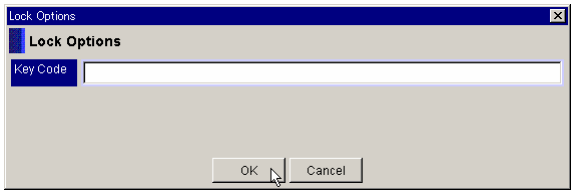
To uninstall Password Protection:

1. Start Navigator and change the mode of operation to **Management Mode**.
2. Register the subsystem in which you will uninstall Password Protection. Connect to this subsystem; the following window is displayed.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon, and click **De-install**. The **De-install Options** dialog box is displayed. (Storage Navigator version 5.00 or later)

   Click the **License Key** icon, and click **Close**. The **Lock Options** dialog box is displayed. (Storage Navigator versions earlier than 5.0)



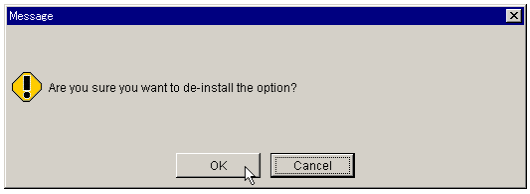
Storage Navigator version 5.00 or later



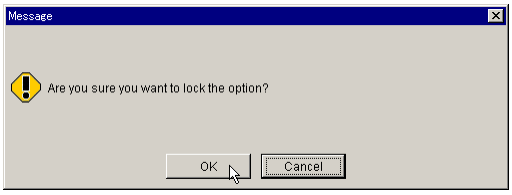
Storage Navigator versions earlier than 5.0

Figure 2.8 De-install/Lock Options Dialog Box

5. Enter a key code in the text box and click **OK**.
6. The following window appears, requesting a confirmation to uninstall the Password Protection option (Figure 2.9). Click **OK**.



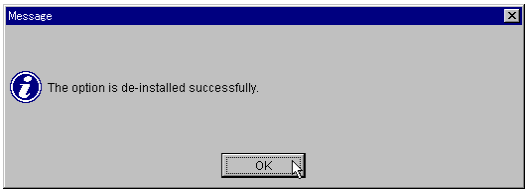
Storage Navigator version 5.00 or later



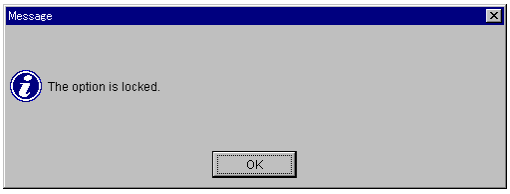
Storage Navigator versions earlier than 5.0

Figure 2.9 Confirmation to Uninstall window

7. The following message appears. To confirm that this feature has been uninstalled (Figure 2.10), click **OK**.



Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0

Figure 2.10 Confirmation of De-install/Lock

8. The **Array System Viewer** window is updated and then displayed. (Refer to Figure 2.1)

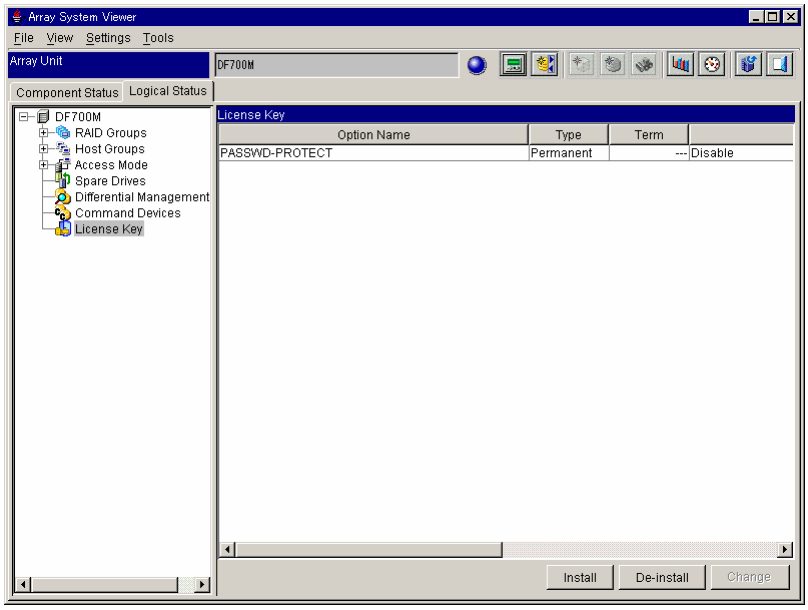
2.3 Enabling and Disabling Password Protection Using the GUI

To enable and disable Password Protection:

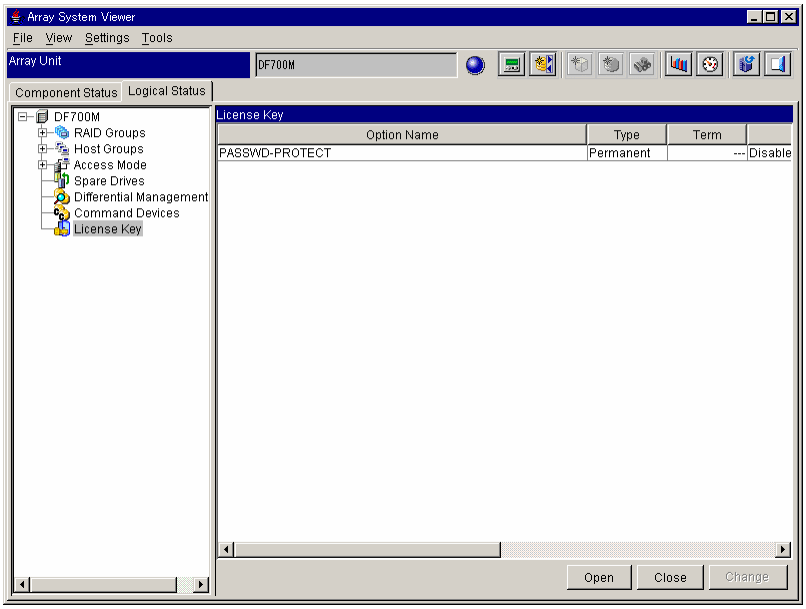
1. Start Navigator and change the mode of operation to **Management Mode**.
2. Select the subsystem you want to set **Password Protection** on. Connect to this unit, and the corresponding unit will display.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.
5. Click on **PASSWD-PROTECT** in the **Option List** text box, and then click **Change**.
6. The following message appears. To confirm that this option is set, click **OK**.

Figure 2.11 Confirmation Panel

The window is updated and then displayed.



Storage Navigator version 5.00 or later



Storage Navigator versions earlier than 5.0

Figure 2.12 Array System Viewer Window (Logical Status Page: Option Disable)

Chapter 3 Setting Security Information Using Navigator (GUI)

This chapter describes how to change and delete user IDs, change passwords, log in and log out. This chapter is divided into the following sections:

- Setting Protection Information (section 3.1)
- Changing the User ID (GUI) (section 3.2)
- Deleting the User ID (GUI) (section 3.3)
- Changing the Password (GUI) (section 3.4)
- Logging in and Logging Out (section 3.5)

3.1 Setting Protection Information

To set the user ID and password:

1. Start Navigator and change the mode of operation to **Management Mode**.
2. Register the subsystem in which you will set Password Protection Information. Connect to this registered subsystem; the **Array System Viewer** window will be displayed.

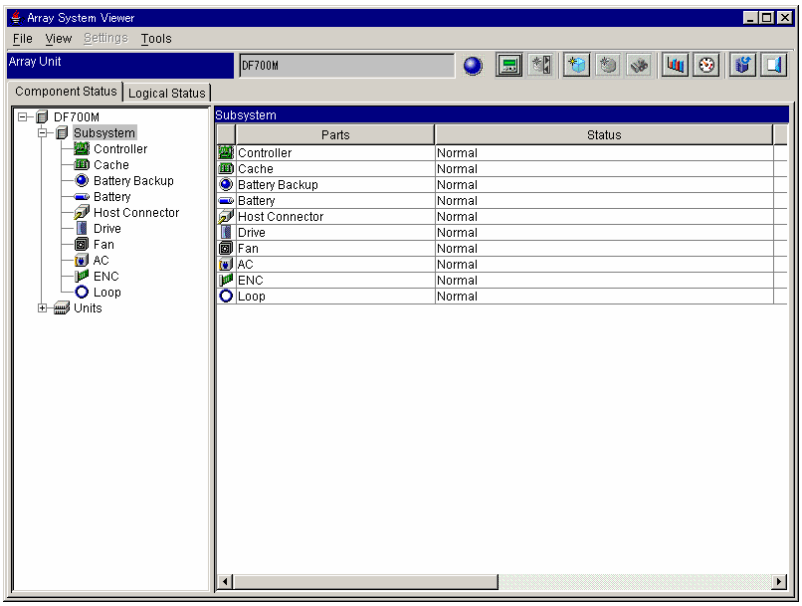


Figure 3.1 Array System Viewer Window (Component Status Page)

3. From the **Settings** menu, select **Configuration Settings**.

   Alternatively, from the tool bar, click the **Configuration Settings** () button. The **Configuration Settings** window is displayed.

   The **Configuration Settings** window is displayed (Figure 3.2).

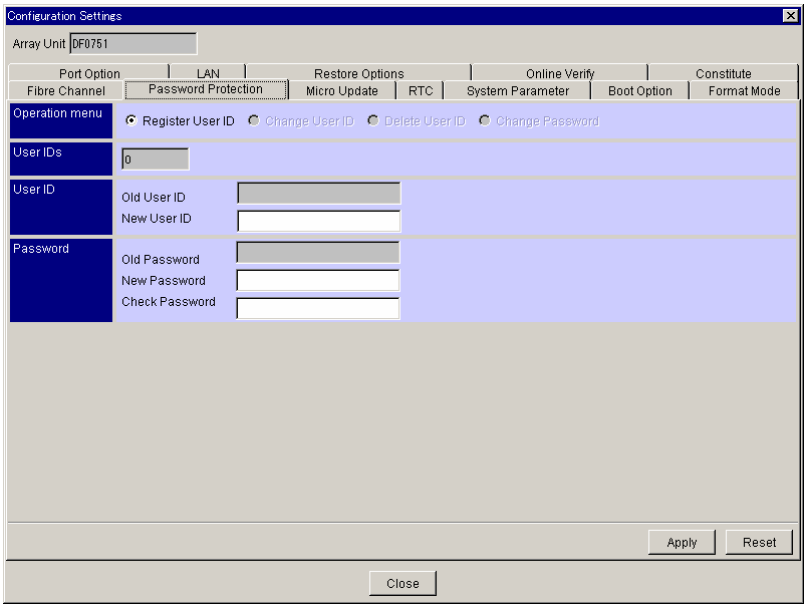


Figure 3.2 Configuration Settings Window (Password Protection Page)

4. From the **Operation menu**, click the **Register User ID** radio button. Enter data as follows:
   - In the **New User ID** field, specify a user ID to register. The new user ID must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - In the **New Password** field, specify the user ID password to register. The new user password must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - In the **Check Password** field, specify the new password again to confirm.
   - Click **Apply** when done.
5. Verify the new information, and click **OK**. The new user ID information is updated and displayed. A confirmation window appears (Figure 3.3).

   The number of registered user IDs is updated and displayed.

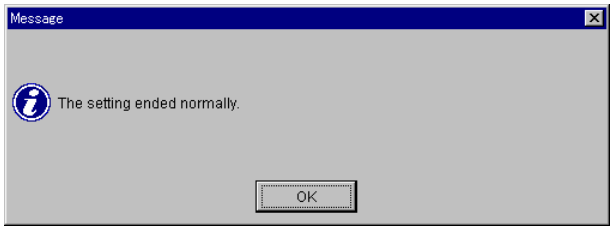


Figure 3.3 Confirmation Window

3.2 Changing the User ID (GUI)

To change an existing user ID:

1. From the **Settings menu**, select **Configuration Settings**. Alternatively, click the **Configuration Settings** ( ) button from the toolbar. The **Configuration Settings** window is displayed as shown in Figure 3.4.
2. Click the **Password Protection** tab.

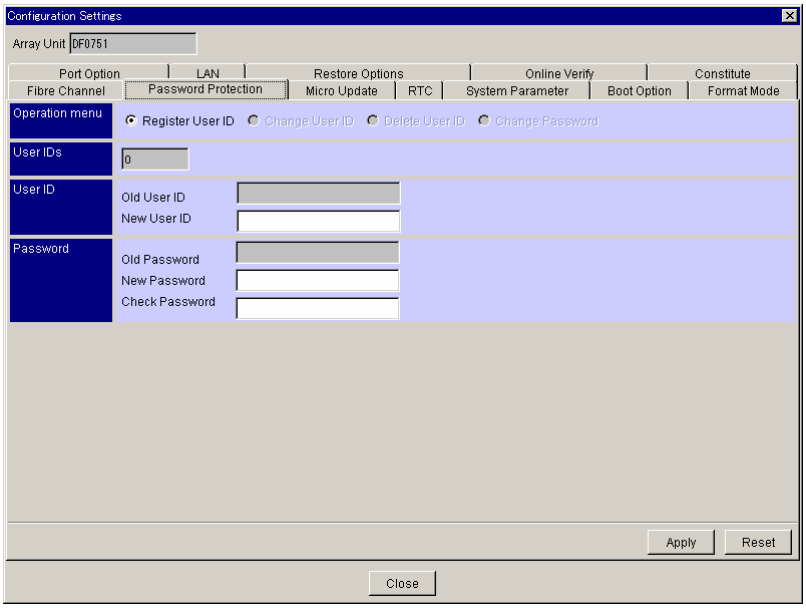


Figure 3.4 Configuration Settings Window (Password Protection Tab)

3. From the **Operation menu**, click the **Register User ID** radio button. Enter data as follows:
   - In the **Old User ID** field, specify a user ID to change.
   - In the **New User ID** field, specify a user ID to register. The new user ID must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - **Old Password**: Specifies the password of a user ID to change.
   - **New Password**: Specifies the password of a user ID to register. The new password must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - **Check Password**: Specifies the same password as that of a user ID to register. The new user ID must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - Click **Apply** when done.
4. A message appears, confirming that the registration is complete. Click **OK**.

3.3 Deleting the User ID (GUI)

The GUI operation to change the User ID already registered with Navigator is as follows.

1. From the **Settings menu**, select **Configuration Settings**. Alternatively, from the tool bar, click the **Configuration Settings** () button.

   The **Configuration Settings** window is displayed as shown in Figure 3.4.

2. Click the **Password Protection** tab.
3. From the **Operation** menu, click the **Delete User ID** radio button. Enter data as follows:
   - In the **Old User ID** field, specify a user ID to delete.
   - In the **Old Password** field, specify the password of a user ID to delete.
   - Click **Apply**.
4. A message appears, confirming that the registration is complete. Click **OK**. The number of registered user IDs is updated and displayed.

3.4 Changing the Password (GUI)

The GUI operation to change the password of a User ID already registered with Navigator is as follows.

1. From the **Settings menu**, select **Configuration Settings**. Alternatively, click the **Configuration Settings** () button from the toolbar.

   The **Configuration Settings** window is displayed (Figure 3.4).

2. Click the **Password Protection** tab.
3. From the **Operation menu**, click the **Change Password** radio button. Enter the data as follows:
   - In the **Old User ID** field, specify a user ID to change.
   - In the **Old Password** field, specify the password of a user ID to change.
   - **New Password:** Specifies the password of a user ID to register. The new password must consist of 4–12 alphanumeric characters and may include - (minus) or _ (underline) signs.
   - **Check Password:** Specifies the same password as that of a user ID to register.
   - Click **Apply**.
4. A message appears, confirming that the registration is complete. Click **OK**.

3.5 Logging In and Logging Out

This section explains how to log in and log out using the GUI version of Storage Navigator Modular. Management of operators by user ID is effective when operating Navigator in Management mode. When operating Navigator in **Monitor Mode**, Navigator may be operated regardless of whether a user ID has been registered or not.

3.5.1 Logging In

To log in:

1. Set the mode of operation to **Management Mode**.
2. In the Main window, double-click the icon for the subsystem to be connected.
3. In the **Login** window, enter a registered user ID and corresponding password. Click **OK**.

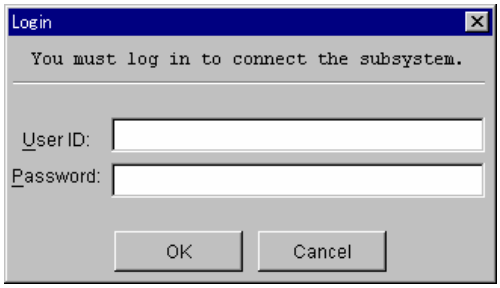


Figure 3.5 Login Dialog Box

4. Log in with the registered user ID. The **Array System Viewer** window is displayed. (Refer to Figure 3.1).
5. Double-click the icon of a subsystem to which a user has already logged in. A message appears, confirming that a user has already logged in.

   The message indicates the user ID of the logged-in user and connection information.
6. Click **OK**, and then login again. The following message appears:

7. Click **OK**.

3.5.2 Logging Out

To log out: From the **Mode** pull-down menu, click **Exit**. Alternatively, click the **Exit** () button on the **Array System Viewer** window. (Refer to Figure 3.1).

3.5.3 Logging Out a User and Logging in Another

To log out a user from a subsystem and replace that user with another registered one.

1. Double-click the icon of a subsystem to which a user has already logged in. A message appears, confirming that a user has already logged in.

   The message indicates the user ID of the logged-in user and connection information.

   The following message displays while operating in the **Array System Viewer** window:

   A user ID with which a user has logged in and connection information are not displayed.

2. Close the **Array System Viewer** window, and then open it again. Check the user ID of the user who has logged in.

3. Terminate Navigator, and then restart it by appending the **-discon** as illustrated in the following examples.

   – If using Windows, Add the **-discon** option by editing the description contents of `startsnm.bat` (a batch file used to start the Navigator).

   Example:

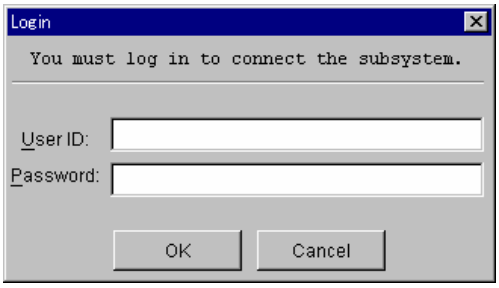
```
java -classpath .\stonavm.jar jp.co.hitachi.str.diskarray.gui.ConmanFrame -discon
```

   – If using Solaris, start the Navigator by appending the **-discon** option when starting.

   Example:

```
. / startsnm -discon
```

4. Next, log in by completing the following steps:
   - Restart the Navigator from startsnm.bat, and set the mode of operation to **Management Mode**.
   - Double-click the icon of the subsystem to be connected on the Main window.
   - Enter a registered user ID and their password. Click **OK**.



5. A user ID and a related password are displayed. When logging in forcibly, click **OK**.

   Logging in with the entered user ID is completed. The **Array System Viewer** window is displayed.

Appendix A Operations Using Storage Navigator Modular (CLI)

In addition to performing Password Protection operations using the GUI, you may also perform these operations using the Storage Navigator Modular command line interface (CLI).

To use the Password Protection feature, you must first install it to make its functions selectable (unlocked). To install this function, the key code or key file is required.

Note: 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.

This appendix is divided into the following sections:

- Installing Password Protection (section A.1)
- Uninstalling Password Protection (section A.2)
- Enabling/Disabling Password Protection (section A.3)
- Setting Protection Information (section A.4)
- Changing the User ID (section A.5)
- Deleting the User ID (section A.6)
- Changing the Password (section A.7)
- Logging In and Logging Out (section A.8)
  - Logging In (section A.8.1)
  - Logging Out (section A.8.2)
  - Logging In Manually (section A.8.3)
  - Checking Login (section A.8.4)

A.1 Installing Password Protection

The Password Protection feature is usually unselectable (locked). To make it available, you must install the Password Protection 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 Password Protection feature. Password Protection is installed and uninstalled using Navigator.

Note: 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.

To install Password Protection using the CLI version of Navigator:

1. From the command prompt, register the subsystem in which you will install the Password Protection feature. Connect to the selected subsystem.
2. Install the optional features by using the Key code as shown in the following examples:

   To install (unlock) with the key code, see the following examples:

   Example:

   Navigator version is 5.00 or later and 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
enabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

   Navigator versions earlier than 5.0 and Cache Partition Manager is enabled

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

   Navigator version is less than 3.00 and Cache Partition Manager is enabled

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

   Example:

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

A.2 Uninstalling Password Protection

To uninstall Password Protection using the CLI version of Navigator:

1. From the command prompt, register the subsystem in which you will uninstall the Password Protection feature. Connect to the selected subsystem.
2. Uninstall the optional features by using one of the following examples:

Example:

Storage Navigator version 5.00 or later

```
% 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.
%
```

Storage Navigator versions earlier than 5.0

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

Example:

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

A.3 Enabling/Disabling Password Protection

Password Protection can be enabled or disabled without uninstalling it. To enable or disable Password Protection without uninstalling it using the CLI version of Navigator:

1. From the command prompt, register the subsystem in which you want to change the status of the Password Protection feature. Connect to the selected subsystem.
2. Execute the `auopt` command to change the status (enable or disable). See the following examples:

   Example:

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

   Example:

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

A.4 Setting Protection Information

To set the user ID and password:

1. From the command prompt, register the subsystem in which you want to set Password Protection information. Connect to the selected subsystem.
2. Execute the `auuidadd` command to specify the subsystem. See the following example:

   Example:

```
% auuidadd -unit subsystem-name
Password: manager-password
User ID for array unit: (User ID to set)
Password for array unit: (Password of a user ID to set)
Retype Password for array unit: (Same password as that of a user ID to set)
Number of registered User ID: n
%
```

3. Specify the number of the registered users to be displayed as shown in this example:

   Example:

```
% auuidadd -unit subsystem-name –num
Password: manager-password
Number of registered User ID: n
%
```

   - **User ID**: Specifies a user ID to register. Specified with alphanumeric, special symbols - (minus) or _ (underline) of 4–12 characters.
   - **Password**: Specifies the password of a user ID to register. Specified with alphanumeric, special symbols - (minus) or _ (underline) of 4–12 characters long.
   - **Retype Password**: Specifies the same password as that of a user ID to register. Specified with alphanumeric, special symbols - (minus) or _ (underline) of 4–12 characters long.

A.5 Changing a User ID

To change a registered user ID, type the following:

Example:

```
% auuidchg –unit subsystem-name
Password: manager-password
Old User ID for array unit: (Already-set user ID)
Old Password for array unit: (Password of an already-set user ID)
New User ID for array unit: (User ID to set)
New Password for array unit: (Password of a user ID to set)
Retype New Password for array unit: (Same password as that of a user ID to set)
Number of registered User ID: n
%
```

A.6 Deleting a User ID

To delete a registered User ID, type the following:

Example:

```
% auuiddel –unit subsystem-name
Password: manager-password
User ID for array unit: (Already-set user ID)
Password for array unit: (Password of an already-set user ID)
Number of registered User ID: n
%
```

A.7 Changing a Password

To change a user password, type the following:

Example:

```
% aupwdchg –unit subsystem-name
Password: manager-password
User ID for array unit: (Already-set user ID)
Old Password for array unit: (Password of an already-set user ID)
New Password for array unit: (Password of a user ID to set)
Retype New Password for array unit: (Same password as that of a user ID to set)
Number of registered User ID: n
%
```

A.8 Logging In and Logging Out

This section explains how to log in and log out. The user must log into a subsystem with a user ID that is presently registered in that subsystem. Once a registered user is logged in, other users IDs are disabled when they attempt to log in.

When a user forcibly logs into a subsystem in which another user is presently logged into, the **-discon** option must be specified. The previous user is logged out.

A.8.1 Logging In

To log in, use the `aulogin` command as follows:

1. From the command prompt, register the subsystem in which you want to set Password Protection information. Connect to the selected subsystem.
2. Execute the `aulogin` command to specify the subsystem. See the following example:

Example:

```
% aulogin –unit subsystem-name
Password: manager-password
User ID for array unit: (Already-set user ID)
Password for array unit: (Password of an already-set user ID)
%
```

A.8.2 Logging Out

To log out, use the `aulogout` command as follows:

Example:

```
% aulogout –unit subsystem-name
Password: manager-password
%
```

A.8.3 Logging in Manually

To log out a current user ID and then log in with another registered user ID, type the following:

Example:

```
% aulogin –unit subsystem-name –discon
Password: manager-password
User ID for array unit: (Already-set user ID)
Password for array unit: (Password of an already-set user ID)
User ID (xxxxxxxxxxxx) has been logged in.
Connected with (xxx.xxx.xxx.xxx).
Do you want to forcibly log in? (y/n[n]): y
%
```

A.8.4 Checking Login

To check the user ID and the connected unit of a user who has already logged into a subsystem, use the `auchkuid` command. This command checks the following information about the connected unit: user ID, connected subsystem.

Note: This command can only be used with a user ID of a user not currently logged in.

Example:

```
% auchkuid –unit subsystem-name
Password: manager-password
User ID (xxxxxxxxxxxx)has been logged in.
Connected with (xxx.xxx.xxx.xxx).
%
```

Acronyms and Abbreviations

AMS	Adaptable Modular Storage
CLI	command line interface
DF700	Hitachi TagmaStore AMS/WMS
GUI	graphical user interface
HDS	Hitachi Data Systems
WMS	Workgroup Modular Storage

Index