HITACHI
DATA SYSTEMS

Hitachi Freedom Storage™ Thunder 9200™

Password Protection 9200 User's Guide

© 2002 Hitachi Data Systems Corporation, ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any electronic or mechanical means, including photocopying and recording, or stored in a database or retrieval system for any purpose, without the express written permission of Hitachi Data Systems Corporation.

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products or services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements, including license agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Trademarks

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

Hitachi Freedom Storage and Thunder 9200 are trademarks of Hitachi Data Systems Corporation.

All other brand or product names are or may be registered trademarks, 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 Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-91DF555-0	June 2001	Initial Release
MK-91DF555-1	November 2001	Supersedes and replaces MK-91DF555-0
MK-91DF555-2	February 2002	Supersedes and replaces MK-91DF555-1

Source Document Revision Level

The following source document was used to produce this 9200 user guide:

- *DF-F500-WSPS Password Protection User's Guide*, Sixth Edition.

Changes in this Revision

References to the Resource Manager 9200 documents were changed to the following:

- *Hitachi Freedom Storage™ Thunder 9200™ Resource Manager 9200 User's Guide Command Line Interface (CLI)* (MK-92DF574)
- *Hitachi Freedom Storage™ Thunder 9200™ Resource Manager 9200 User's Guide Graphical User Interface (GUI)* (MK-92DF575)

Preface

Password Protection 9200 is installed on your Thunder 9200 disk array unit. Before using Password Protection 9200, read the operating procedures and notices included in this guide. Carefully follow the safety precautions and instructions.

The *Hitachi Freedom Storage™ Thunder 9200™ Password Protection 9200 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 Freedom Storage™ Thunder 9200™ array subsystem.

For further information on Hitachi Data Systems products and services, please contact your Hitachi Data Systems account team, or visit the Hitachi Data Systems worldwide web site at http://www.hds.com. For specific information on the supported host systems and platforms for the 9200, please refer to the user documentation for the product, or contact the vendor's customer support service.

Note: The term "9200" refers to the Hitachi Thunder 9200™ subsystem, unless otherwise noted. Please refer to the *Hitachi Thunder 9200™ User and Reference Guide* (MK-90DF504) for further information on the 9200 disk array subsystem.

Note: The use of Password Protection 9200 and all other Hitachi Data Systems products is governed by the terms of your license agreement(s) with Hitachi Data Systems.

COMMENTS

Please send us your comments on this document: doc.comments@hds.com.

Make sure to include the document title, number, and revision.
Please refer to specific page(s) and paragraph(s) whenever possible.

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

Thank you!

Safety Precautions

Note the following when using Password Protection 9200:

- Only administrators, system engineers, and field engineers who are familiar with Hitachi Data Systems disk array units are allowed to run the Password Protection 9200 function.
- Make certain you read and fully understand this guide before you operate the Password Protection 9200 function.
- Carefully follow instructions included with the "CAUTION" label.

  Failure to follow these instructions can result in serious system damage and/or the loss of system data.

Contents

Chapter 1 Introducing Password Protection 9200 1

1.1 Specifications 2

Chapter 2 Installing and Uninstalling Password Protection 9200 (GUI) 3

2.1 Installation 3
2.2 Uninstallation 7

Chapter 3 Enabling/Disabling Password Protection 9200 (GUI) 11

Chapter 4 Setting Security Information (GUI) 15

4.1 Setting Protection Information 15
4.2 Changing the User ID 18
4.3 Deleting the User ID 19
4.4 Changing the Password 21

Chapter 5 Logging In and Logging Out (GUI) 23

5.1 Logging In 23
5.2 Logging Out 24
5.3 Logging In Forcibly 25

Chapter 6 Installing and Uninstalling Password Protection 9200 (CLI) 27

6.1 Installation 27
6.2 Uninstallation 29

Chapter 7 Enabling/Disabling Password Protection 9200 (CLI) 31

Chapter 8 Setting Security Information (CLI) 33

8.1 Setting Protection Information 33
8.2 Changing the User ID 34
8.3 Deleting the User ID 34
8.4 Changing the Password 34

Chapter 9 Logging In and Logging Out (CLI) 35

9.1 Logging In 35
9.2 Logging Out 35
9.3 Logging In Forcibly 36
9.4 Checking Login 37

List of Figures

Figure 1.1 Password Protection Control Feature 1

List of Tables

Table 1.1 Outline of Password Protection 9200 1
Table 1.2 Specifications of Password Protection 9200 2

Chapter 1 Introducing Password Protection 9200

By using Password Protection 9200, you can limit the number of Resource Manager 9200 users that are permitted to access the optional 9200. Users can also be prevented from accessing it at the same time. This can deter 9200 information from being offered to users who have no right to access and can prevent concurrent updates to 9200 configuration information by exclusively controlling the users.

To register the user, specify a user ID and a password using the Resource Manager 9200. The 9200 refers to the registered user IDs and passwords when a login is made from the Resource Manager 9200 and rejects a login made by an unregistered user. The 9200 which has been logged in by a certified user rejects another login attempted by another user.

The Password Protection 9200 feature can be installed, uninstalled, set, logged into and logged out from using either of the following versions of the Resource Manager 9200:

- Graphical User Interface (GUI): Chapters 2 through 5.
- Command Line Interface (CLI): Chapters 6 through 9.

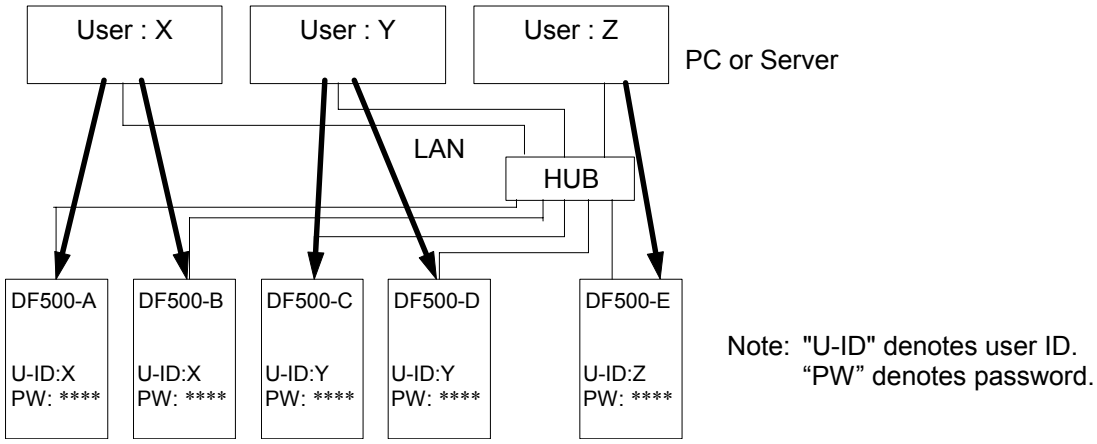


Figure 1.1 Password Protection Control Feature

The following table shows whether access by each user of Resource Manager 9200 from the example above is accepted or rejected.

Table 1.1 Outline of Password Protection 9200

9200 / User	A	B	C	D	E
X	Accepted	Accepted	Rejected	Rejected	Rejected
Y	Rejected	Rejected	Accepted	Accepted	Rejected
Z	Rejected	Rejected	Rejected	Rejected	Accepted

1.1 Specifications

Specifications of the Password Protection 9200 control feature are shown below.

Table 1.2 Specifications of Password Protection 9200

Item	Specifications
Devices which can set the feature	• SCSI and Fibre Channel interface devices can set the feature. • Only devices in which the Password Protection 9200 control feature (DF-F500-WSPS), which is a software option, is installed can set this feature.
Registration of the user ID and password and guard against access	• Up to 20 sets of a user ID and a password can be registered for one 9200 from the Resource Manager 9200. • Future login attempts by a user of Resource Manager 9200 whose user ID and password are not registered are rejected. (***Note 1***)
Rejection of concurrent logins attempted by users of Resource Manager 9200	• The 9200 which has been logged in by a user of Resource Manager 9200 whose user ID and password have been registered will reject another login attempted by another user even if its user ID and password have been registered, until the former user logs out. • An error message issued by Resource Manager 9200 will clarify whether the login is rejected due to non-registration or a result of a concurrent login attempt.

Note 1: Service personnel use the Resource Manager 9200 for maintenance of array units as well. When registering user IDs, register the user ID for service personnel.

Chapter 2 Installing and Uninstalling Password Protection 9200 (GUI)

⚠ CAUTION

The User ID and Password must be configured immediately after the software key has been installed. Please contact Hitachi Data Systems Customer Support if you lose your password and are unable to access the system.

The Password Protection 9200 option is usually unselectable (closed); to make it available, you must install Password Protection 9200 (DF-F500-WSPS) and make its functions selectable (open). **To install this function, an option FD provided with the optional feature or the key code is required.**

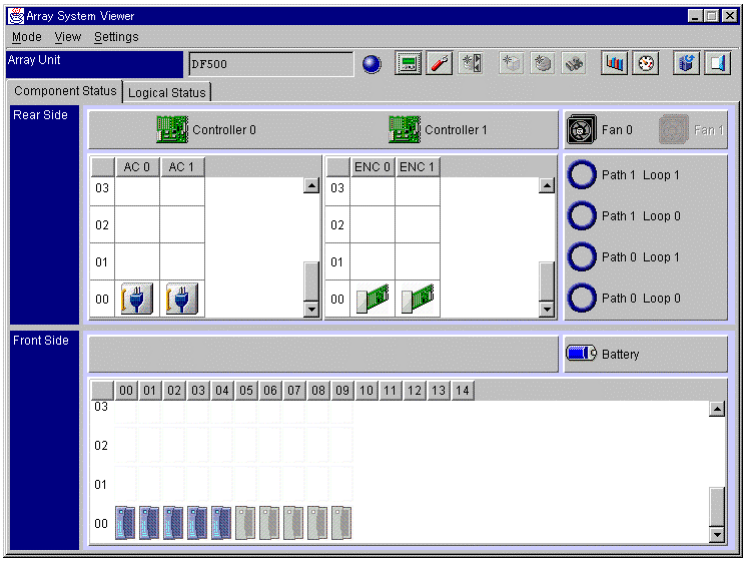
Follow the instructions below to install Password Protection 9200 (DF-F500-WSPS). Password Protection 9200 is installed and uninstalled using Resource Manager 9200. To operate the Resource Manager 9200 using a graphic interface, refer to the *Hitachi Freedom Storage™ Thunder 9200™ Resource Manager 9200 User's Guide Graphical User Interface (GUI)* (MK-92DF575).

Note: Before installing and uninstalling, make sure that the array unit 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

The following paragraphs describe installation procedures performed by using the GUI version of Resource Manager 9200.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit; the corresponding window will be displayed.

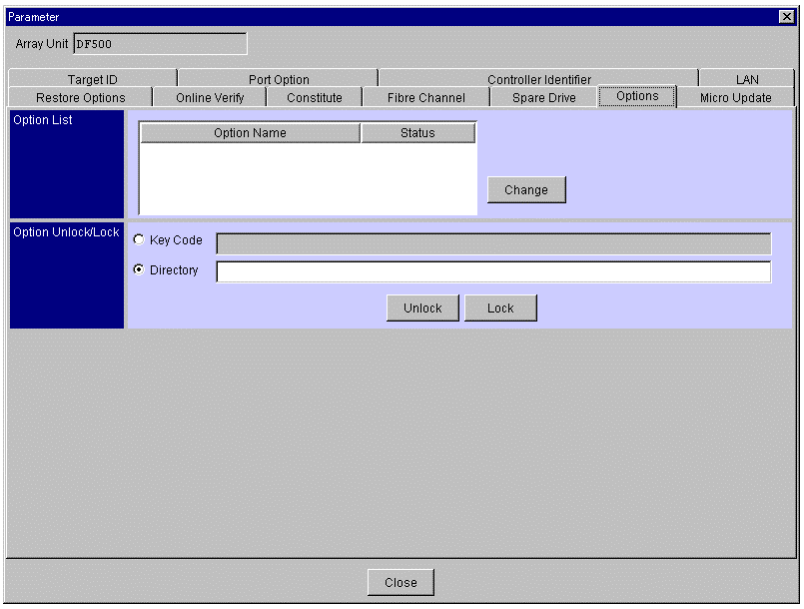


3. From the **Settings** menu, select **Configuration Settings**.

   Alternatively, from the tool bar, select the **Configuration Settings** button.

   The Parameter dialog box is displayed.

4. Click the **Option** tab.



5. Unlock the optional feature by using either of the following:
   - Password Protection 9200 Key FD
   - Key Code

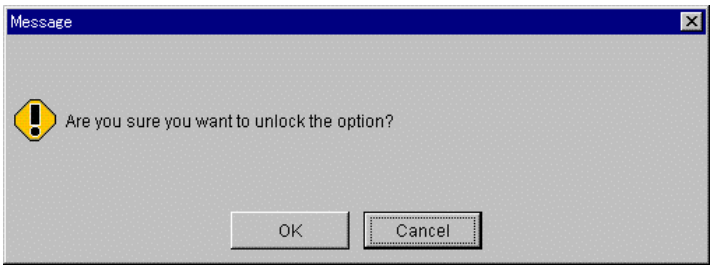
   Password Protection 9200 Key FD

   a) Insert the key FD into the FDD of the system where Resource Manager 9200 is installed.

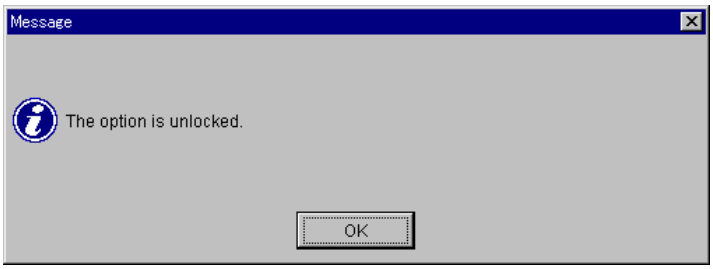
   b) Click the **Directory** radio button to enter a path to the FD.

c) Click the **Unlock** button.

d) A screen appears, requesting confirmation to unlock Password Protection 9200. Click the **OK** button.



e) A message appears, confirming that this feature is unlocked. Click the **OK** button.

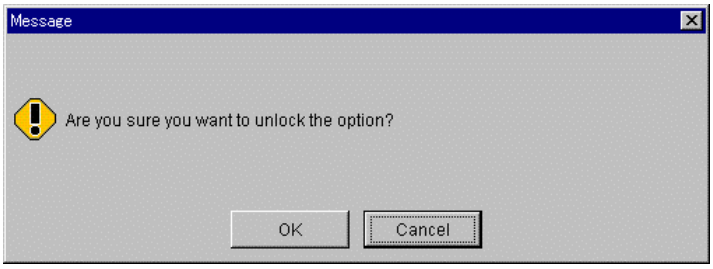


Password Protection 9200 Key Code

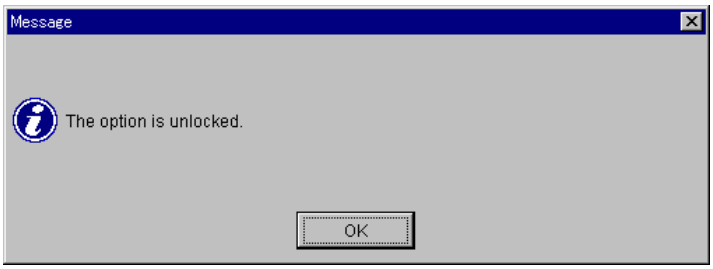
a) Click the **Key Code** radio button to enter a key code in the text box.

b) Click the **Unlock** button.

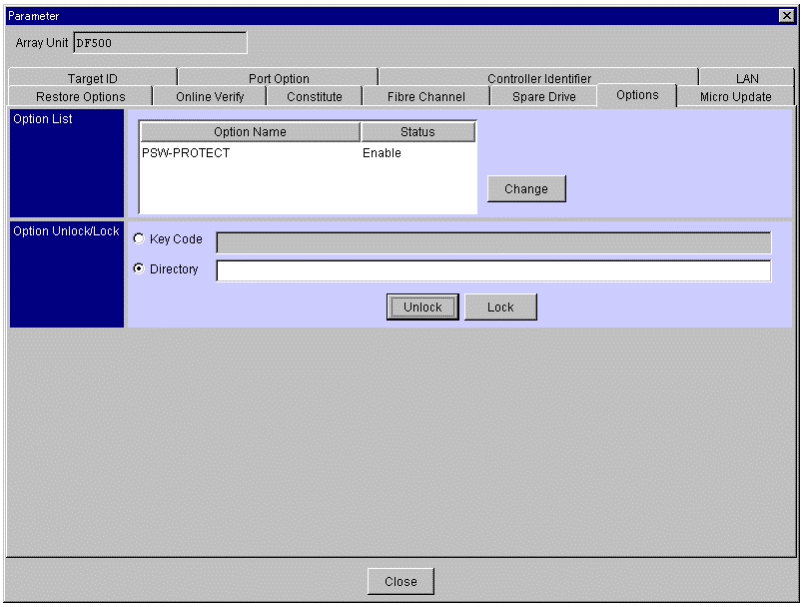
c) A screen appears, requesting a confirmation to unlock the Password Protection 9200 option. Click the **OK** button.



d) A message appears, confirming that this feature is unlocked. Click the **OK** button.



6. The window is updated and then displayed.



CAUTION **The User ID and Password must be configured immediately after the software key has been installed (see Chapter 4).** Please contact Hitachi Data Systems Customer Support if you lose your password and are unable to access the system.

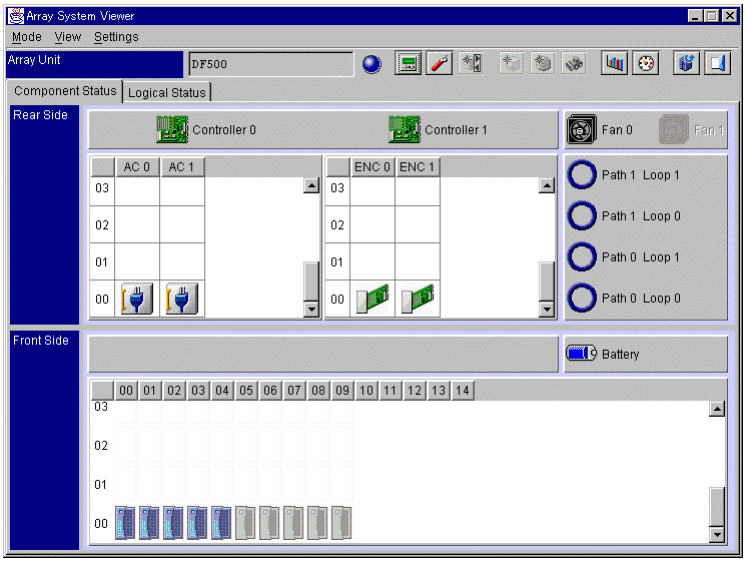
2.2 Uninstallation

Follow the instructions below to uninstall Password Protection 9200. When it is uninstalled, the Password Protection 9200 is not available (locked) until it is opened by the Option floppy disk or the key code.

To uninstall Password Protection 9200, the key FD provided with the Password Protection 9200 feature or the key code described in the key FD is required.

Follow the instructions below to uninstall Password Protection 9200 (DF-F500-WSPS).

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit; the corresponding window will be displayed.



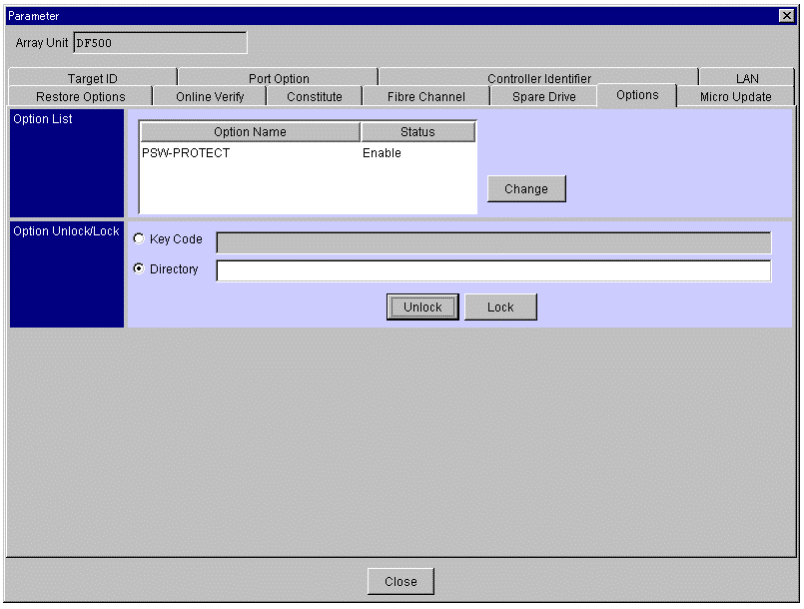
3. From the **Settings** menu, select **Configuration Settings**.

   Alternatively, from the tool bar, select the **Configuration Settings** button.

   The Parameter dialog box is displayed.

4. Click the **Parameters** button.

5. Click the **Option** tab.



6. Close (lock) the optional feature by using either of the following:
   - Password Protection 9200 Key FD
   - Key Code

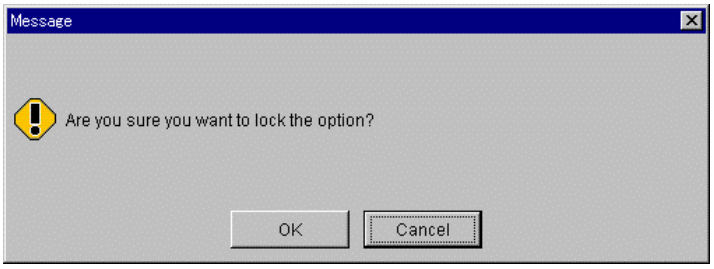
   Password Protection 9200 Key FD

   a) Insert the key FD into the FDD of the system where Resource Manager 9200 is installed.

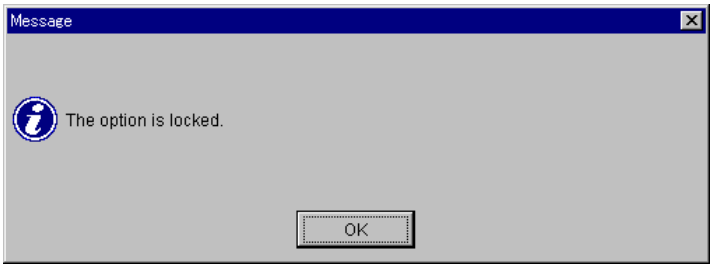
   b) Click the **Directory** radio button to enter a path to the FD.

   c) Click the **Lock** button.

   d) A screen appears, requesting a confirmation to lock the Password Protection 9200 option. Click the **OK** button.



e) A message appears, confirming that this feature is locked. Click the **OK** button.

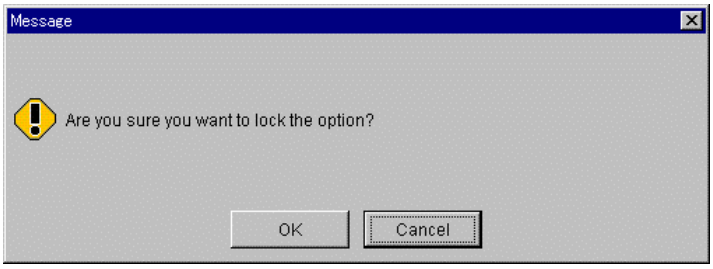


Password Protection 9200 Key Code

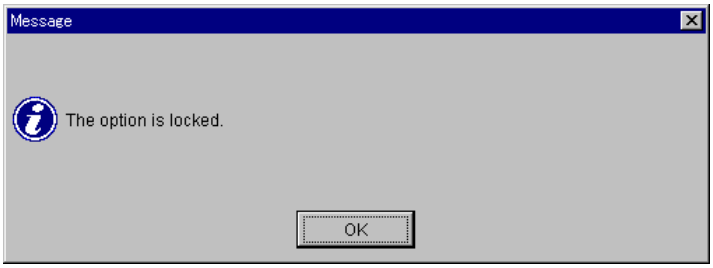
a) Click the **Key Code** radio button to enter a key code in the text box.

b) Click the **Lock** button.

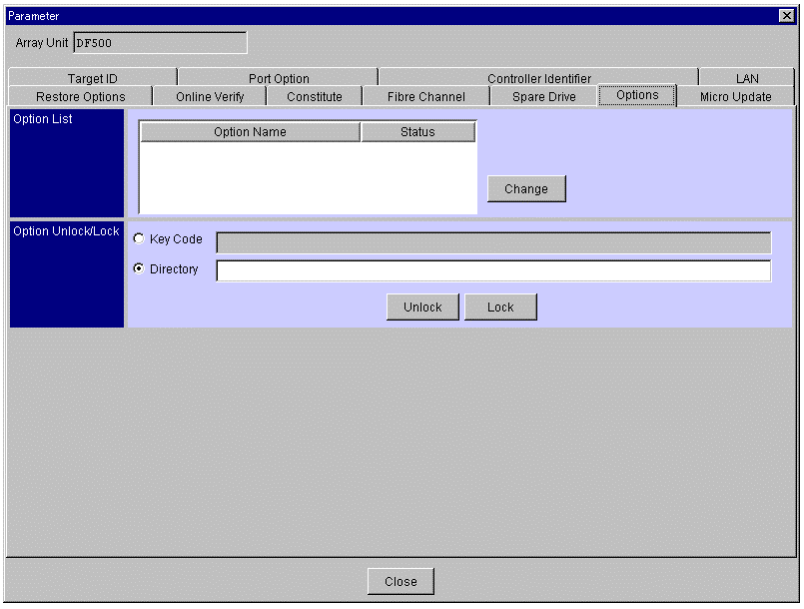
c) A screen appears, requesting a confirmation to lock the Password Protection 9200 option. Click the **OK** button.



d) A message appears, confirming that this feature has been locked. Click the **OK** button.



7. The window is updated and then displayed.



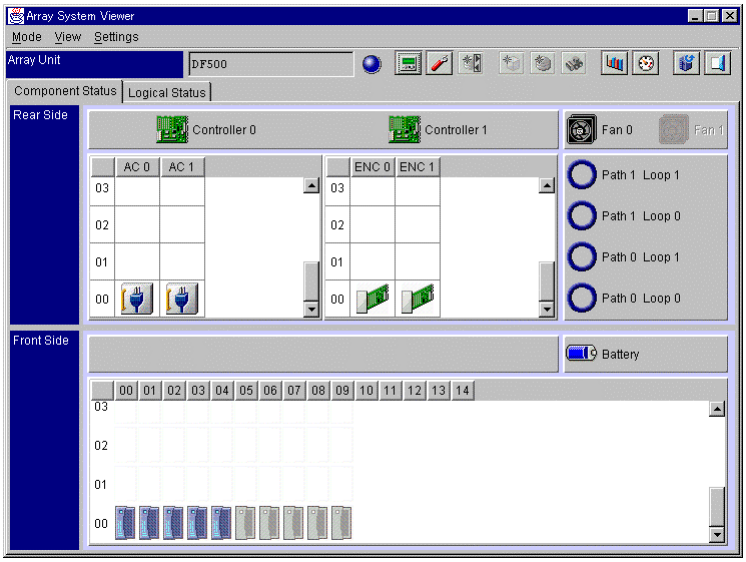
Chapter 3 Enabling/Disabling Password Protection 9200 (GUI)

The Password Protection 9200 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 Password Protection 9200 Control feature stays in an unlocked state.

These procedures can be performed by using the GUI version of Resource Manager 9200.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit; the corresponding window will be displayed.

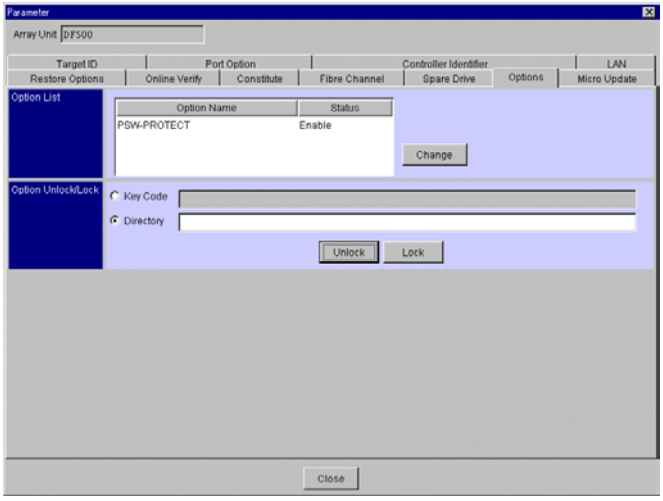


3. From the **Settings** menu, select **Configuration Settings**.

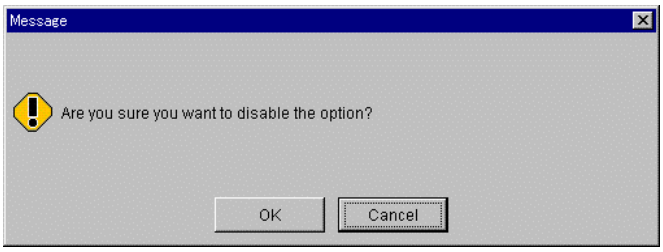
   Alternatively, from the tool bar, select the **Configuration Settings** button.

   The Parameter dialog box is displayed.

4. Click the **Option** tab.

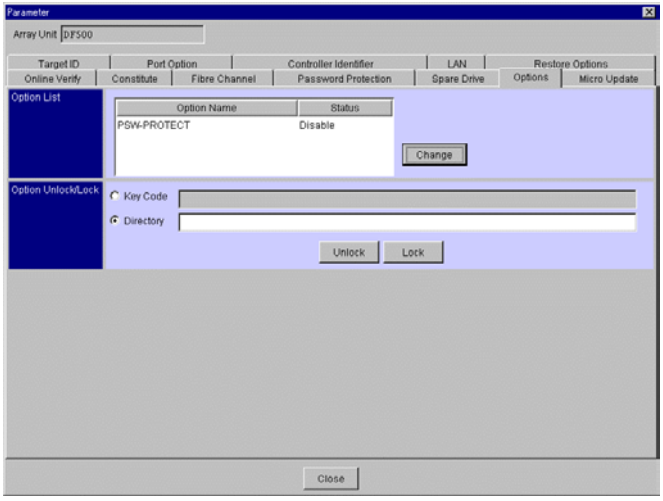


5. Click on **PSW-PROTECT** in the **Option List** text box, then click the **Change** button.



6. A message appears, confirming that this option is set. Click the **OK** button.

7. The window is updated and then displayed.



Chapter 4 Setting Security Information (GUI)

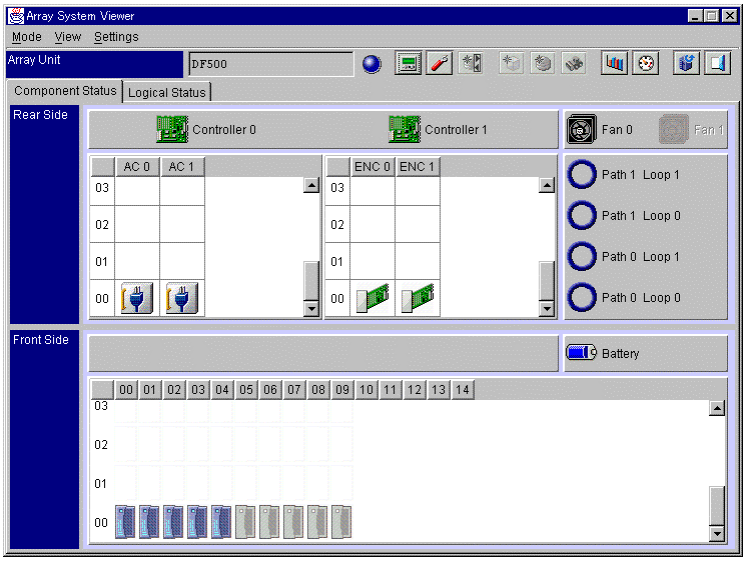
This chapter is divided into the following sections:

- Setting Protection Information
- Changing the User ID
- Deleting the User ID
- Changing the Password

4.1 Setting Protection Information

The GUI operation to set the User ID and Password with Resource Manager 9200 is as follows.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit; the corresponding window will be displayed.

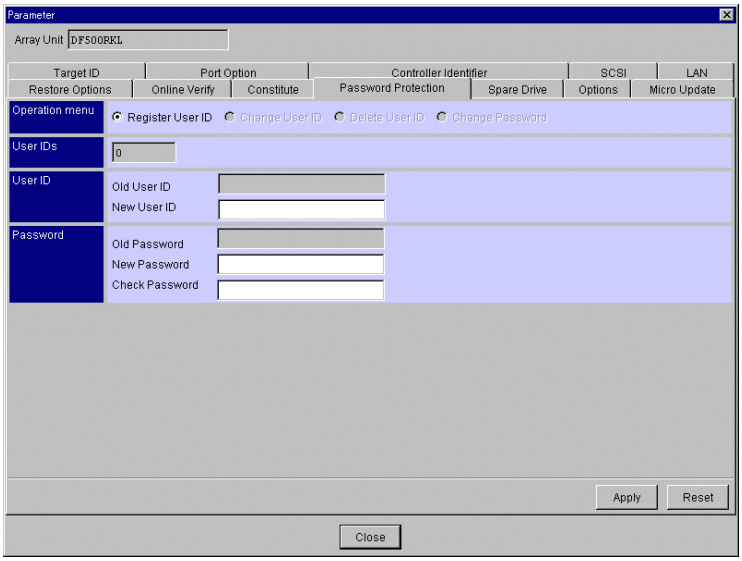


3. From the Settings menu, select Configuration Settings.

   Alternatively, from the tool bar, select the **Configuration Settings** button.

   The Parameter dialog box is displayed.

4. Click the **Password Protection** tab.



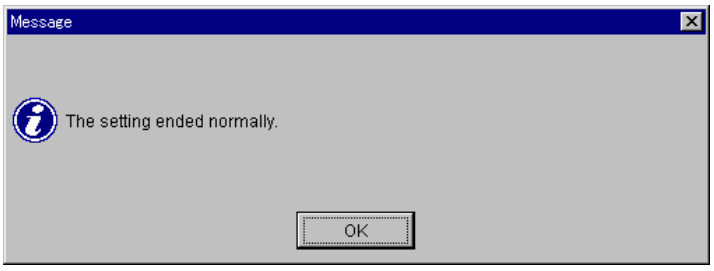
5. From the **Operation menu**, click the **Register User ID** option button. In the **New User ID**, **New Password** and **Check Password** fields, enter their respective data. Click the **Apply** button.

   This menu contains the following:

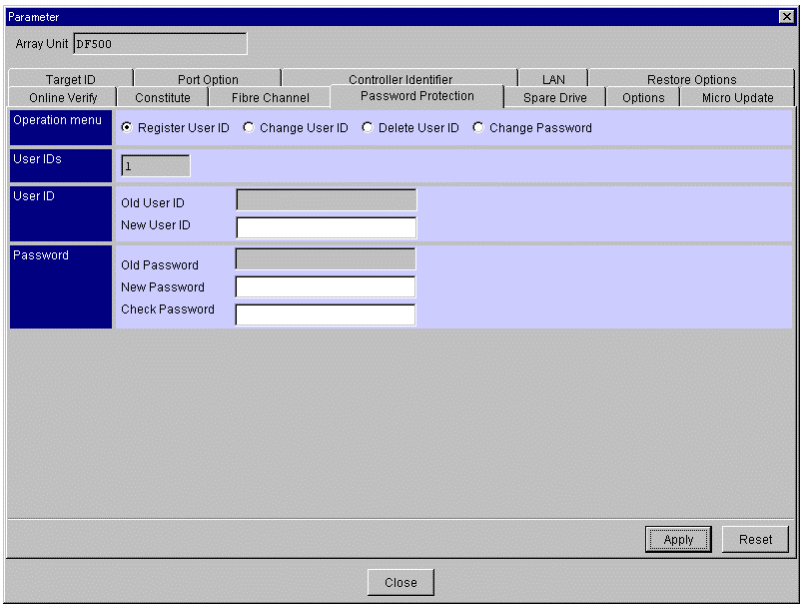
   - **New User ID:** Specifies a user ID to register. Specified with alphanumeric, special symbols **- (minus)** or **_ (underline)** of 4 to 12 characters long.
   - **New Password:** Specifies the password of a user ID to register. Specified with alphanumeric, special symbols **- (minus)** or **_ (underline)**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

   Check the settings for complete User ID and Password.

   A message appears, confirming that the registration is complete. Click the **OK** button.



The number of registered user IDs is updated, then displayed.



CAUTION

The User ID and Password must be configured immediately after the software key has been installed. Please contact Hitachi Data Systems Customer Support if you lose your password and are unable to access the system.

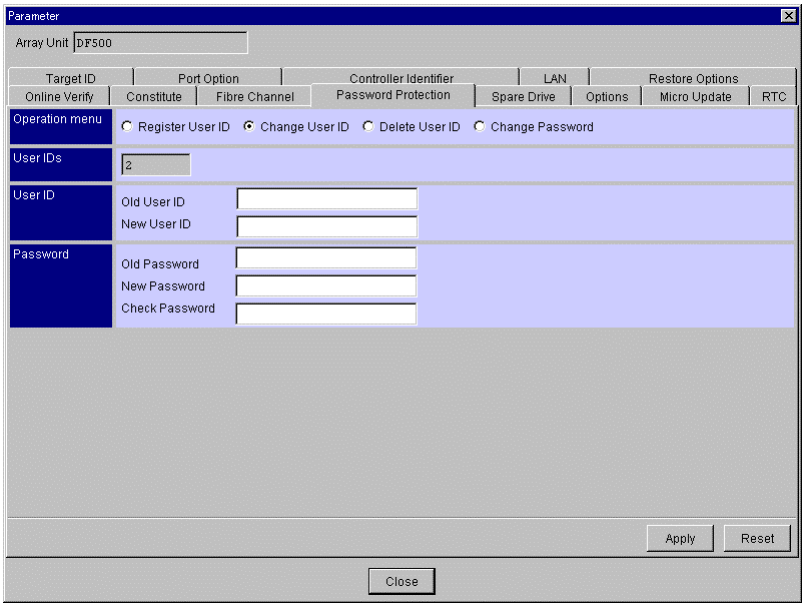
4.2 Changing the User ID

The GUI operation to change the User ID already registered with Resource Manager 9200 is as follows.

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

   The Parameter dialog box is displayed.

2. Click the **Password Protection** tab.

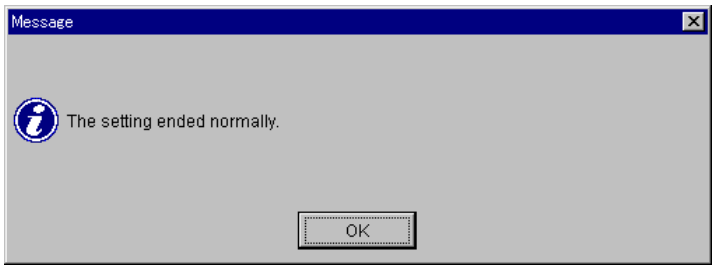


3. From the **Operation menu**, click the **Change User ID** option button. In the **Old User ID**, **New User ID**, **Old Password, New Password,** and **Check Password** fields, enter their respective data. Click the **Apply** button.

   This menu contains the following:

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

4. A message appears, confirming that the registration is complete. Click the **OK** button.



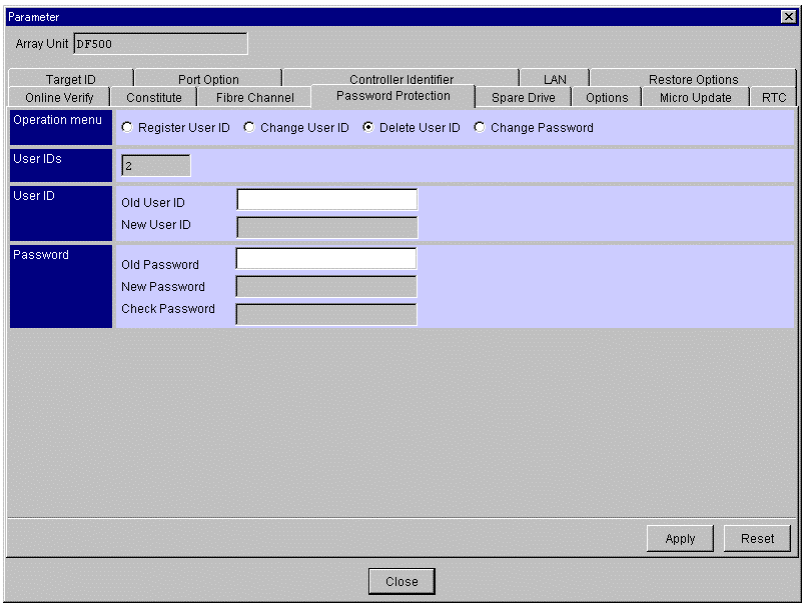
4.3 Deleting the User ID

The GUI operation to delete the User ID already registered with Resource Manager 9200 is as follows.

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

   The Parameter dialog box is displayed.

2. Click the Password Protection tab.

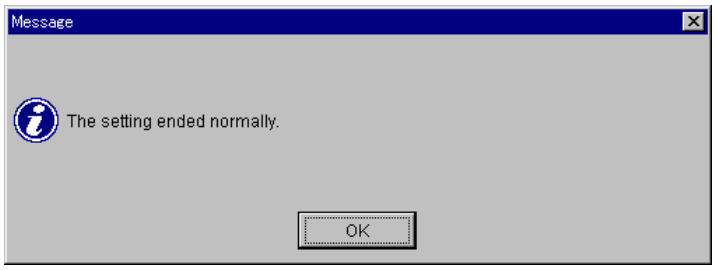


3. From the **Operation menu**, click the **Delete User ID** option button. In the **Old User ID**, **Old Password** fields, enter their respective data. Click the **Apply** button.

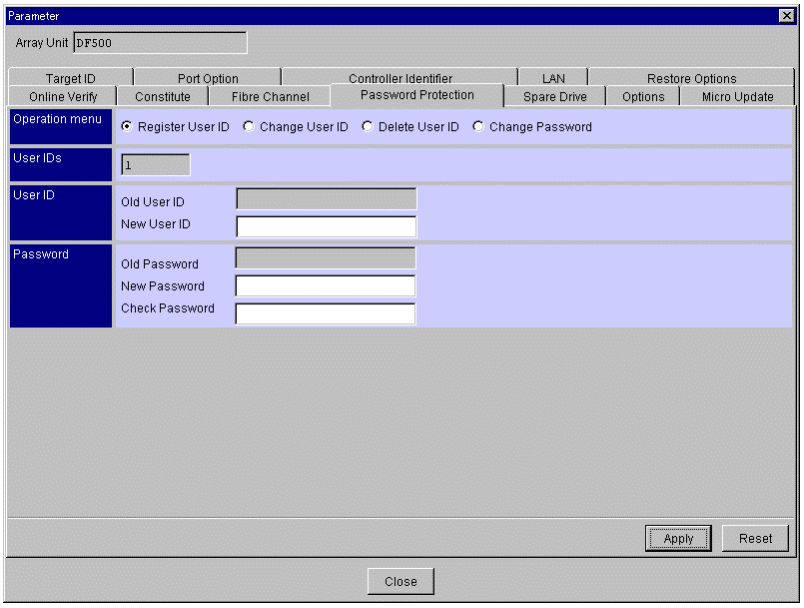
   This menu contains the following:

   - **Old User ID:** Specifies a user ID to change.
   - **Old Password:** Specifies the password of a user ID to change.

4. A message appears, confirming that the registration is complete. Click the **OK** button.



The number of registered user IDs is updated, then displayed.



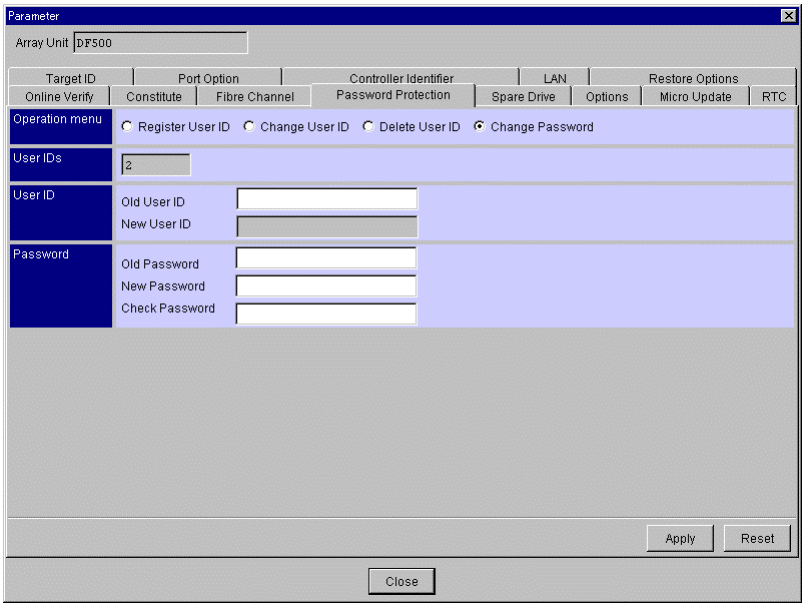
4.4 Changing the Password

The GUI operation to change the password of a User ID already registered with Resource Manager 9200 is as follows.

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

   The Parameter dialog box is displayed.

2. Click the Password Protection tab.

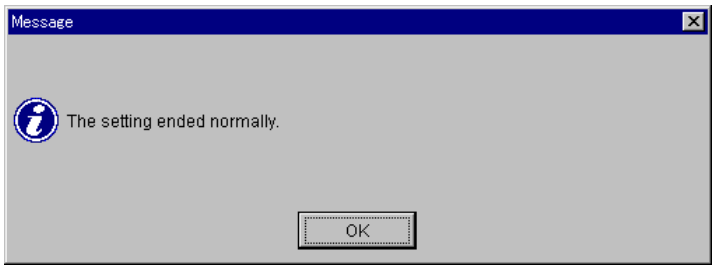


3. From the **Operation menu**, click the **Change Password** option button. In the **Old User ID**, **Old Password, New Password,** and **Check Password** fields, enter their respective data. Click the **Apply** button.

   This menu contains the following:

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

4. A message appears, confirming that the registration is complete. Click the **OK** button.

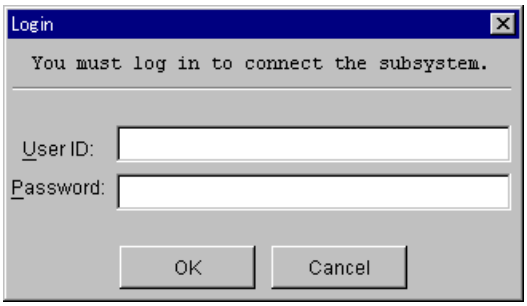


Chapter 5 Logging In and Logging Out (GUI)

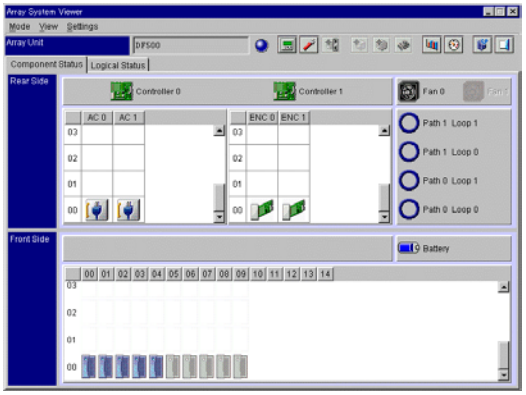
This chapter explains how to log in and log out using the GUI version of Resource Manager 9200. Management of operators by user ID is effective when operating Resource Manager 9200 in Management mode. When operating Resource Manager 9200 in Monitor mode, Resource Manager 9200 may be operated regardless of whether a user ID has been registered or not.

5.1 Logging In

1. Set the mode of operation to **Management Mode**.
2. In the main window, double-click the icon for the array unit to be connected, then click the **OK** button.
3. Enter a registered user ID and its password, then click the **OK** button.



4. Log in with the registered user ID. The unit window is displayed.



5. Double-click the icon of an array unit to which a user has already logged in. A message appears, confirming that a user has already logged in.

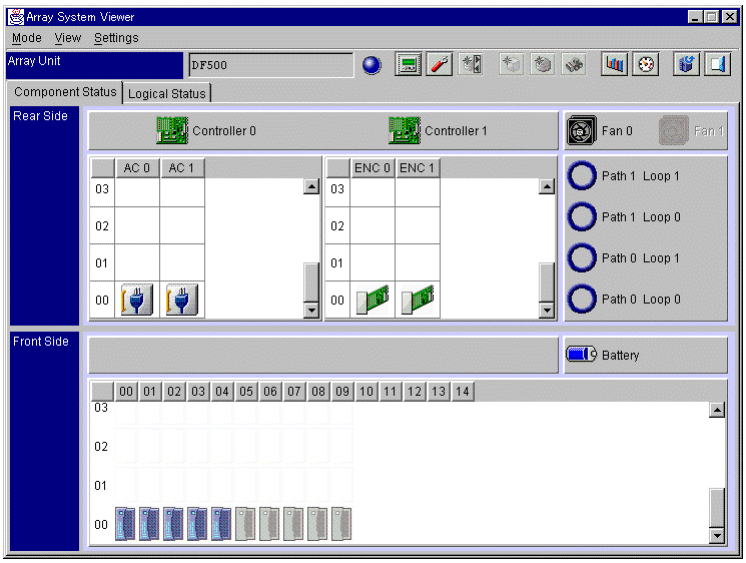
   The message indicates the user ID of the logged-in user and connection information.

6. Click the **OK** button; retry login again. The following message appears.

5.2 Logging Out

From the **Mode** menu, select **Exit**.

Alternatively, from the tool bar, select the **Exit** button on the unit window.

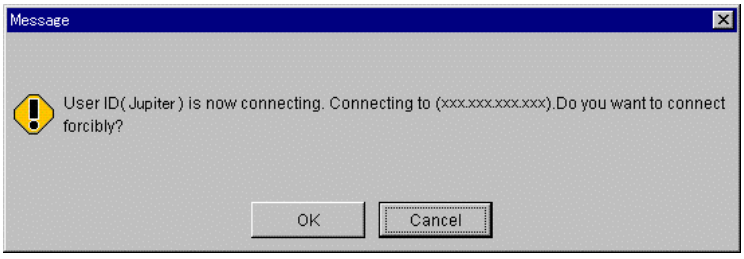


5.3 Logging In Forcibly

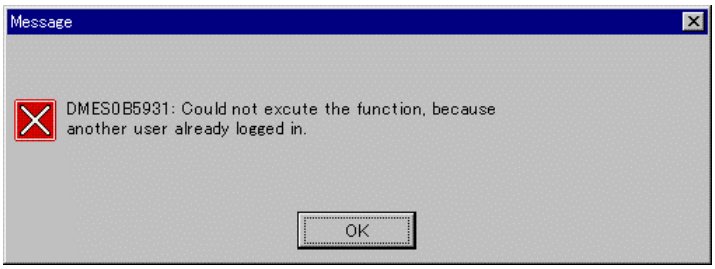
This section describes how to log out a user ID forcibly from an array unit to which a user has already logged in with the user ID, then forcibly log in with another registered user ID.

1. Double-click the icon of an array unit 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.



Message while operating in the unit window:



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

2. Close the unit window, then open it again. Check the user ID of the user who has logged in.

3. Terminate Resource Manager 9200, and restart Resource Manager 9200 by appending the **-discon** option of the Forcibly Logging In command.

4. *When using Windows:* Edit the description contents of **startmgr.bat2** (a batch file used to start the manager). Add the **-discon** option.

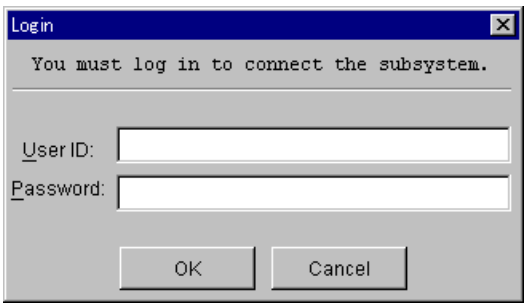
   Example: java -classpath .\CONFMNG2.JAR jp.co.hitachi.str.diskarray.gui.ConmanFrame -discon

   When using Solaris: Start the Manager by appending the **-discon** option when starting.

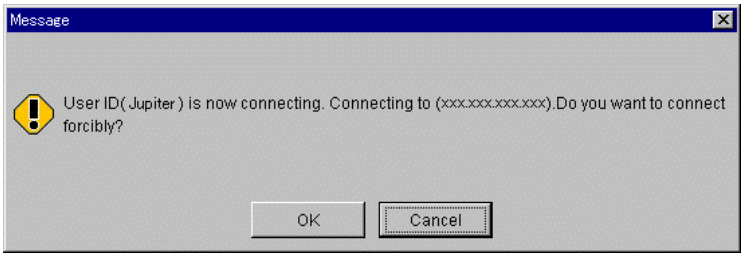
   Example: ./startmgr2 -discon

Next, log in by the following procedure.

1. Restart the Resource Manager 9200, and set the mode of operation to **Management Mode**.
2. Double-click the icon of the array unit to be connected on the main window. Then click the **OK** button.
3. Enter a registered user ID and its password. Then click the **OK** button.



4. A user ID with which a user has logged in and its password are displayed. When logging in forcibly, click the **OK** button.



Logging in with the entered user ID is completed. The unit window is displayed.

Chapter 6 Installing and Uninstalling Password Protection 9200 (CLI)

⚠ CAUTION

The User ID and Password must be configured immediately after the software key has been installed. Please contact Hitachi Data Systems Customer Support if you lose your password and are unable to access the system.

The Password Protection 9200 option is usually unselectable (closed); to make it available, you must install Password Protection 9200 (DF-F500-WSPS) and make its functions selectable (open). **To install this function, an option FD provided with the optional feature or the key code is required.**

Follow the instructions below to install Password Protection 9200 (DF-F500-WSPS). Password Protection 9200 is installed and uninstalled using Resource Manager 9200. To operate the Resource Manager 9200 using a command line interface, refer to the *Hitachi Freedom Storage™ Thunder 9200™ Resource Manager 9200 User's Guide Command Line Interface (CLI), MK-92DF574*.

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

6.1 Installation

The following paragraphs describe installation procedures performed by using the CLI version of Resource Manager 9200.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit.
3. Unlock the optional feature by using either of the following:
   - Password Protection 9200 Key FD
   - Key Code

Password Protection 9200 Key FD

a) Insert the key FD into the FDD of the system where Resource Manager 9200 is installed.

Example:

```
% auopt -unit df500 -lock off -keycode Key code
Password:
Option was opened.
```

Example:

```
% auopt -unit df500 -refer
Password:
Option name     Status
PSW-PROTECT     Enable
%
```

Password Protection 9200 Key Code

Example:

```
 % auopt -unit df500 -lock off -keycode Key code
Password:
Option was opened.
%
```

Example:

```
% auopt -unit df500 -refer
Password:
Option name     Status
PSW-PROTECT     Enable
%
```

6.2 Uninstallation

Follow the instructions below to uninstall Password Protection 9200. When it is uninstalled, the Password Protection 9200 is not available (locked) until it is opened by the Option floppy disk or the key code.

To uninstall Password Protection 9200, the key FD provided with the Password Protection 9200 feature or the key code described in the key FD is required.

Follow the instructions below to uninstall Password Protection 9200 (DF-F500-WSPS).

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit.
3. Close (lock) the optional feature by using either of the following:
   - Password Protection 9200 Key FD
   - Key Code

Password Protection 9200 Key FD

a) Insert the key FD into the FDD of the system where Resource Manager 9200 is installed.

Example:

```
% auopt -unit df500 -lock on -keyfd a:
Password:
Option was closed.
%
```

Example:

```
% auopt -unit df500 -refer
Password:
DMEC002015:No information displayed.
%
```

Password Protection 9200 Key Code

Example:

```
% auopt -unit df500 -lock on -keycode Key code
Password:
Option was closed.
%
```

Example:

```
% auopt -unit df500 -refer
Password:
DMEC002015:No information displayed.
%
```

Chapter 7 Enabling/Disabling Password Protection 9200 (CLI)

The Password Protection 9200 function can be set to Disable or Enable depending on the conditions in which the feature has been installed.

The following paragraphs describe a CLI procedure for setting the function to Disable or Enable while the Password Protection 9200 Control feature stays in an unlocked state.

These procedures can be performed by using the CLI version of Resource Manager 9200.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit.

   Example:

```
% auopt -unit df500 -option PSW-PROTECT -st disable
Password:
Option setting ended normally.
%
```

Chapter 8 Setting Security Information (CLI)

This chapter is divided into the following sections:

- Setting Protection Information
- Changing the User ID
- Deleting the User ID
- Changing the Password

8.1 Setting Protection Information

The CLI operation to set the User ID and Password with Resource Manager 9200 is as follows.

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit.

   Example:

```
% auuidadd -unit df500
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 as follows when setting the number of registered users to be displayed.
4. Specify as follows when making the number of the registered users to be displayed.

```
% auuidadd -unit df500 -num
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 to 12 characters long.
   - **Password:** Specifies the password of a user ID to register. Specified with alphanumeric, special symbols - (minus) or _ (underline) of 4 to 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 to 12 characters long.

CAUTION

The User ID and Password must be configured immediately after the software key has been installed. Please contact Hitachi Data Systems Customer Support if you lose your password and are unable to access the system.

8.2 Changing the User ID

The CLI operation to change the User ID already registered with Resource Manager 9200 is as follows.

Example:

```
% auuidchg -unit df500
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
%
```

8.3 Deleting the User ID

The CLI operation to delete the User ID already registered with Resource Manager 9200 is as follows.

Example:

```
% auuiddel -unit df500
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
%
```

8.4 Changing the Password

The CLI operation to change the password of a User ID already registered with Resource Manager 9200 is as follows.

Example:

```
% aupwdchg -unit df500
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
%
```

Chapter 9 Logging In and Logging Out (CLI)

This chapter explains how to log in and log out using the CLI version of Resource Manager 9200. The user must log into an array unit with a user ID that is presently registered in that array unit. Once a user is logged in, other user IDs are disabled when they attempt to log in.

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

9.1 Logging In

1. Start Resource Manager 9200 and change the mode of operating to **Management Mode**.
2. Register the array unit in which you will install Password Protection 9200. Connect to this registered array unit.

```
% aulogin -unit df500
Password:
User ID for array unit : (Already-set user ID)
Password for array unit : (Password of an already-set user ID)
%
```

9.2 Logging Out

To log out, enter the following:

```
% aulogout -unit df500
Password:
%
```

9.3 Logging In Forcibly

This section describes how to log out a user ID forcibly from an array unit to which a user has already logged in with the user ID, then forcibly log in with another registered user ID.

```
% aulogin -unit df500 -discon
Password:
User ID for array unit : (Already-set user ID)
Password for array unit : (Password of an already-set user ID)
User ID (xxxxxxxxxxx) has been logged in.
Connected with (xxx.xxx.xxx.xxx). (See Note)
Do you want to forcibly log in? (y/n[n]): y
%
```

Note: The destination of the connection is presented as:

```
Connected with (xxx.xxx.xxx.xxx)
```

The item in parentheses is an IP address when a LAN connection is used. When an RS232C connection is used, the destination of the connection is presented as:

```
Connected with (RS232C)
```

9.4 Checking Login

This section describes how to check the user ID and the connected unit of a user who has already logged into an array unit. This command checks the following information about the connected unit:

- For a LAN connection: IP address
- For an RS232C connection: RS232C

This command can only be used with a user ID that is not presently logged in.

```
% auchkuid -unit df500
Password:
User ID (xxxxxxxxxxxx)has been logged in.
Connected with (xxx.xxx.xxx.xxx). (See Note)
%
```

Note: The destination of the connection is presented as:

```
Connected with (xxx.xxx.xxx.xxx)
```

The item in parentheses is an IP address when a LAN connection is used. When an RS232C connection is used, the destination of the connection is presented as:

```
Connected with (RS232C)
```