HITACHI
DATA SYSTEMS

Hitachi Freedom Storage™
Lightning 9900™

LDEV Security User’s Guide

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 and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable 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., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

Hitachi Freedom Storage and Lightning 9900 are trademarks of Hitachi Data Systems Corporation.

S/390 is a registered trademark of International Business Machines Corporation (IBM) 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. Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK—90RD036-P	May 2000	Initial Release
MK—90RD036-0	August 2000	Rev. 0 supersedes and replaces MK-90RD036-P
MK—90RD036-1	September 2000	Rev. 1 supersedes and replaces MK-90RD036-0
MK—90RD036-2	November 2000	Rev. 2 supersedes and replaces MK-90RD036-1

Source Document Revision Level

The following STR source document was used to produce this 9900 user guide: *Hitachi Freedom Storage™ Lightning 9900™ LDEV Security User's Guide*, MK-90RD036-S2.

Preface

The *Hitachi Lightning 9900™ LDEV Security User's Guide* describes and provides instructions for performing LDEV Security operations on the Hitachi Lightning 9900™ RAID disk subsystem. This user's guide assumes that:

- the user has a background in data processing and understands direct-access storage device (DASD) subsystems and their basic functions,
- the user has read and understands both the *Hitachi Lightning 9900™ User and Reference Guide* and the *Hitachi Lightning 9900™ Remote Console User's Guide.*

Note: The term "9900" refers to the entire Hitachi Lightning 9900™ subsystem family, unless otherwise noted. Please refer to the *Hitachi Lightning 9900™ User and Reference Guide (MK-90RD008* for further information on the 9900 disk array subsystems.

Note: The use of the LDEV Security remote console software product is governed by the terms of your license agreement(s) with Hitachi Data Systems.

Contents

List of Figures

List of Tables

Chapter 1 Overview of LDEV Security

1.1 Overview of LDEV Security

The LDEV Security feature of the Hitachi Lightning 9900™ subsystem allows you to restrict S/390® host access to the logical devices (LDEVs) on the 9900 subsystem. You can set LDEVs to communicate only with user-selected host(s). The LDEV Security feature prevents other hosts from seeing the secured LDEV and from accessing the data contained on the secured LDEVs.

The licensed LDEV Security software on the 9900 Remote Console PC displays the LDEV Security information and allows you to perform LDEV Security operations. The LDEV Security software functions as a component of the 9900 Remote Console Main (RMCMAIN) software. The 9900 Remote Console PC is attached to the 9900 subsystems via the 9900-internal local-area network (LAN). The Remote Console PC communicates and exchanges data directly with the service processor (SVP) of each attached 9900 subsystem. For further information on the 9900 Remote Console PC and RMCMAIN software, refer to the *9900 Remote Console PC User's Guide*.

This user's guide describes and provides instructions for performing LDEV Security operations on the S/390® volumes (and HMBR volumes) on the 9900 subsystem. This document does not cover LUN Security operations for UNIX and PC-server data. For information and instructions on performing LUN Security operations, please refer to the *9900 LUN Manager User's Guide*.

Note: The use of the 9900 LDEV Security remote console software is governed by the terms of your license agreement(s) with Hitachi Data Systems.

Note: The availability of 9900 functions and device types depends upon the level of microcode installed on your 9900 subsystem.

Chapter 2 Overview of LDEV Security Operations

Figure 2.1 illustrates LDEV Security operations on the 9900 subsystem.

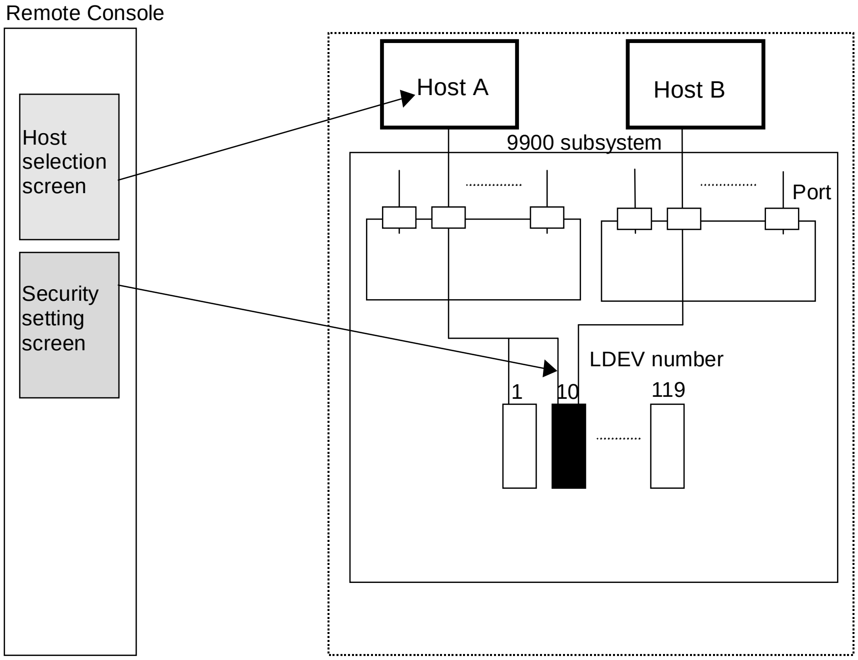


Figure 2.1 Outline of LDEV Security Function

Host selection screen	To select the host for which the LDEV Security is to be set.
Security setting screen	To specify restricted LDEV accesses.
Port	A port for connection to the host.
LDEV number	Identification number of a logical volume.

2.1 LDEV Security Specifications

Table 2.1 lists the specifications for LDEV Security operations.

Note: The availability of 9900 functions and device types depends upon the level of microcode installed on your 9900 subsystem.

Table 2.1 Specifications of LDEV Security

Item	Specification
Settable LDEV	All logical volumes installed. Open volumes used in the Hitachi Multiplatform Backup/Restore (HMBR) are included. LDEV Security is invalid on the open host side.
Number of settable hosts	Up to 32.
Host ID	A host is identified by a combination of a node ID and an LPAR number. A node ID must be changed to a channel extender if a connection via a channel extender is used.
Security setting	Hosts cannot access specific logical volumes. More than one host may be restricted from accessing a specific logical volume Access restriction take effect 5 seconds after setting.
LDEV Security range	LDEV security is valid for all ports of the 9900.
Setting up LDEV Security	LDEV security may be set while the 9900 is online. The target volume must be offline from the 9900.
Removing LDEV restrictions	LDEV Security restrictions are not automatically removed. If LDEV Security is set for a specific volume, that volume cannot be removed until LDEV Security restrictions are removed.
Relation to ShadowImage (HMRCF) and Hitachi Remote Copy (HRC).	When a volume is copied, the LDEV Security settings are not automatically transferred to the destination volume.

Note: Do not set up LDEV security while a volume is executing a job or the job may terminate abnormally.

CAUTION: If incorrect settings are made, any job in progress may terminate abnormally.

Chapter 3 Preparing for LDEV Security Operations

3.1 System Requirements

LDEV Security operations involve the 9900 subsystem containing the S/390® volumes and the LDEV Security software on the 9900 Remote Console PC.

The LDEV Security system requirements are:

- Hitachi Lightning 9900™ subsystem
- 9900 Remote Console PC and RMCMAIN software. Please refer to the *9900 Remote Console User's Guide* for instructions on installing and using the Remote Console PC and RMCMAIN software.

  Note: Administrator access to RMCMAIN is required to perform LDEV Security operations. Users without administrator access can only view LDEV Security information.
- LDEV Security license key code (password) for enabling the LDEV Security option on the Remote Console PC (RMCMAIN) and the SVP (DKCMAIN).

  Note: You must have separate DKCMAIN license key codes for each 9900 subsystem. You may not re-use the same key code for multiple 9900 subsystems.

3.2 Installing the LDEV Security Software

Installation of the LDEV Security software on the 9900 Remote Console PC is performed by the user and requires the license key code for LDEV Security. ***Note:*** You must have a separate LDEV Security license key code for each 9900 subsystem. You may not re-use the same key code for multiple 9900 subsystems.

Important: A license key is a textual key that functions as a password, because it is entered into Remote Console PC and unlocks the protection of a program product. Because each license key is generated with a subsystem serial number and program product ID input, each subsystem requires a unique license key number. License key numbers for each program product and subsystem are provided at the time of purchase.

There are three types of license keys: a temporary key, a permanent key, and an emergency key. A temporary key is for trial use. 75 days after the temporary license key is installed (or when there are 45 days left before the expiration), a warning message is displayed on the Remote Console panel when you either start the Remote Console PC or connect to a controller with the temporary license key. After 120 days, the temporary license key expires. A SIM is displayed that warns the user of the expiration of the license key, and the license key expiration is also reported to the host.

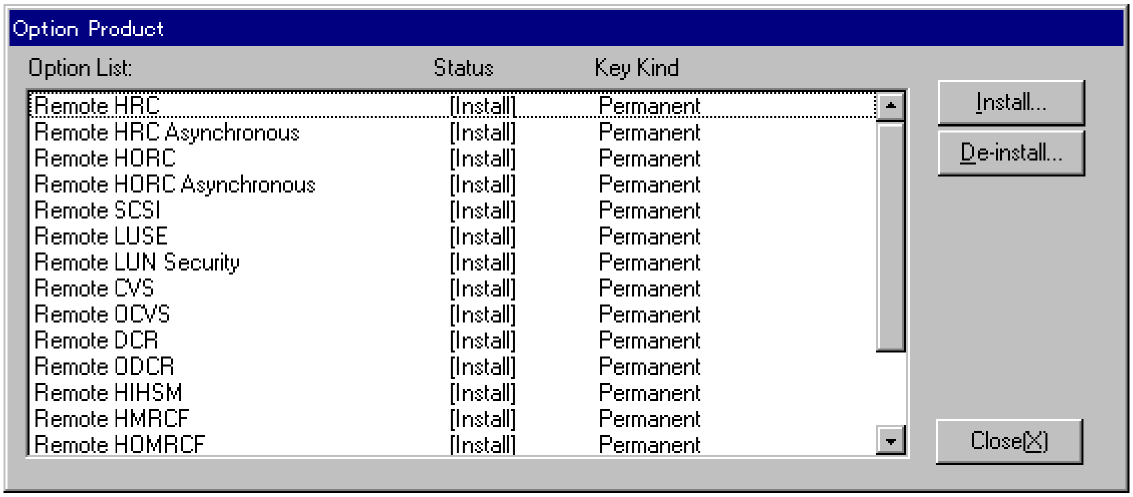
For HRC, HRCA, HORC, HORCA, HMRCF, HOMRCF, LUNM, LUSE, LUN Security, HMBR, and HXRC, the expiration of a temporary license key will have the following effects:

- No new configuration settings may be performed.
- The configuration settings that were made before the temporary license key expired remain in effect and cannot be deleted.
- Non-configuration settings that were made before the temporary license key expired can be deleted.

To enable the LDEV Security remote console software:

Check with your Hitachi Data Systems representative to verify that the correct microcode and SVP software are installed and enabled on the 9900 subsystems which will perform LDEV Security operations. Also make sure that your RMCMAIN software version is correct.

1. Make sure that the 9900 Remote Console PC and RMCMAIN software are installed and functioning properly. Refer to the *9900 Remote Console User’s Guide* for instructions on installing the Remote Console PC and RMCMAIN software.
2. Enable the LDEV Security software using the license key code as follows:
   a) Start up and log in to the *9900* RMCMAIN software with administrator access.
   b) Select **Option…** to open the RMCMAIN Option Product panel. See Figure 2.1.



Option List:	Status	Key Kind
Remote HRC	[Install]	Permanent
Remote HRC Asynchronous	[Install]	Permanent
Remote HORC	[Install]	Permanent
Remote HORC Asynchronous	[Install]	Permanent
Remote SCSI	[Install]	Permanent
Remote LUSE	[Install]	Permanent
Remote LUN Security	[Install]	Permanent
Remote CVS	[Install]	Permanent
Remote OCVS	[Install]	Permanent
Remote DCR	[Install]	Permanent
Remote ODCR	[Install]	Permanent
Remote HIHSM	[Install]	Permanent
Remote HMRCF	[Install]	Permanent
Remote HOMRCF	[Install]	Permanent

Figure 3.1 RMCMAIN Option Product Panel

c) On the Option Product panel, select **Remote LDEV Security**, and then select **Install.**

d) The Input Key Code panel opens. Enter the license key (password) in the **Key Code** text box, and then select **OK**.

e) If the password is approved, the Program Product Confirmation panel opens. This panel shows the program product model name (for example, **Remote LDEV Security**), type of key (for example, **Permanent**), and effective term (for example, Free). After confirming the content of the Program Product Confirmation panel, select **Install**.

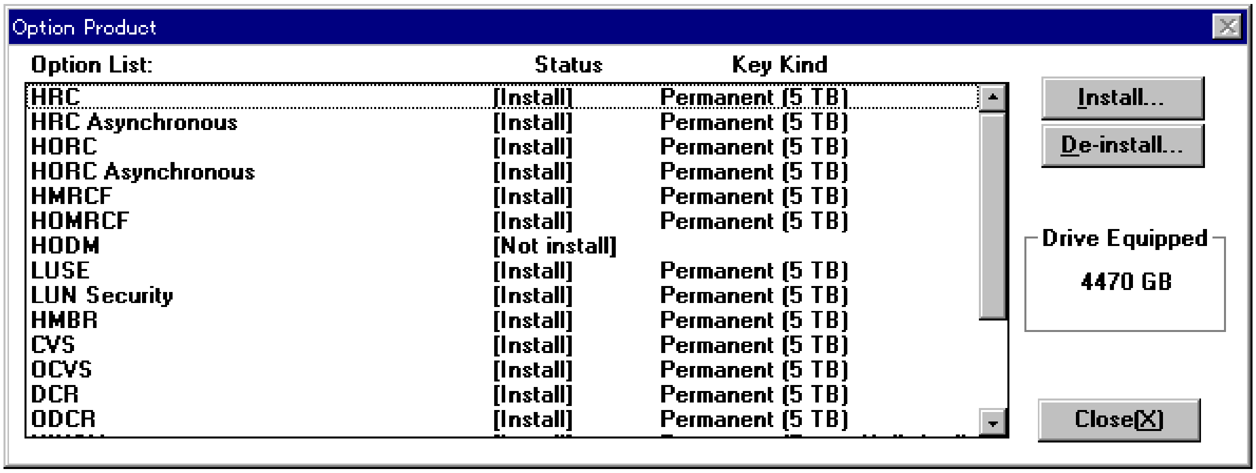
f) When this process is complete, the RMCMAIN Option Product panel reopens and the displayed status of the selected option changes from **Not install** to **Install**.

g) Select **Close** to return to the Remote Console Main panel.

3. Check with your Hitachi Data Systems representative to see if the LDEV Security option is enabled on the SVP of each 9900 subsystem on which you will perform LDEV Security operations. If not, enable the LDEV Security option on the SVP using the LDEV Security license key code (subsystem-specific) as follows:

   a) On the Remote Console Main panel, select **Controller…** to open the Connection Control panel.

   b) On the Connection Control panel, select the subsystem on which you will perform LDEV Security operations, and select **Install…** to open the DKCMAIN Option Product panel.



Option List:	Status	Key Kind
HRC	[Install]	Permanent (5 TB)
HRC Asynchronous	[Install]	Permanent (5 TB)
HORC	[Install]	Permanent (5 TB)
HORC Asynchronous	[Install]	Permanent (5 TB)
HMRCF	[Install]	Permanent (5 TB)
HOMRCF	[Install]	Permanent (5 TB)
HODM	[Not install]	
LUSE	[Install]	Permanent (5 TB)
LUN Security	[Install]	Permanent (5 TB)
HMBR	[Install]	Permanent (5 TB)
CVS	[Install]	Permanent (5 TB)
OCVS	[Install]	Permanent (5 TB)
DCR	[Install]	Permanent (5 TB)
ODCR	[Install]	Permanent (5 TB)

Drive Equipped
4470 GB

Figure 3.2 DKCMAIN Option Product Panel

c) On the Option Product panel, select **LDEV Security**, select **Install…**.

d) The Input Key Code panel opens. Enter the license key (password) in the **Key Code** text box, and then select **OK**.

e) If the password is approved, the Program Product Confirmation panel reopens. This panel shows the program product model name (for example, **LDEV Security**), key kind (for example, **Permanent**), and effective term (for example, **Free**).

f) To enable LDEV Security on another 9900 subsystem, repeat steps (a) through (e).

g) When you are finished enabling options on the 9900 subsystems, select **Close** to return to the Remote Console Main panel.

4. You are now ready to prepare for LDEV Security operations as described in the next section.

3.3 Starting LDEV Security Operations

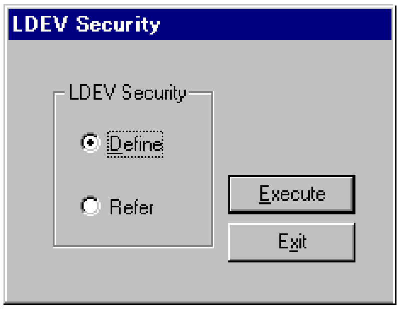
To start up the LDEV Security remote console software:

1. Log on to the 9900 Remote Console PC (RMCMAIN) with administrator access, and connect to the desired 9900 subsystem.

2. On the Function Select screen, select **LDEV Security** to open the LDEV Security activation screen (see Figure 3.3).

3. On the LDEV Security activation screen, select **Define** to perform LDEV Security operations, or select **Refer** to view LDEV Security information.

4. Select **Execute** to open the LDEV Security main screen (see Figure 3.4). The LDEV Security main screen displays the host information for the connected 9900 subsystem.

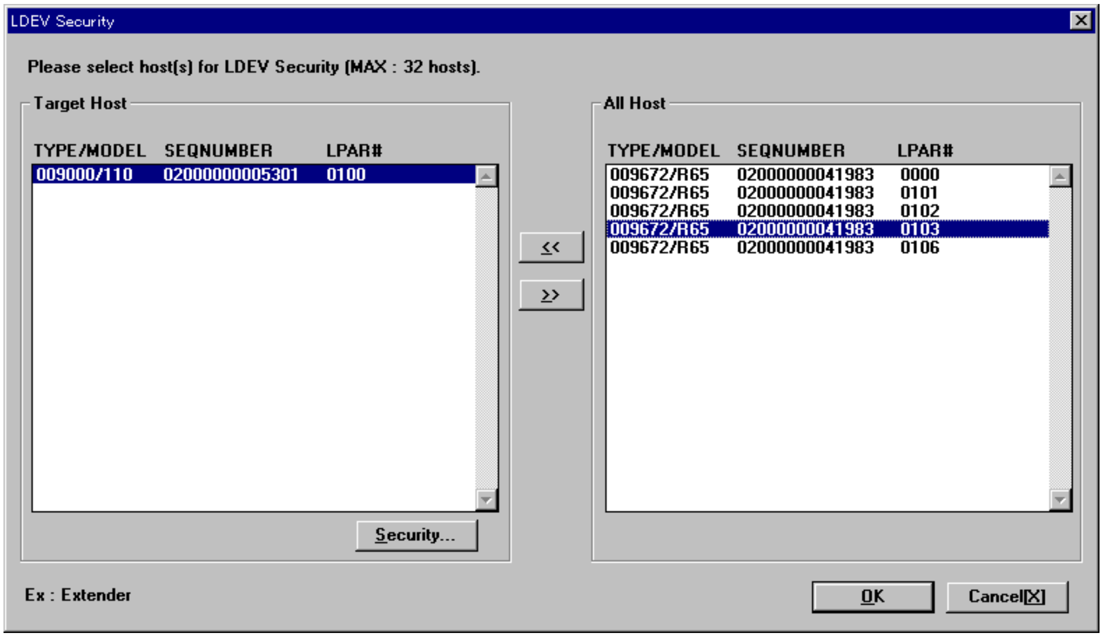


LDEV Security

● Define

○ Refer

Figure 3.3   LDEV Security Activation Screen



Please select host(s) for LDEV Security (MAX : 32 hosts).

Target Host

TYPE/MODEL	SEQNUMBER	LPAR#
009000/110	02000000005301	0100

All Host

TYPE/MODEL	SEQNUMBER	LPAR#
009672/R65	02000000041983	0000
009672/R65	02000000041983	0101
009672/R65	02000000041983	0102
009672/R65	02000000041983	0103
009672/R65	02000000041983	0106

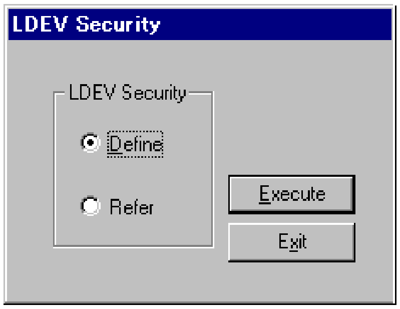
Ex : Extender

Figure 3.4   LDEV Security Main Screen

Chapter 4 Performing LDEV Security Operations

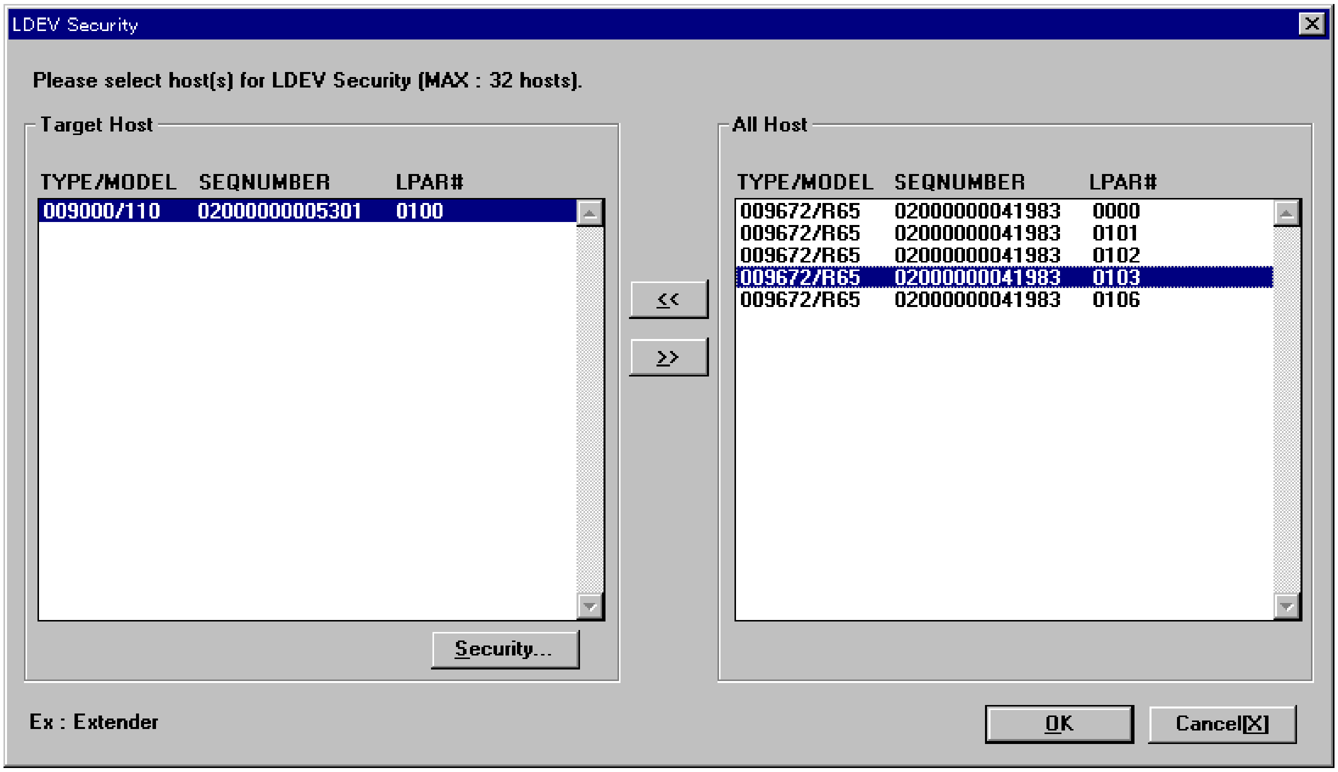
4.1 Description of LDEV Security Remote Console Software

The LDEV Security screens are shown and described in Figure 4.1 through Figure 4.5.



Screen Item	Explanation
Define	Select to perform LDEV Security operations.
Refer	Select to view LDEV Security information.
Execute	Select to start LDEV Security remote console software in selected mode (define or refer).
Exit	Select to cancel your request to start LDEV Security, return to the RMCMAIN Function Select panel.

Figure 4.1 LDEV Security Activation Screen



Please select host(s) for LDEV Security (MAX : 32 hosts).

Target Host

TYPE/MODEL	SEQNUMBER	LPAR#
009000/110	02000000005301	0100

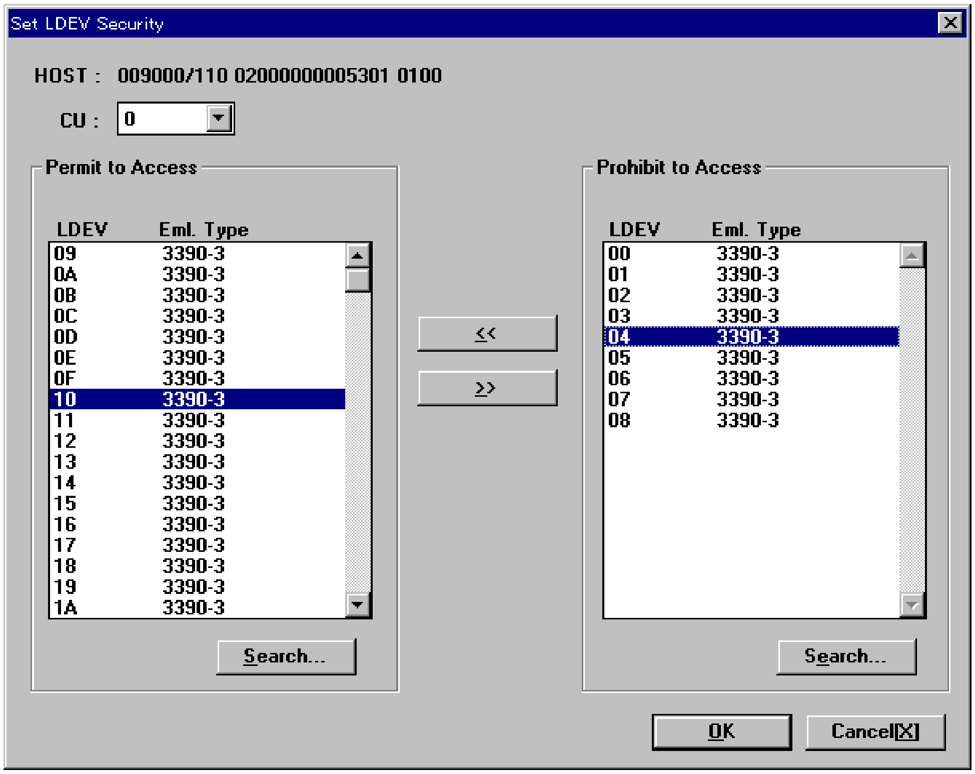
All Host

TYPE/MODEL	SEQNUMBER	LPAR#
009672/R65	02000000041983	0000
009672/R65	02000000041983	0101
009672/R65	02000000041983	0102
009672/R65	02000000041983	0103
009672/R65	02000000041983	0106

Ex : Extender

Screen Item	Explanation
Target Host	Select hosts for which LDEV Security will be set.
All Host	Displays list of all hosts recognized by the 9900.
<<	Specifies the host(s) for which LDEV Security is to be set from the All Host list box. This button cannot be selected if a selection in the All Host list box has not been highlighted.
>>	Deletes the host(s) for which LDEV Security has been set by selecting it from the Target Host list box. (Information on LDEV Security which has been set is entirely deleted.) This button cannot be selected if a selection in the Target Host list box has not been made.
Security	Activates a screen for setting Security for the selected target host of LDEV Security. This button cannot be selected when two or more hosts have been selected.
OK	Executes selection and closes screen.
Cancel	Invalidates all the setting operations and closes the screen with no action taken.

Figure 4.2 Screen for Selecting Target Host of LDEV Security



HOST : 009000/110 02000000005301 0100

CU : 0

Permit to Access

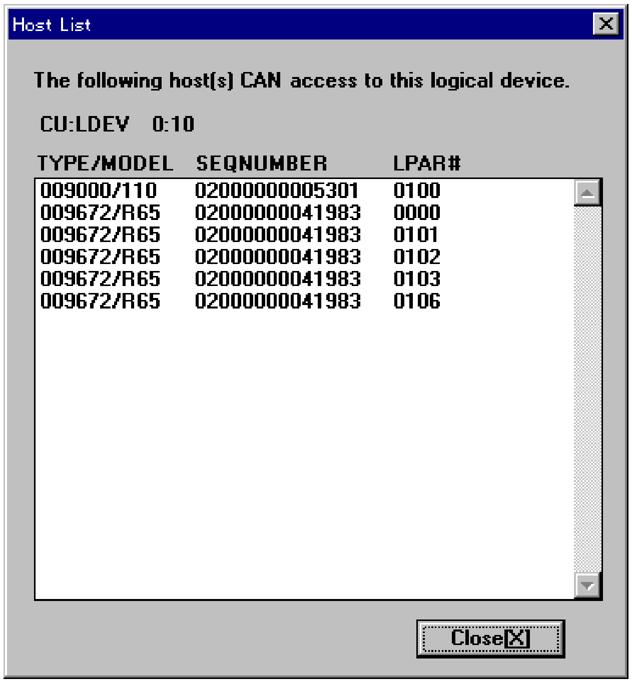
LDEV	Eml. Type
09	3390-3
0A	3390-3
0B	3390-3
0C	3390-3
0D	3390-3
0E	3390-3
0F	3390-3
10	3390-3
11	3390-3
12	3390-3
13	3390-3
14	3390-3
15	3390-3
16	3390-3
17	3390-3
18	3390-3
19	3390-3
1A	3390-3

Prohibit to Access

LDEV	Eml. Type
00	3390-3
01	3390-3
02	3390-3
03	3390-3
04	3390-3
05	3390-3
06	3390-3
07	3390-3
08	3390-3

Screen Item	Explanation
HOST	Displays host selected as target host for LDEV Security.
CU	Selects CU# of the logical device that will have access or will not have access to the selected host. Only installed CUs are displayed here.
Permit to Access	Displays a list of logical devices which the selected host can access. Only the LDEVs under the specified CU# are displayed.
LDEV	LDEV ID (00 to FF)
Eml. Type	A name of an LDEV emulation type. In the case of an extended LU, it is displayed including a number of the connected LUs as shown in the following example, "OPEN-3 *5".
Prohibit to Access	Displays a list of logical devices which the selected host cannot access. Only the LDEVs under the specified CU# are displayed.
LDEV	LDEV ID (00 to FF)
Eml. Type	A name of an LDEV emulation type. In the case of an extended LU, it is displayed including a number of the connected LUs as shown in the following example, "OPEN-3 *5".
<<	The selected LDEV is deleted from Prohibit to Access list and moved to Permit to Access list.
>>	The selected LDEV is deleted from Permit to Access list and moved to Prohibit to Access list.
Search (Permit to Access)	Displays list of all hosts that can access the LDEV selected from the Permit to Access list. Only one LDEV may be selected for each Search.
Search (Prohibit to Access)	Displays list of all hosts that cannot access the LDEV selected from the Prohibit to Access list. Only one LDEV may be selected for each Search.
OK	Executes selection and closes screen.
Cancel	Invalidates all the setting operations and closes the screen with no action taken.

Figure 4.3 LDEV Security Setting Screen



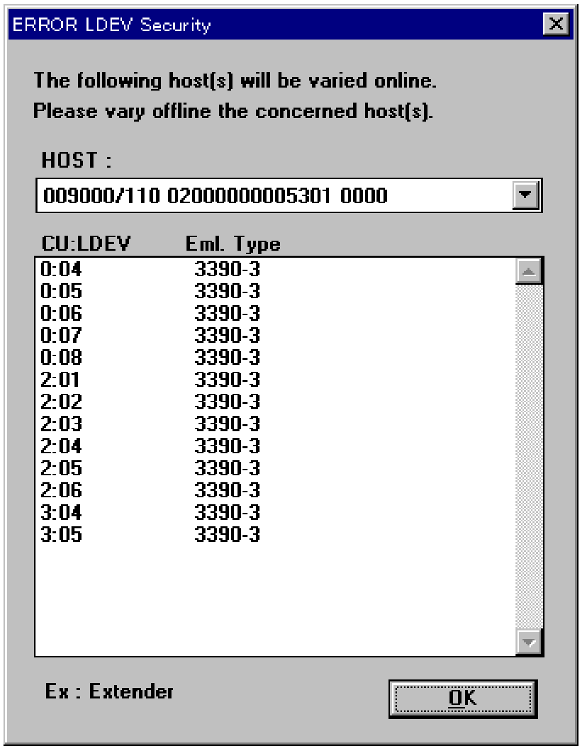
The following host(s) CAN access to this logical device.

CU:LDEV 0:10

```
TYPE/MODEL   SEQNUMBER         LPAR#
009000/110   02000000005301    0100
009672/R65   02000000041983    0000
009672/R65   02000000041983    0101
009672/R65   02000000041983    0102
009672/R65   02000000041983    0103
009672/R65   02000000041983    0106
```

Screen Item	Explanation
The following host[s] CAN access this logical device.	Lists all hosts which can access the selected logical device.
The following hosts CANNOT access this logical device.	Lists all hosts which cannot access the selected logical device.
CU:LDEV	Displays the CU:LDEV# selected on the Set LDEV Security screen.
Close	Closes the screen with no action taken.

Figure 4.4 Host List Screen


ERROR LDEV Security

The following host(s) will be varied online.
Please vary offline the concerned host(s).

HOST :

009000/110 02000000005301 0000

CU:LDEV	Eml. Type
0:04	3390-3
0:05	3390-3
0:06	3390-3
0:07	3390-3
0:08	3390-3
2:01	3390-3
2:02	3390-3
2:03	3390-3
2:04	3390-3
2:05	3390-3
2:06	3390-3
3:04	3390-3
3:05	3390-3

Ex : Extender

Screen Item	Explanation
HOST :	Allows you to select the host where implementing LDEV Security failed.
CU:LDEV	Lists logical devices where LDEV Security failed for selected host.
OK	Closes the screen.

Figure 4.5 Error LDEV Security Screen

4.2 Setting LDEV Security

To set the LDEV Security settings for a specific host:

1. Registering target host: Select a host to be a target of LDEV Security from the hosts displayed in the list box of the All Host area on the screen for selecting target host of LDEV Security (Figure 4.2) and select [<<]. The selected host appears in the list box in the Target Host area.
2. Specifying Target Host To Be Set: Select a host for which LDEV Security is to be set from the list box in the Target Host area on the screen for selecting target host of LDEV Security and double-click it or press **Security...**.
3. Specifying Restricted CU Accesses: The LDEV Security setting screen (Figure 4.3) is displayed. First, select a CU for which the Security is to be set.
4. Setting Secured LDEV Access: Next, select an LDEV for which LDEV Security is to be set from the list box in the Permit to Access area and press [>>]. The selection is reflected on the list box in the Prohibit to Access area.
5. Terminating LDEV Security Setting: When **OK** is pressed on the LDEV Security setting screen (Figure 4.3), the set information is saved and the screen returns to the screen for selecting target host of LDEV Security (Figure 4.2). When **Cancel** is pressed, the set information is canceled and the screen returns to the screen for selecting target host of LDEV Security. Terminating Registration: When **OK** is pressed on the screen for selecting target host of LDEV Security (Figure 4.2) after the entry is completed, the set information is saved and the screen returns to the LDEV Security activation screen. When **Cancel** is pressed, the set information is canceled and the screen returns to the LDEV Security activation screen.

4.3 Resetting LDEV Security for Specific Hosts

To reset the LDEV Security settings for a specific host:

1. Remove Host from Target: When a host to be removed from the target of LDEV Security is selected from the list box in the Target Host area on the screen for selecting target host of LDEV Security and [>>] is pressed, a name of the host which has been removed from the target appears in the All Host list. (When the host is removed from the target, the set information of LDEV Security is entirely deleted.)
2. Verify Setting Cancellation: Press **OK** after removing the host from the target. The information on the setting cancellation is saved and the screen returns to the LDEV Security activation screen.

4.4 Resetting LDEV Security for Specific LDEVs

To reset the LDEV security for one or more specific LDEVs:

1. Specify target host. Select a host to be removed from the target of LDEV Security from the list box in the Target Host area on the screen for selecting target host of LDEV Security and double-click it or press **Security**.
2. Specify CU setting to be canceled. The LDEV Security setting screen is displayed. First, select the CU for which the Security setting is to be canceled.
3. Specify LDEV setting for which is to be canceled. Next, select an LDEV the Security setting for which is to be canceled from the list box in the Prohibit to Access area and press [<<]. The selection is reflected on the Permit to Access list.
4. Terminate LDEV Security setting cancellation. Press **OK** on the LDEV Security setting screen. The setting/cancellation information is saved and the screen is returned to the screen for selecting target host of LDEV Security.
5. Verifying setting cancellation. Press **OK** on the screen for selecting target host of LDEV Security. The information on the setting cancellation is saved and the screen is returned to the LDEV Security activation screen.

4.5 Displaying Host Access

To display the host(s) which have access to a specific LDEV:

1. Select a CU on the LDEV Security setting screen (Figure 4.3).
2. Then, specify an LDEV by selecting it from the Permit to Access area and double-click it or press **Search**. The screen showing a list of hosts which can access the selected CU:LDEV is displayed.

To display the host(s) which do not have access to a specific LDEV:

1. Select a CU from the LDEV Security setting screen (Figure 2.1).
2. Specify an LDEV by selecting it from the Prohibit to Access area and double-click it or press **Search**. The screen (Figure 4.3) showing a list of the hosts which cannot access the selected CU:LDEV is displayed.

Chapter 5 Troubleshooting

5.1 Troubleshooting LDEV Security Operations

If you have a problem with the 9900 Remote Console PC or RMCMAIN software, first make sure that the problem is not being caused by the PC or Ethernet hardware or software, and try restarting the PC. If an LDEV Security error message is displayed on the Remote Console PC, refer to section 5.2 for a description of the error codes. If you need to call the Hitachi Data Systems Support Center, refer to section 5.3 for instructions.

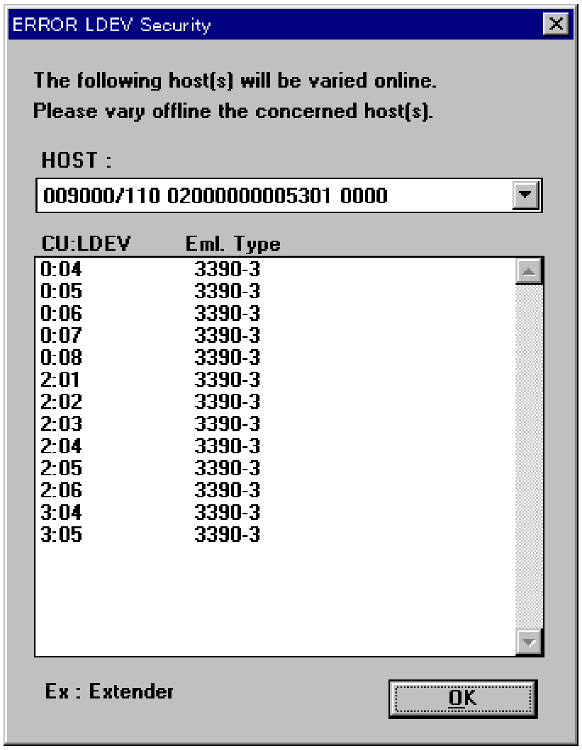
Table 5.1 provides general troubleshooting instructions for LDEV Security operations.

Table 5.1 General LDEV Security Troubleshooting

Error	Corrective Action
LDEV Security operations do not function properly.	Make sure all LDEV Security requirements and restrictions are met. Make sure the 9900 subsystem is powered on and fully functional (NVS, cache, DFW). Please refer to the *Hitachi Lightning 9900™ User and Reference Guide* (MK-90RD008) for operational and troubleshooting information for the 9900 subsystem. Check all input values and parameters to make sure you entered the correct information on the Remote Console PC (for example, LDEV ID).
Channel enable LED indicators (on the 9900 control panel) are off or flashing.	Please call the Hitachi Data Systems Support Center for assistance.
LDEVs are not displaying correctly.	Make sure the correct CU image is selected.
An R-SIM warning is displayed on the 9900 Remote Console PC.	Locate the SIM using the RMCMAIN R-SIM panel (see the *9900 Remote Console User's Guide* for instructions). Refer to the *Hitachi Lightning 9900™ User and Reference Guide* for a listing of 9900 SIMs.
An LDEV Security error message is displayed on the Remote Console PC.	Refer to section 5.2 for the error codes.
There is a problem with the Remote Console PC or LDEV Security remote console software.	Make sure the problem is not the PC or LAN hardware or software. Try restarting the PC and reconnecting to the subsystem.

5.2 LDEV Security Error Codes

When an LDEV Security setting fails, the Error LDEV Security screen (see Figure 5.1) is displayed automatically. The Error LDEV Security panel displays the affected LDEV(s) for each attached host. Since the specified LDEV(s) is/are already online to the host, you must take the volume(s) offline before performing the LDEV Security setting operation again.



The following host(s) will be varied online.
Please vary offline the concerned host(s).

HOST : 009000/110 02000000005301 0000

CU:LDEV	Eml. Type
0:04	3390-3
0:05	3390-3
0:06	3390-3
0:07	3390-3
0:08	3390-3
2:01	3390-3
2:02	3390-3
2:03	3390-3
2:04	3390-3
2:05	3390-3
2:06	3390-3
3:04	3390-3
3:05	3390-3

Ex : Extender

Figure 5.1 Error LDEV Security Panel

5.3 Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including the circumstances surrounding the error or failure and the exact content of any error messages and/or codes displayed on the Remote Console PC and/or logged at the host.

The worldwide Hitachi Data Systems Support Centers are:

- Hitachi Data Systems North America/Latin America
San Diego, California, USA
1-800-348-4357
- Hitachi Data Systems Europe
Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific
North Ryde, Australia
011-61-2-9325-3300

Appendix A Acronyms and Abbreviations

CVS	Custom Volume Size
HMBR	Hitachi Multiplatform Backup/Restore
HMRCF	Hitachi Multiple RAID Coupling Feature
HRC	Hitachi Remote Copy
LDEV	logical device
PC	personal computer
R-SIM	remote service information message
SIM	service information message