NEC

**NEC Express5800 Series
Web-based Promise Array
Management Professional User's Guide
(Linux Version)
(For N8103-105 Disk Array Controller)**

Preface

This User's Guide explains the management utility [Web-based Promise Array Management Professional] to be used for operating N8103-105 Disk Array Controller provided by Promise.

Some of the features explained in this guide may not be supported in your environment. Please be sure to read the User's Guide supplied with the platform.

The guide is intended for persons who are familiar with Linux functions and operation methods. For details on Linux operation, see Linux Online Help or manuals.

Copyrights

Promise® and its logo are registered trademarks of Promise Technology Inc. of the U.S.A.

Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

Red Hat, RPM, and all the trademarks and logos based on Red Hat are the trademarks or registered trademarks in the United States and other countries.

MIRACLE LINUX and its logo are registered trademarks of MIRACLE LINUX Corporation.

NEC ESMPRO and NEC EXPRESSBUILDER are registered trademarks of NEC Corporation.

Microsoft, its logo, Windows, Windows Server and MS-DOS are worldwide registered trademarks of Microsoft Corporation of the U.S.A.

All company names and product names mentioned herein are trademarks or registered trademarks of their respective companies.

Notes:

(1) No part of this manual may be reproduced in any form without the prior written permission of NEC Corporation.

(2) The contents of this manual may be revised without prior notice.

(3) The contents of this manual shall not be copied or altered without the prior written permission of NEC Corporation.

(4) All efforts have been made to ensure the accuracy of all information in this manual. If you notice any part unclear, incorrect, or omitted in this manual, contact the sales agent where you purchased this product.

(5) NEC assumes no liability arising from the use of this product, nor any liability for incidental or consequential damages arising from the use of this manual regardless of Item (4).

(6) Should any of these products be considered as strategic goods, and thereby governed by foreign exchange or foreign trade regulations, the Government of Japan will require an export license before said products can be exported from Japan.

(7) NEC will not guarantee the proper operation of the open source software including Linux kernels. Please be sure to implement and operate the Linux system based on the principle of self-responsibility.

Contents

1. Overview

1.1 Web-based Promise Array Management Professional

Web-based Promise Array Management Professional (hereafter abbreviated for WebPAM PRO) is a Web-based application that locally or remotely manages N8103-105 Disk Array Controller provided by Promise.

WebPAM PRO only supports Mozilla Firefox 1.5 or later (when monitoring from the Linux environment) and Microsoft Internet Explorer (IE) 6.0 or later (when monitoring from the Windows environment) as its browser. After installing WebPAM PRO, the following features become available in the system.

- Creating or deleting the following logical arrays on the graphical operation screen of the browser

  – RAID0 (data striping with one or more hard disk drives)

  – RAID1 (data mirroring with two hard disk drives)

  – RAID5 (data striping with parity with more than two hard disk drives)

  – RAID1 spanning (same as RAID10. Data mirroring and striping with four hard disk drives)

- Checking consistency among logical drives (redundancy check)

- Checking media error in disks (media patrol)

- Auto-recovering degraded logical drives if entered into the state (rebuild)

To manage N8103-105 remotely from the management computer, WebPAM PRO must be installed in the machine to which N8103-105 is connected. These two computers must be set to allow communication with each other via TCP/IP. HTTPS or SSL is used for communication via TCP/IP in order to endure security and encrypt transfer data.

1.2 Precautions

Be sure to read the following notes and precautions before using WebPAM PRO:

■ It is strongly recommended to provide media patrol or redundancy check routinely for all logical drives and HDDs to be connected. Whether the media patrol or the redundancy check is used may be determined as follows depending on the environment of your system.

Redundancy check	Environment in which your system is always subject to load. --- Redundancy check can continue at a constant rate under heavy system load
Media patrol	Environment in which your system is subject to comparatively small load in any period including the night. --- Media Patrol has lower priority than other tasks in the system, so it may make little progress under heavy system load

The above action allows you to find subsequent defects (due to degradation such as aging) in files of low access frequency and unused areas as soon as possible. In rebuilding after replacement of a HDD due to a failure, subsequent defects may be found in remaining HDDs. In such a case, the system cannot be recovered. Thus, detecting subsequent defects as early as possible is extremely effective as preventive maintenance. Periodical redundancy check or media patrol is effective to keep the stable operation of your system. It is strongly recommended to take the action once per week or at least once per month. For the detailed explanation and routine action, see the description on the scheduling of the redundancy check or media patrol in this manual. Note that a media patrol task has been scheduled to be done on AM0:00 every Wednesday by default.

■ Setting for security is required when you log on to WebPAM PRO first time. See "Appendix A First Logon."

■ To start WebPAM PRO, more than 255 colors must be selected in the screen setup.

■ A message that indicates "Unknown"may be registered in the Event Frame of WebPAM PRO when the system is under heavy load such as the case when mutilple background activities are running at the same time. Even in that case, all the background activities are properly done and will successfully be finished, and the messages will be registered in syslog. Please close WebPAM PRO and then restart it.

■ The "HTTP 500 Error" window may be displayed when some load is added during operation of WebPAM PRO or, in particular, while multiple background activities are running. In this case, refresh the screen from the Refresh tab. For the Refresh tab, see Section 3.3.

2. Installation/Uninstallation

2.1 Operation Environment for WebPAM PRO

The following operation environment is required for the proper operation of WebPAM PRO.

- Hardware
  NEC EXPRESS5800 server available for the "N8103-105 Disk Array Controller (SAS)"

- Software
  RHEL AS/ES 4 Update 5 or later
  ML4SP2 or later

IMPORTANT:

- Only users authorized as root are permitted to install and uninstall WebPAM PRO.
- If you have used Web-based Promise Array Manager (WebPAM, N8103-101/103 management utility), be sure to uninstall WebPAM before installing WebPAM PRO. You cannot use WebPAM PRO with WebPAM. For uninstalling WebPAM, see "Web-based Promise Array Manager User's Guide (Linux Version)".

2.2 Installing WebPAM PRO

1. Untar the WebPAM PRO installation module.

    Ex.) As the WebPAM PRO installation module is "WPPInst-1.00.tar.gz":
    # tar -zxvf WPPInst-1.00.tar.gz

2. Execute the WebPAM PRO installation script as follows:

    # ./WPPInst.sh –e

3. Check that WebPAM PRO has been successfully installed.
    ```
     WPP: Installation completed. Please reboot the system.
    ```

    After installation completed, restart the system.

2.3 Uninstalling WebPAM PRO

IMPORTANT: Follow the procedure described in this chapter to uninstall WebPAM PRO.

NOTE: WebPAM PRO is required for managing the RAID system. Do not uninstall WebPAM PRO unless you have to uninstall for maintenance including the upgrade of the utility.

1. Go to the folder that WebPAM PRO has been installed.
    # cd /opt/Promise/WebPAMPRO.

2. Execute the WebPAM PRO uninstallation script as follows.
    # ./WPPUninst.sh

3. Check that WebPAM PRO has been successfully uninstalled.

    If the installation has finished successfully, the following messages will appear.
    ```
    WPP: Uninstallation completed. Please reboot the system.
    ```

    After installation completed, restart the system.

3. Operation

This chapter describes how to start WebPAM PRO and operations on screens appearing after starting WebPAM PRO.

3.1 Starting and Exiting WebPAM PRO

IMPORTANT:

- For a specific controller, do not start more than one web browser or more than one tab in a browser concurrently.

- You need a certificate for security when logging in for the first time. Install the security certificate according to Appendix A.

- Opening the WebPAM PRO screen with Internet Explorer 7 always causes [Certificate Error] to appear at the top of Internet Explorer. However, this does not affect proper operations of WebPAM PRO.

- When using Internet Explorer 7, a certificate warning is always displayed on the upper right of the Internet Explorer screen. This has no effect on WebPAM Pro operation.

- The default user name and password are "administrator" and "password," respectively. At the first logon, enter "administrator" and "password" as the user name and password, respectively. For changing the administrator's password after the logon, see "3.4 Managing Users." The user name and password for logon to WebPAM PRO are accounts exclusively used for WebPAM PRO. They are different from the user name and password used for logon to OS.

- When you start WebPAM PRO first time, messages with the date of 1970s may be registered. This has no effect on WebPAM PRO operation.

NOTE: Depending on the OS used, browser, and/or color scheme, the images shown in this manual may be different from the actual images.

3.1.1 Controlling WebPAM PRO with a Local Computer

1. Start WebPAM PRO by either of the following methods.
- Double-click the WebPAM PRO icon on the desktop.
- **<On RHEL>** Select [Application] (the main menu on the panel) → [Accessory] → [WebPAMPRO]. Then click [WebPAMPRO]. **<On Miracle>** Select [Start] (the main menu on the panel) → [Applications] → [Utilities]. Then click [WebPAMPRO].

2. The Security Alert window will appear. See Appendix A to install the certificate.

3. If the "Security Error: Domain Name Mismatch" message is displayed, click OK.

4. Perform the following operation on the logon screen.

- Enter your user ID and password in the [User Name] and [Password] fields, respectively. (At the first logon, specify "administrator" and "password" as the user ID and password, respectively.)

- Click [Login].

3.1.2 Controlling WebPAM PRO with a Remote Computer

NOTES:

- If using a proxy server for making access to the Internet, you need to bypass the proxy server. See Appendix A for the setting procedure.

- If a firewall function is running on the system (server), you may not controll from the remote computer. In this case, change the setting to make it possible to connect from the remote computer (e.g. check the port setting for firewall).

- The procedure provided below is for connecting from the Windows environment. If you want to connect from the Linux environment, after performing Steps 1 and 2 shown below, follow the Steps 2 and 3 in "3.1.1 Controlling WebPAM PRO with a Local Computer" instead of Step3 below. Then go back to Step 4 below.

---

1. Start the Web browser.

2. Enter the IP address of the Promise RAID system to be controlled in the browser address and press Enter.

   For example, if the IP address is "10.10.10.10," type "https://10.10.10.10:8443/promise."

   If a session with the remote system can be established, the WebPAM PRO logon screen appears.

3. The Security Alert window will appear. Click [Yes].
   The [Block by Security Enforcement] screen may appear. Click [Add] to register WebPAM PRO to a zone in the trusted site.

4. On the logon screen, perform the following operations:

   - Enter your user ID and password in the [User Name] and [Password] fields, respectively. (At the first logon, specify "administrator" and "password" as the user ID and password, respectively.)

   - Click [Login].

3.1.3 Exiting WebPAM PRO

Click [Logout] on the WebPAM PRO Header of the WebPAM PRO operation window to exit the WebPAM PRO operation window. Click [x] at the upper right corner of the WebPAM PRO logon window to exit it.
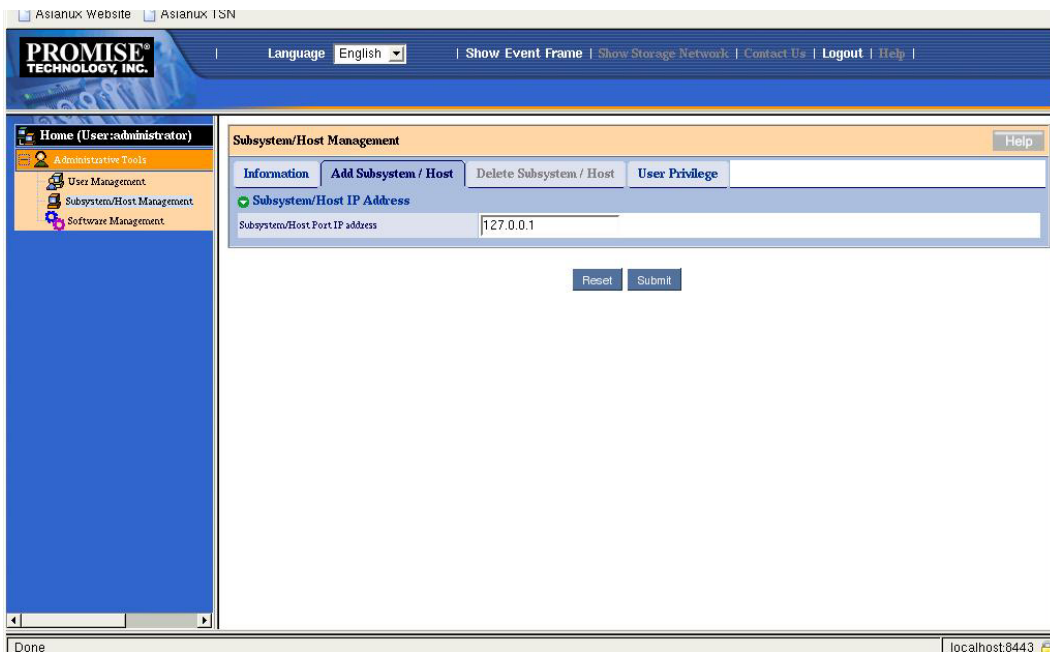
3.2 WebPAM PRO Operation Window

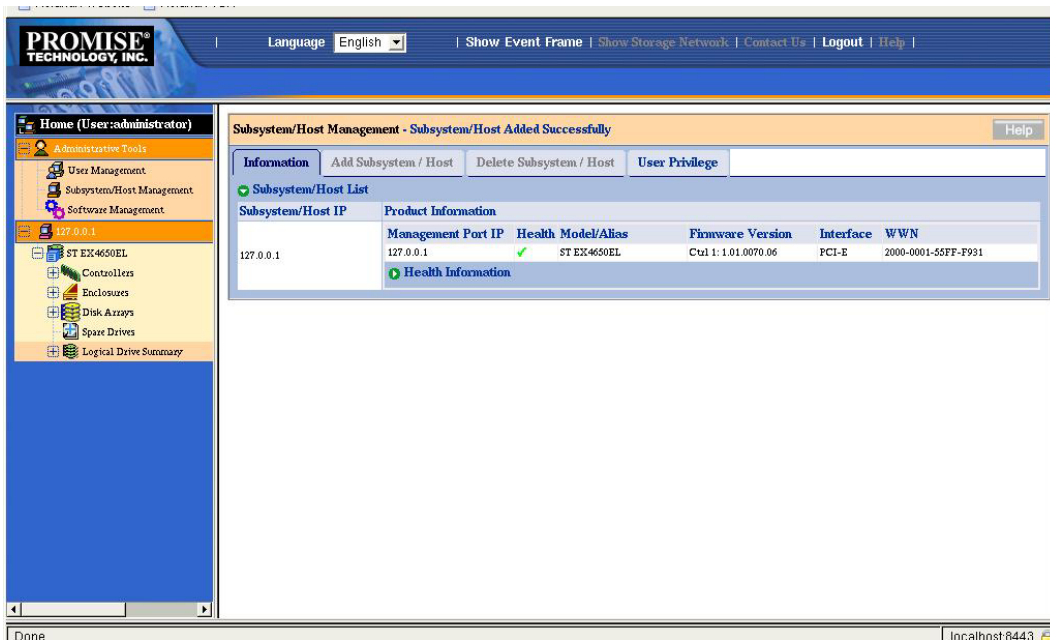### 3.2.1 Using WebPAM PRO for the First Time

1. Click the Subsystem/Host Management icon in the Tree View appearing at the left side of the screen.
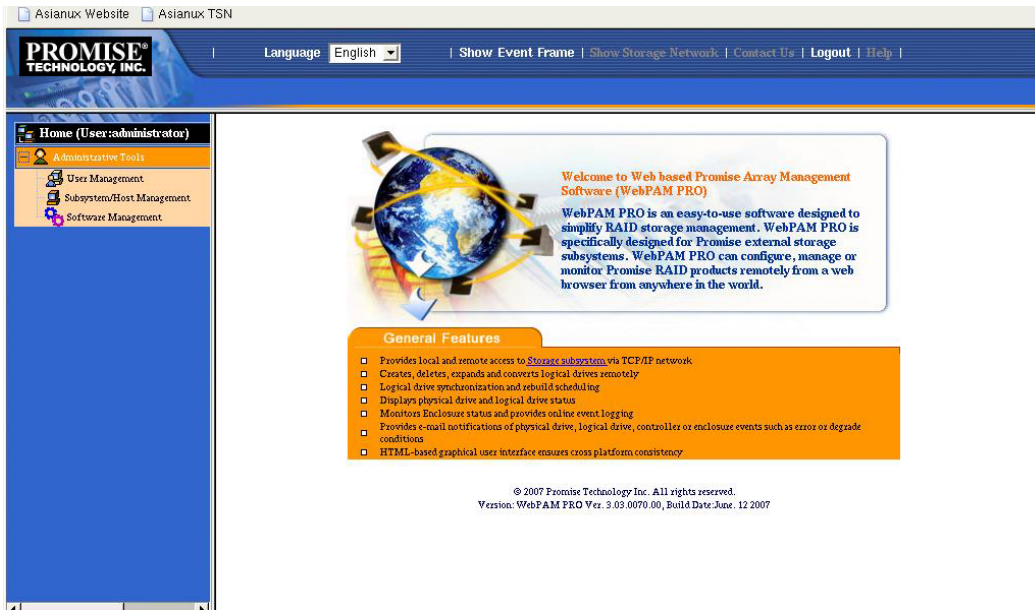
2. Click the Add Subsystem/Host tab in the screen appearing at the right side of the screen.
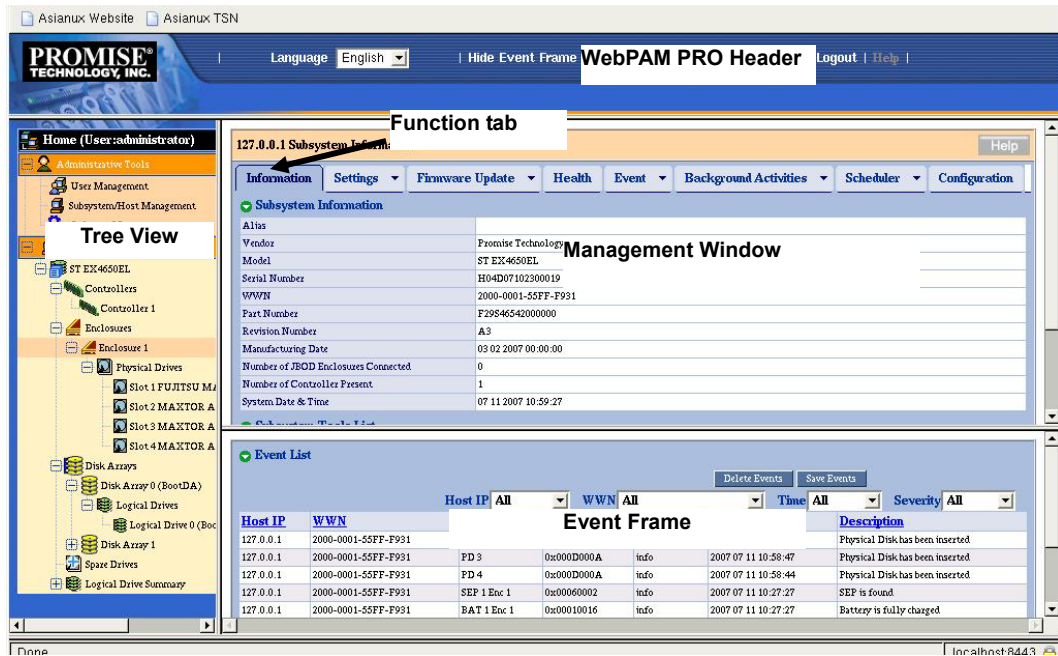
3. Make sure that "127.0.0.1" is entered in the Subsystem/Host Port IP address field, and click the [Submit] button.

The host PC information appears in the Tree View.

3.2.2 WebPAM PRO Operation Screen

The WebPAM PRO window is mainly configured with three parts; Tree View, Management Window, and Event Frame.

Tree View

The Tree View can indicate the configuration of the RAID system hierarchically in the similar way as Windows Explorer. Each item at a specific level can be expanded by displaying the relevant information at the lower levels.
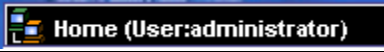
Management Window

The information appearing in the Management Window varies depending on the item selected in the Tree View. The window allows the information set on users and/or devices to be checked or updated or logical drives to be created, maintained, deleted or monitored. The information to be displayed includes text and list boxes, fields and buttons. In each function tab, various tasks and processes can be controlled. Function tabs unavailable depending on the status of logical drives or HDDs are grayed out.

Event Frame

The Event Frame indicates the list of events. The Event Frame can be either displayed or not alternately by selecting [Show Event/Hide Event] on the WebPAM PRO Header. See "3.17 Events" for details.

3.3 Icons

When you click the link to an icon on the Tree View, several setting and status display screens appear on the Management Window. The features grayed out on the Management Window are unavailable. For details of features, see the relevant chapters.

Tree View	Management Window display
Home icon 🖥️ Home (User:administrator) Indicates the name of the current logon user in parentheses.	Indicates the version information of WebPAM PRO.
Administrative Tools icon 👤 Indicates the user, host and software management information in WebPAM PRO.	User Management tab Subsystem/Host Management tab Software Management tab
User Management icon 👥	Lists user names registered currently in the Information tab. Logging on to WebPAM PRO as a super privilege user, you can create, delete or set users in the Create or Delete tab. Logging on to WebPAM PRO as another user, you can only change your password and Display Name.
Subsystem/Host Management icon 🖥️ (Displayed at logon as a super privilege user) Indicates the information on the current host.	Indicates the IP address of the host, the firmware version of the controller and the Display Name. You can change privilege levels of users in the User Privilege tab.
Software Management icon ⚙️ (Displayed at logon as a super privilege user)	Logging on to WebPAM PRO as a super privilege user, you can set the interval for refreshing the Event Frame. The Event Frame can be selected out of 15, 30, 60 and 300 seconds. The default is 30.
Host icon 🖥️ Indicates the information on the host including its IP address.	Indicates the version of WebPAM PRO, firmware version and host information including its IP address. Logging on to WebPAM PRO as a super privilege user, you can change privilege levels of users in the User Rights tab. Clicking [Submit] in the Refresh tab allows the screen to be updated to the latest status. If you click [Submit], confirmation dialog "Are you sure you want to refresh" appears. Then click [OK].
ST EX4650EL icon 📇 (Subsystem icon)	Indicates the information on the installed RAID card. You can provide settings for background tasks including redundancy check and media patrol and scheduling and get configuration information. See the following description for details.

Tree View	Management Window display
Controller icon	Indicates the information on BIOS and drivers. In addition, you can provide various settings including performance, display battery status and display or change buzzer setting.
Enclosure icon	Indicates the enclosure information. See the following description for details.
Physical Drives icon Indicates HDDs in the enclosure and connected HDDs.	Indicates the information on all connected HDDs.
Disk Arrays icon Indicates HDDs in the enclosure and connected HDDs.	Indicates the information on disk arrays. You can provide creation, deletion, rebuild, transition or PDM for disk arrays here.
Logical Drives icon Displays the list of logical drives installed in this host.	Indicates the information on logical drives. You can initialize logical drives and provide redundancy check for each logical drive.
Spare Drives icon	Indicates the information on spare drives. You can create or delete spare drives here.
Logical Drive Summary icon Displays the battery.	Indicates the information on all logical drives subordinate to the controller. The displayed information is the same as that appearing when you click a logical drive subordinate to Disk Arrays.

3.4 Managing Users

Creating user account

To create a new user account, follow the procedure described below:

1. Logon to WebPAM PRO as an administrator, or a super privilege user.

2. Click the User Management in the Tree View and then click the Create tab in the Management Window.

3. Set the items in the Create tab as shown in the table below:

Item name	Description	Available characters
User Name	Account used at login	Alphanumeric characters of 1 - 31 bytes
New Password	Password	Alphanumeric characters of 0 - 31 bytes (Always set the password for security enforcement.)
Retype Password	Same as the value entered in the New Password field	
Display Name	Name of user	Alphanumeric characters of 0 - 10 bytes
Privilege	Privilege to be given to the user	
Enable	Check the checkbox.	

Privileges are defined as described in the table below.

Privilege	Description
View	Users of the privilege can set or check every status but cannot create or modify any status.
Maintenance	Users of the privilege can provide rebuild, PDM, transition, media patrol and redundancy check.

Privilege	Description
Power	Users of the privilege can create (but cannot delete) disk arrays and logical drives, change RAID levels and stripe sizes and set or change components of disk arrays, logical drives and physical drives
Super	Users of the privilege have all access authorities. The users can create, delete or change all disk arrays, logical and physical drives and users.

4. After completing the entry, click [Submit].

If the user is created successfully, message "User was created successfully" appears.

The created user is added to the list in the Information tab.

Setting or changing a user account

You may select an existing user and change the display name in the Settings tab and the password in the Password tab.
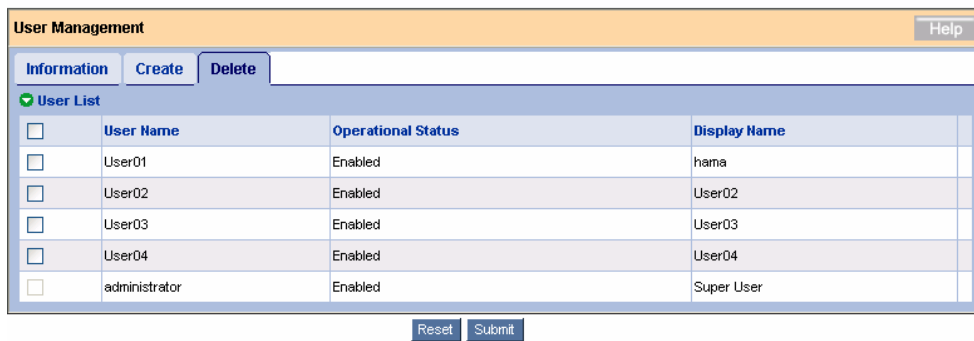

If you logon to WebPAM PRO as a super privilege user, you can select the User Privilege tab in the Subsystem/Host Management window to change the privilege levels of users.

(Selecting the User Privilege tab and clicking the link of the displayed IP address allows the privileges of registered users to be changed through pull-down menus.)

Deleting User Account

1. Logon to WebPAM PRO as an administrator, or a super privilege user.

2. Click the User Management in the Tree View and then click the Delete tab appearing in the Management Window.

User Management			Help
Information	Create	**Delete**	

⊙ User List

☐	User Name	Operational Status	Display Name	
☐	User01	Enabled	hama	
☐	User02	Enabled	User02	
☐	User03	Enabled	User03	
☐	User04	Enabled	User04	
☐	administrator	Enabled	Super User	

Reset   Submit

3. Check the checkbox located to the left of each user to be deleted and click [Submit].

The confirmation dialog box appears. Click [OK].

https://localhost:8443	□ ✕
? Are you sure to delete user(s)?	
	✗ Cancel ◄▌OK

Now the specified user accounts are deleted.

IMPORTANT: Administrator accounts cannot be deleted.

3.5 Several Settings and Information Review

Clicking an icon on the Tree View allows the relevant information to be displayed on the Management View.

In the Management Window, you can view the following information or set several features.

3.5.1   Subsystem (ST EX4650EL) Icon

If you select the subsystem (ST EX4650EL) icon in the Tree View, the controller information screen appears in the Management Window. This screen indicates the information on BIOS and drivers. In addition, the screen allows you to set various information including performance, provide redundancy check and check or delete scheduling of media patrol.

Information tab

The Information tab indicates the information on the subsystem.

Clear Statistics - Clears the statistical information accumulated for the controller. Do not manipulate this item because it is provided only for maintenance.

Settings tab

The Settings tab allows you to set an alias of the subsystem. If you enter a name in the Alias field and click [Submit], the subsystem name in the Tree View will be changed to the entered name at the screen update timing.

Firmware Update tab

The Firmware Update tab allows the firmware for the RAID card to be updated from WebPAM PRO. Do not manipulate this tab generally because it is provided only for maintenance.

Health tab

The Health tab indicates the health status of the controller, disk arrays, logical drives, spare drives and connected HDDs.

Event tab

If you click the center of the Event tab, then the log information saved in the RAMs on the RAID card (runtime events) appears.

If you click the downward arrow at the right end of the tab, then the log information (subsystem events) saved in NVRAMs appears in addition to runtime events.

> **NOTE:** You cannot sort the list in this screen.

Background Activities tab

If you click the center of the Background Activities tab, then the progresses of tasks being executed, the priority of each tack and other information appear.

Clicking the link of a task being progressed allows detailed information to be displayed further.
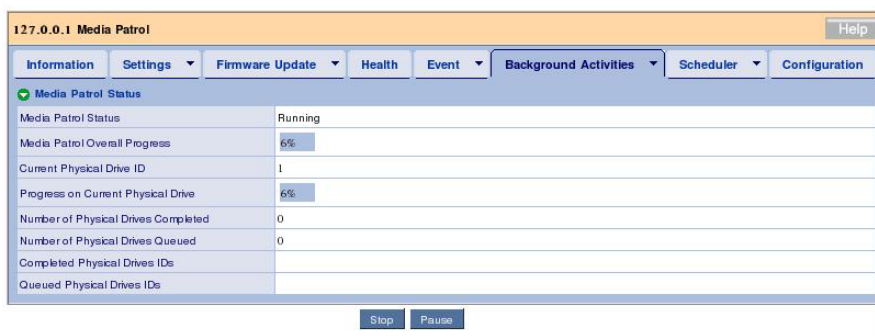
If you click the downward arrow at the right end of the tab, then a menu item for changing the priorities of tasks (Settings) and those for starting tasks appear.
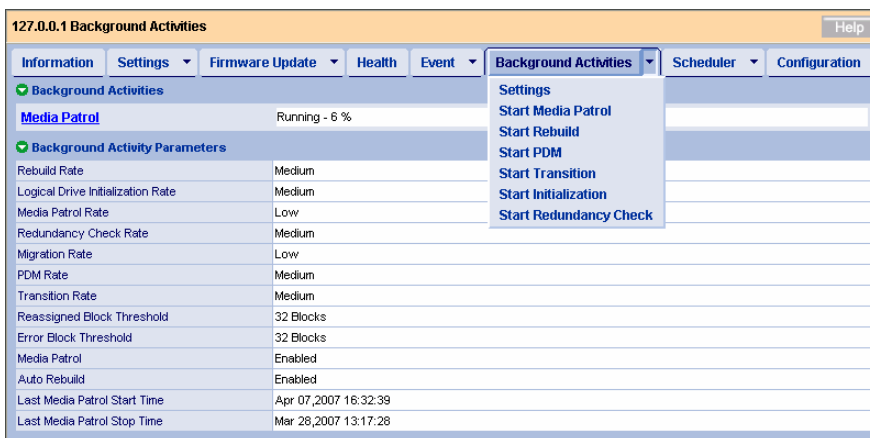
Settings menu
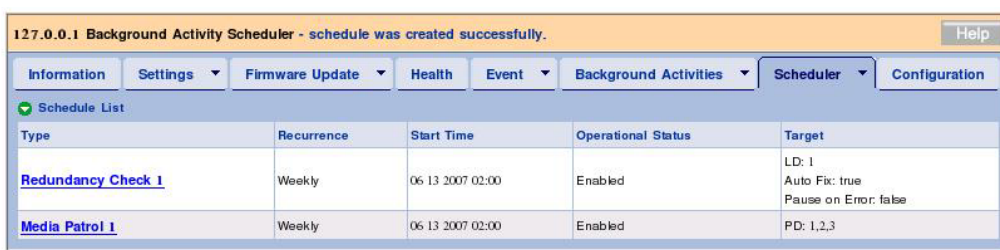
Rebuild Rate	Set the priority of rebuild processing. The default is Medium.
Logical Drive Initialization Rate	Set the priority of logical drive initialization. The default is Medium.
Media Patrol Rate	Set the priority of media patrol. The default is Low.
Redundancy Check Rate	Set the priority of redundancy check. The default is Medium.
Migration Rate	Set the priority of expansion. The default is Low.
PDM Rate	Set the priority of PDM. The default is Medium.
Transition Rate	Set the priority of transition. The default is Medium.
Reassigned Block Threshold	Set the reassigned block threshold. The default is 32.
Error Block Threshold	Set the error block threshold. The default is 32.
Enable Media Patrol	Set whether the media patrol is enabled or not. The default is [Enable].
Enable Auto Rebuild	Set whether the auto rebuild is enabled or not. The default is [Enable].

When you change a setting value but want to return it to the value at the screen display, click [Reset]. To change a setting value and enable the new value, click [Submit]. To return to the recommended default value (set in the above screen image), first click [Default] and then [Submit].

> **IMPORTANT:** The information is set to proper values by
> default. Do not change the settings.

Scheduler tab

If you click the center of the Scheduler tab, then tasks already scheduled are listed.

Type	Recurrence	Start Time	Operational Status	Target
Redundancy Check 1	Weekly	06 13 2007 02:00	Enabled	LD: 1 Auto Fix: true Pause on Error: false
Media Patrol 1	Weekly	06 13 2007 02:00	Enabled	PD: 1,2,3

One or more tasks may be scheduled. If you click the link of a scheduled task, the detailed settings appear.

This screen allows you to change the information on a scheduled task. The procedure is the same as that for creating a schedule.

If you click the downward arrow at the right end of the tab, you can create a new schedule or delete an existing schedule. See the description of each task for details.

Configuration tab

For details of the Configuration tab, see "3.18 Collecting Configuration Information."

3.5.2   Controller

If you expand the Controllers icon in the Tree View, then the information on the controller connected now appears. Clicking the icon of the controller displayed by the expansion allows the information to be displayed in the Management Window. On the screen, you can check the status information of the controller or provide settings for batteries and buzzers.
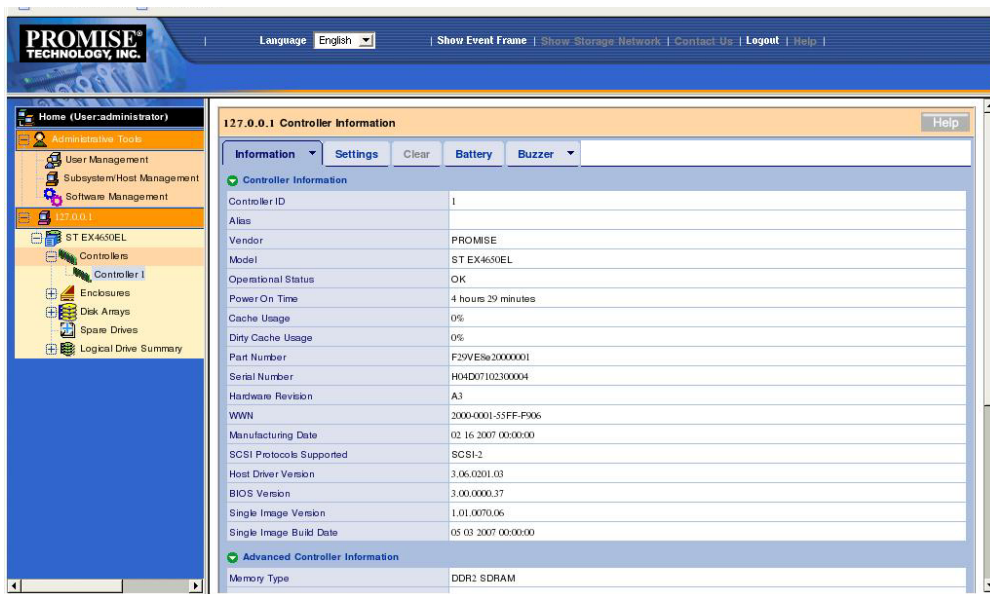
Information tab

The Information tab indicates the information on the controller.

Settings tab

The Settings tab allows you to set alias of the controller, provide settings on S.M.A.R.T. detection or set write cache of the controller. The information is set to proper values by default. As a rule, do not change the settings.

> **IMPORTANT:**
>
> ■ The information is set to proper values by default. As a rule, do not change the settings.
>
> ■ If you put or remove a checkmark in Enable SMART Log or Enable Coercion check box, it is validated immediately, regardless of clicking of Submit or Reset button.

<Description of major items>

Adaptive Writeback Cache	Adaptive Writeback Cache controls the write cache mode for all of the logical drives per controller base.
	Checked: When the following conditions match, the write policy of all logical drives under the controller sets to "Write Through", regardless of the write policy setting for individual logical drive. - Operational Status: status EXCEPT FOR "Fully Charged" - Estimated Hold Time: less than 70 hours - Battery Temperature: Above 60 centigrade. Unchecked: The write cache mode of individual logical drive depends on the setting of each logical drive. For details of the settings of battery, see "Battery" section described below. For details of the settings of write cache mode for each logical drive, see "3.5.9 Logical Drive."

Battery tab

The Battery tab indicates the current information on the battery if connected.

127.0.0.1 Batteries Information		Help
Information ▼	Settings	Clear	**Battery**	Buzzer ▼		
● Batteries Information	
Device	1
Operational Status	Fully Charged
Battery Chemistry	Li-ion
Manufacturing Date	Jul 26 2006
Remaining Capacity	100 %
Battery Cell Type	1-cell
Estimated Hold Time	92 Hours
Temperature Threshold Discharge	60 ºC / 140 ºF
Temperature Threshold Charge	60 ºC / 140 ºF
Battery Temperature	45 ºC / 113 ºF
Cycle Count	2
Voltage	4187 mV
Current	0 mA

<Description of major items>

Operation Status	Fully Charged: The battery is fully charged.
	Charging: The battery is being charged.
Estimated Hold Time	Indicates the estimated hold time of the battery.
Battery Temperature	Indicates the temperature of the battery.

Without battery connection, message "No Battery detected" appears.

Buzzer tab

If you click the center of the Buzzer tab, the current buzzer setting appears.

Clicking the downward arrow at the right end of the tab and selecting "Settings," you can change the buzzer setting. If the setting is changed, click [Submit] to enable the new setting. Buzzer ringing is disabled by default.

3.5.3   Enclosure

If you expand the Enclosure icon in the Tree View, then the overview of the current enclosure and the information on connected physical drives appear.

Information tab

The information tab indicates the information on the enclosure.

FRU VPD tab

The FRU VPD tab indicates the information on the controller and battery.

3.5.4   Physical Drives

If you click [Physical Drives] below the Enclosure icon in the Tree View, then the information on physical drives connected to the enclosure appears.

Information tab

The Information tab lists all physical drives.

Global Settings tab

The Global Settings tab allows you to provide settings on write and read caches for all physical drives.

IMPORTANT:

- "SATA Drive Settings" is not supported.

- The write cache option is provided for HDDs and different from the cache on the disk array controller. For the setting of write cache for logical drives in battery installation, see the description of setting write cache for each logical drive in "3.6.5 Logical Drive."

- It is recommended to set write cache for HDDs to [Disable] (no check). If you feel poor performance of HDDs, take proper measures for preventing instantaneous power interruption including use of an uninterruptible power supply (UPS) and set the write cache to [Enable] (checking).

- Even if you change the following settings, they return to the default values after restarting the system.
  - Enable Write Cache
  - Enable Read Lock Ahead Cache
  - Enable Command Queuing
  - Enable Read Cache

BBM tab

The BBM (Bad Block Mapping) tab allows you to check bad blocks in all physical drives. Detecting an irreparable block in a physical drive, WebPAM PRO registers the information in this list.

3.5.5   Physical Drive

If you click a specific Slot icon below Physical Drives in the Tree View, then the information on the HDD appears in the Management Window.

Information tab

<Description of major items>

Operation Status	OK	The physical drive operates normally.
	Rebuilding	The physical drive is being rebuilt.
	OK, PDM Running	The physical drive is running PDM.
	OK, Media Patrol Running	The physical drive is running media patrol.
	OK, Transition Running	The physical drive is running transition.
	OK, Migration Running	The physical drive is running migration.
	Dead, Forced Offline	Force Offline has been done.
	OK, Forced Online	Force Online has been done.
	Dead	The Disk Array of which the physical drive consists is in Degraded or Offline status.
	Stale, PFA	S.M.A.R.T. error has occurred.

Settings tab
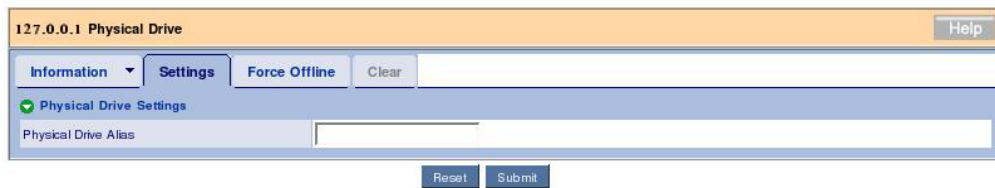
The Settings tab allows you to set an alias of the physical drive.

If you change the value to another, click [Submit] to fix it.

Force Offline/Online tab

The Force Offline/Online tab enables you to force an online physical drive to go offline or an offline physical drive to go online.

> **IMPORTANT:** Forcing a physical drive offline or online is likely to cause data loss. Be sure to back up your data before you proceed.

Clear tab

The Clear tab only appears when either of the following conditions is present.

- A fault occurs in a physical drive configuring logical drives and the physical drive contains obsolete logical drive information incompletely.

- A preventive maintenance error occurs in a physical drive.

3.5.6 Disk Arrays

If you select the Disk Arrays icon in the Tree View, all disk arrays are listed in the Management Window.

Information tab

The Information tab lists existing disk arrays.

Create tab

For the Create tab, see "3.6 Creating Disk Array and Logical Drive."

Delete tab

For the Delete tab, see "3.7 Deleting Disk Array and Logical Drive."

3.5.7 Disk Array

If you click a specific disk array (DA) icon below "Disk Arrays" in the Tree View, then the information on the disk array appears in the Management Window.

<Description of major items>
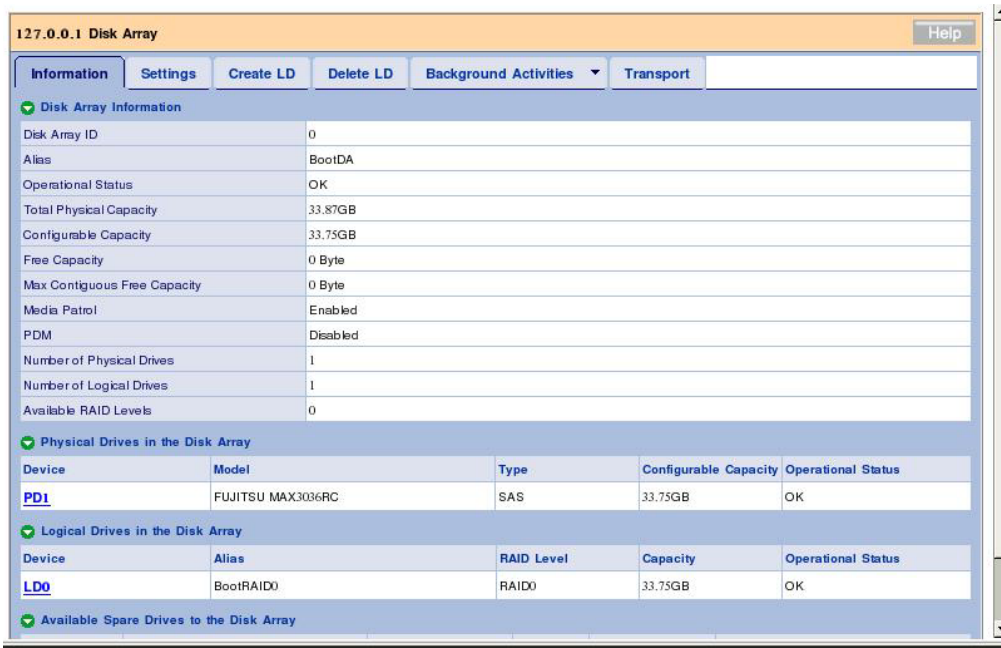
Operation Status	OK	The disk array operates normally.
	Degraded	One of the members of the disk array is in abnormal status.
	Offline	The disk array is in offline status.
	OK, Rebuilding	The disk array is being rebuilt.
	OK, PDM Running	The disk array is under PDM.
	OK, Transition Running	The disk array is under Transition.
	OK, Migration Running	The disk array is under expansion.
	Transport Ready	The disk array is ready for transport.

Settings tab

The Settings tab allows you to enable or disable the alias, media patrol and PDM.

> **IMPORTANT:** If an error occurred in any HDD in logical drive while the PDM feature is being enabled, the data is copied onto the spare drive automatically. Consequently, the slot location initially assigned for a physical drive configuring logical drives may be changed. Consideration must be taken into account to use the PDM feature. See "3.11 PDM" for details.

Create LD tab

For the Create LD tab, see "3.6 Creating Disk Array and Logical Drive."

Delete LD tab

For the Delete LD tab, see "3.7 Deleing Disk Array and Logical Drive."

Background Activities tab

If you click the center of the Background Activities tab, the BGA being run in the selected disk array appears. Clicking the arrow at the right end of the tab allows the BGA start menu executable at the RAID level (including expansion, rebuild, PDM and transition) to be displayed. See the section describing each BGA for details.

Transport tab

For the Transport tab, see "3.13 Transport."

3.5.8   Logical Drives

If you select the Logical Drives icon in the Tree View, all logical drives are listed in the Management Window.

Information tab

The Information tab lists existing disk arrays.

3.5.9   Logical Drive

If you click a specific Logical Drive icon below "Logical Drive View" in the Tree View, then the information on the HDD appears in the Management Window.

Information tab

127.0.0.1 Logical Drive		Help
Information ▼	Settings	Background Activities ▼	Check Table

Logical Drive Information

Logical Drive ID	0
Alias	BootRAID0
RAID Level	RAID0
Operational Status	OK
Capacity	33.75GB
Physical Capacity	33.75GB
Number of Axles	1
Number of Used Physical Drives	1
Stripe Size	64KB
Sector Size	512Bytes
Disk Array ID	0
Read Policy	ReadAhead
Write Policy	WriteThrough
Current Write Policy	WriteThrough
Serial Number	000000000000000000000067B4415026B96C65
WWN	22D4-0001-5591-1705
Synchronized	Yes
Tolerable Number of Dead Drives	N/A
Parity Pace	N/A
Codec Scheme	N/A

<Description of major items>

Operational Status

Operation Status	OK	The logical drive operates normally.
	Critical	The logical drive is in Critical condition.
	Offline	The logical drive is in Offline condition.
	Offline, Transport Ready	The disk array is ready for transport.
	Critical, Rebuilding	The logical drive is being rebuilt.
	OK, Redundancy Checking	The logical drive is under redundancy check.
	OK, Initializing	The logical drive is being initialized.

Current Write Policy

This item indicates the status of the current write cache for this logical drive. The status varies depending on the setting of write cache for each logical drive, setting of write cache for the entire controller (Adaptive Writeback Cache), existence of battery connection and battery status in the battery connection environment. For Adaptive Writeback Cache, see "3.5.2 Controller."

Setting of Adaptive Writeback Cache	Battery status	Write Policy (setting of write cache for each logical drive)	Current Write Policy
Disable	No battery connected or abnormal status	Write Back	Write Back
		Write Through	Write Through
	Battery connected and normal status	Write Back	Write Back
		Write Through	Write Through
Enable	No battery connected or abnormal status	Write Back	Write Through
		Write Through	Write Through
	Battery connected and normal status	Write Back	Write Back
		Write Through	Write Through

Settings tab

Alias	Alias name
Read Policy	Read Cache: Uses cache in reading.
	Read Ahead: Uses cache in reading and provides read ahead. Improves performance by read ahead before request.
	No Cache: Does not use cache in reading.
Write Policy	Write Through: Does not use cache in writing.
	Write Back: Always uses cache in writing. It is expected that the setting can improve write performance.
	However, despite the setting, the actual write cache status may vary depending on the setting of write cache for the controller (Adaptive Writeback Cache) and the battery status. See the description of the Current Write Policy in the Information tab in "3.5.9 Logical Drive" for details.

If you change either or both of the policies, click [Submit] to enable the change.

> **IMPORTANT:** If you change an option for Read Policy, it is validated immediately, regardless of clicking of Submit or Reset button.

Background Activities tab

If you click the center of the Background Activities tab, the BGA being executed in the selected disk array appears. Clicking the arrow at the right end of the tab allows the BGA start menu items executable at the RAID level (including Initialize and Redundancy Check) to be displayed.

See the description of each BGA for details.

Check Table tab

If a consistency error is detected during redundancy check and the error cannot be repaired, the error is registered in the Check Table tab.

Check Table Type	All: Indicates all error types.
	Read Check: Lists read errors.
	Write Check: Lists write errors.
	Inconsistent Block: Lists inconsistent blocks detected by redundancy check.
#	No.
Table Type	Type of Read Check, Write Check or Inconsistent Block
Start Logical Block Address	LBA of first block
Count	Number of successive blocks starting from the above LBA

3.5.10 Spare Drives

If you click the Spare Drives icon in the Tree View, the information on spare drives appears in the Management Window.

Information tab

The Information tab indicates the status of the spare drives being set.

Create tab

For the Create tab, see "3.15.1 Creating a spare drive."

Delete tab

For the Delete tab, see "3.15.2 Deleting a spare drive."

3.5.11 Logical Drive Summary

The Logical Drive Summary indicates the information on all logical drives below the controller collectively. The displayed contents are the same as those appearing when you click a specific logical drive below disk arrays.

3.6 Creating Disk Array or Logical Driver

A disk array can be created in any of the following three ways.

Automatic Configuration	Checks the number of unconfigured HDDs connected currently and creates disk arrays of a proper capacity and RAID level and logical drives automatically.
Express Configuration	Creates disk arrays and logical drives semi-automatically only if you select a RAID level fit to the environment used and the number of logical drives to be created.
Advanced Configuration	Creates disk arrays and logical drives if you select or enter every parameter.

3.6.1 Automatic Configuration

1. Click Disk Arrays in the Tree View.

2. Click the Create tab in the Management Window and select Automatic Configuration.

3. Click [Submit].

Disk arrays and logical drives are automatically created.

In the automatic configuration, the RAID level to be created is automatically determined depending on the number of free HDDs as follows:

RAID0 for a single HDD
RAID1 for two HDDs
RAID5 for three HDDs
RAID5 for four HDDs

3.6.2 Express Configuration

1. Click Disk Arrays in the Tree View.

2. Click the Create tab in the Management Window and select Express Configuration.

The following options can be set.

Redundancy	Determines whether redundant logical drives are created or not. If you check the checkbox, RAID1, RAID5 or RAID10 is created depending on the number of connected HDDs available for creating logical drives. If you do not check the checkbox, RAID0 is created. Note: If only a single HDD available for creating logical drives is connected, RAID0 is created despite whether the checkbox is checked or not.
Capacity	If you check the checkbox, the maximum capacity available for the creation is set.
Performance	If you check the checkbox, the maximum read/write performance is set.
Number of Logical Drives	Enter the number of logical drives to be created.
Application Type	Select an application type suit to your purpose out of the following types: • File Server • Video Stream • Transaction Data • Transaction Log • Other Each option sets the configuration (stripe size, write policy, etc.) suitable for your purpose, however, if you want to do more detailed settings, create an array and logical drive with Advanced Configuration wizard. (See "3.6.3 Advanced Configuration".)
Automatic Update	Clicking the Update button allows the automatic update to be reflected on the Logical Drives field below this field. If you check the checkbox, the automatic update is automatically reflected on the Logical Drives field only by changing the value of "Number of Logical Drives."

The following list shows the difference of the settings for each Application Type.

Type	Stripe Size	Read Policy	Write Policy
File Server	64KB	Read Ahead	Write Back
Video Stream	1MB	Read Ahead	Write Through
Transaction Data	64KB	No Cache	Write Through -
Transaction Log	64KB	Read Cache	Write Back -
Other	64KB	Read Ahead	Write Back

The following options are automatically set.

Disk Arrays	Number of Physical Drives
	Physical Drive IDs
	Total Configurable Capacity: Total capacity configurable to logical drives
	Number of Logical Drives: Set to the number of logical drives specified for the Number of Logical Drives option above.

3. Click [Submit].

Disk arrays and logical drives are automatically created.

3.6.3   Advanced Configuration

1. Click Disk Arrays in the Tree View.

2. Click the Create tab in the Management Window and select Advanced Configuration.
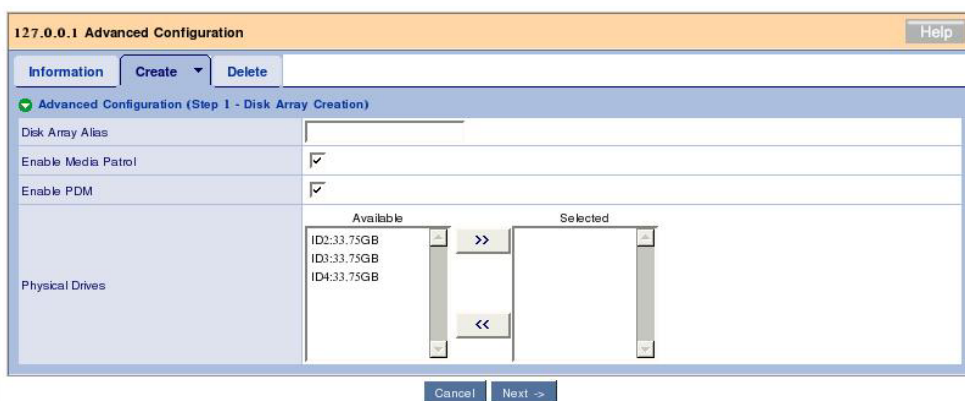
Set the items in the Create tab as shown in the table below.

Advanced Configuration (Step 1 - Disk Array Creation)

Disk Array Alias	Alias (any name)
Enable Media Patrol	Enables media patrol. The checkbox is checked by default. For details of media patrol, see "3.9 Media Patrol."
Enable PDM	Enables PDM. The checkbox is checked by default.
	If an error occurred in any HDD in logical drive while the PDM feature is being enabled, the data is copied onto the spare drive automatically. Consequently, the slot location initially assigned for a physical drive configuring logical drives may be changed. Consideration must be taken into account to use the PDM feature. For details of PDM, see "3.11 PDM."
Physical Drives	Select physical drives which you want to use to configure a disk array and click the >> button to move them to the selection list.
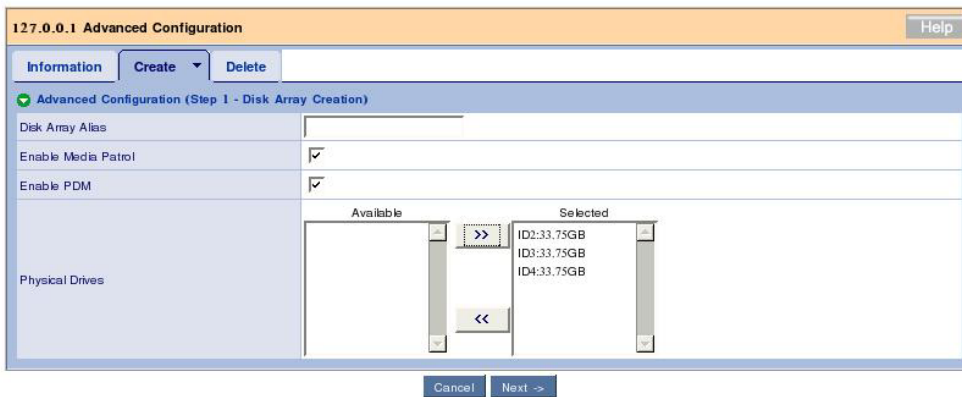
Click [Next].

3. The screen for setting details of logical drives appears.

Advanced Configuration (Step 2 - Logical Drive Creation)

Alias	Alias (any value)
RAID level	Indicates the available RAID level depending on the number of physical drives selected in the previous screen.
	RAID0 for a single physical drive
	RAID0 or RAID1 for two physical drives
	RAID0 or RAID5 for three physical drives
	RAID0, RAID5 or RAID10 for four physical drives
Capacity	Specify the capacity of a logical drive to be created. The maximum permissible capacity is shown to the right of [Max:].
Strip Block Size	Indicates the block size of a logical drive. The default is 64KB.
Sector	Indicates the sector size. The default is 512 bytes.
Read Policy	Set read policy.
	Read Cache: Uses cache in reading.
	Read Ahead: Uses cache in reading and further provides previous reading. Previous reading before request can improve the system performance (default).
	No Cache: Does not use cache in reading.
Write Policy	Set write policy.
	Write Through: Does not use cache in writing.
	Write Back: Always uses cache in writing. It is expected that this setting can improve writing performance.
	However, in spite of the setting, the actual write cache state may change depending on the write cache setting of the controller (Adaptive Writeback Cache) and the battery state.
Initialization	Set whether logical drives are initialized just after they are created.
	None: Does not initialize logical drives (default).
	Quick: Initializes master boot sectors only.
	Full: Initializes all logical drives.
	In RAID0, only "None" or "Quick" is selectable.

4. After the selections, click [Update].

The logical drive is added and displayed graphically in Capacity Usage. If some capacity remains in [Max:] of the Capacity field, clicking the Update button allows another logical drive to be added. The above configuration can be unique to each logical drive.

5. After required logical drives are added completely, click [Next].

The summary appears.

Advanced Configuration (Step 3 - Summary)

If no problems are found, click [Submit].

Disk arrays and logical drives are created.

3.6.4 Adding Logical Drives

If a disk array already created has empty capacity, logical drive can be added later.

1. Select a disk array to which you want to add logical drives and click the Create LD tab.

The logical drives already created are displayed graphically with the colors of their RAID levels.

The following procedure is the same as the description of "Advanced Configuration (Step 2 - Logical Drive Creation)" in "3.6.3 Advanced Configuration."

3.7 Deleting Disk Array or Logical Drive

> **IMPORTANT:** Delete neither disk arrays nor logical drives saving Windows file systems. Before a disk array or logical drive can be deleted, you must confirm that the disk array or logical drive does not save any Windows system file.

3.7.1 Deleting Disk Array

1. Click a disk array icon which you want to delete in the Tree View.

2. Click the Delete tab in the Management Window.
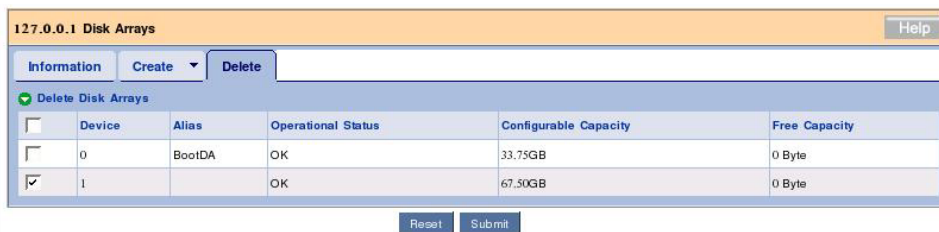
Check the checkbox of the logical drive to be deleted and click [Submit].

3. The confirmation dialog box appears. Type "confirm" and click [OK].

3.7.2 Deleting Logical Drive

Logical drives subordinate to a disk array can only be deleted.

1. Select a disk array that contains logical drive which you want to delete in the Tree View and click the Delete LD tab.

Check the checkbox of the logical drive to be deleted and click [Submit].

2. The confirmation dialog box appears. Type "confirm" and click [OK].

3.8 Redundancy Check

Routine redundancy check allows consistencies to be detected, checked and repaired to prevent rebuild from failing at occurrence of a fault in an HDD. This is possible for logical drives of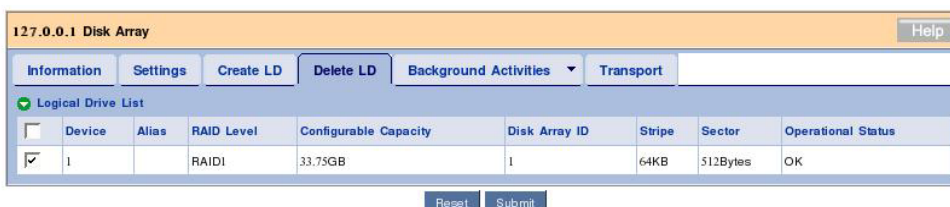 RAID level 1, 10 or 5. The redundancy check can also repair bad sectors detected during inconsistency check. To keep a RAID system operating stably, it is highly recommended to provide routine redundancy check by using the scheduling feature.

The redundancy check is executable however system load may be and thus can be used in a system environment where accessing to HDDs occurs frequently to always apply high load to them.

IMPORTANT:

- Redundancy check for a logical drive not full-initialized or not subject to redundancy check in the Auto Fix mode at all is forcibly set to the Auto Fix mode.

- Note that load is applied to the system to decrease its processing rate during redundancy check.

To provide a logical drive with redundancy check, follow the procedure below.

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the downward arrow at the right end of the Background Activities tab in the Management Window and then click Start Redundancy Check.

3. Make settings required for the redundancy check.

Redundant Logical Drive	Select a logical drive to be subject to redundancy check from the pull-down menu.
AutoFix	Set processing to be done when an inconsistency error is detected.
	If Auto Fix is checked, data in other HDDs configuring RAID is repaired at detection of an inconsistency error.
	If Auto Fix is not checked, any inconsistency error detected is not repaired.
Pause On Error	Set whether the processing is paused when an inconsistency error is detected.
	If Pause On Error is checked, processing is paused at detection of an inconsistency error. However, if Auto Fix is also checked, processing is paused only when the error cannot be repaired.
	If Pause On Error is not checked, the processing is not paused in spite of detection of an inconsistency error.

4. Click [Submit].

The redundancy check is started.

The progress of the redundancy check appears in the Background Activities tab. If you click the link of the displayed task being advanced, the current progress status appears. On the screen, you can pause or stop the task.

Click
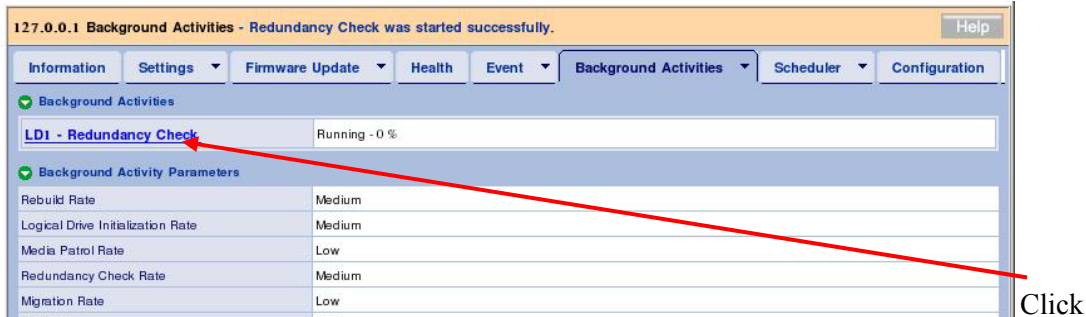
You can see the Progress bar.
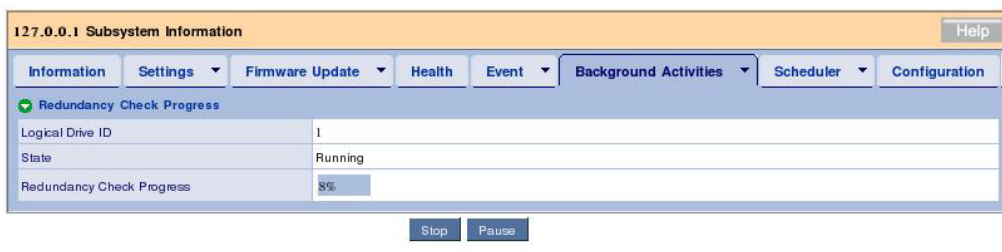
NOTES:

- If you try to provide a logical drive not full-initialized after its creation with redundancy check in the Auto Fix mode for the first time, the following message is registered. However, this does not have bad influences on system processing.
  ```
  Redundancy check is started on
  unsyncronized logical drive (event
  ID:1547).
  ```

- After redundancy check is completed, be sure to see the event log to check whether one or more errors occur during the redundancy check. If a media error occurred, a message indicating the occurrence appears before the message showing that the redundancy check is completed without any problem.

- If rebuild is done for a logical drive at a time when redundancy check of the logical drive is previously scheduled, the redundancy check is skipped.

- While redundancy check is run to a logical drive, a time when another scheduled redundancy check is to be run to the logical drive may come. If so, the scheduled redundancy check is skipped.

- If the power is off at a time when redundancy check is scheduled previously, the scheduled redundancy check is skipped.

3.8.1   Scheduling Redundancy Check

To schedule routine redundancy check, follow the procedure below.

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the downward arrow at the right end of the Scheduler tab in the Management Window and then click Add BGA Scheduler.

3. Set the following values and click [Next].
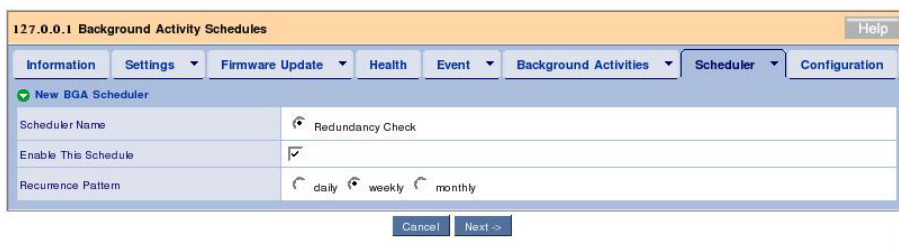
Scheduler Name	Select the Redundancy Check radio button. (In the above screen, only the Redundancy Check option appears. However, depending on the environment, the Media Patrol option may appear.
Enable This Schedule	Check the checkbox.
Recurrence Pattern	daily: Redundancy check is done at the defined time everyday.
	weekly: Redundancy check is done on the defined day of every week.
	monthly: Redundancy check is done on the defined date every month.

4. Set the following values.

(The figure below appears when you select "weekly" as the Recurrence Pattern.)
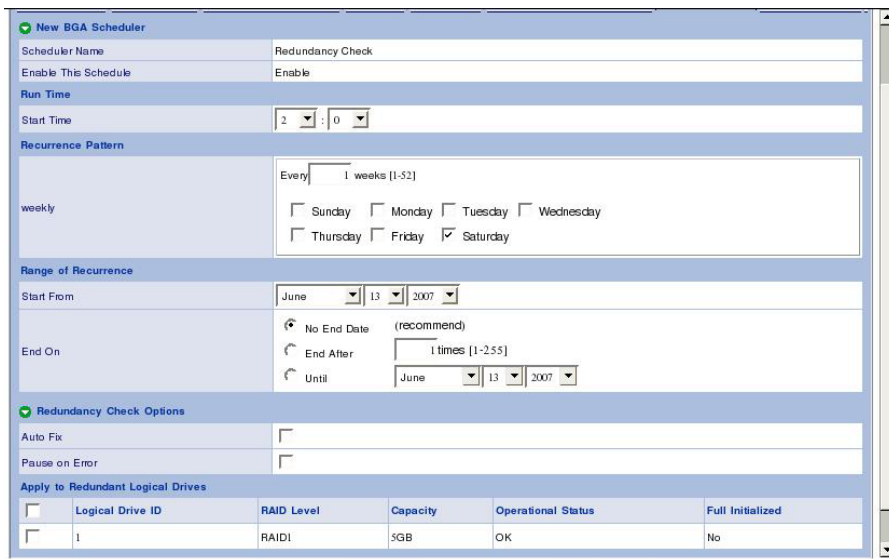
(Do not provide setting for any option with "*unavailable." Failure to follow this instruction may cause the system to operate improperly.)

| Run Time - Start Time	Enter the start time. You can set the hour with the left pull-down menu and the minute in five minutes with the right pull-down menu.
Recurrence Pattern	The display screen varies depending on the Recurrence Pattern selected in the previous screen. [daily] • [Every–days] (*unavailable) [weekly] • [Every–weeks] (*unavailable) • Check the checkbox of the day of the week on which you want to run redundancy check. [monthly] • [Day of Month] Set the date on which you want to run redundancy check every month. [The] (*unavailable) • Check the checkbox of the month in which you want to run redundancy check.

Range of Recurrence	Start from: Start date
	
	 End on–No End Date: Select this option.
	
	     –End After: (*unavailable)
	
	     –Until: (*unavailable)

Redundancy Check Options	[Auto Fix] Set the processing to be performed when an inconsistency error is detected. If the checkbox is checked, data is repaired from other HDDs configuring RAID at detection of an inconsistency error. If the checkbox is not checked, a consistency error is not repaired at detection of the error. [Pause on Error] Set whether processing is paused if an inconsistency error is detected. If the checkbox is checked, processing is paused at detection of an inconsistency error. However, if Auto Fix is also checked, processing is paused only when the error cannot be repaired. If the checkbox is not checked, the processing is not paused in spite of detection of an inconsistency error. Note: Redundancy check without Auto Fix for a logical drive not initialized or not subject to redundancy check in the Auto Fix mode at all cannot be scheduled. If you try, the following message is registered and the redundancy check is not done. Failed to create the scheduler: Redundancy Check can not be scheduled for logical drive x as it is not Fully initialized or AutoFix is not enable In this case, schedule the redundancy check in "Auto Fix."

Apply to Redundant Logical Drives	Check the checkboxes of logical drives for which you want to schedule redundancy check.

Do not use the options with "*unavavailable" suffixed in the above list.

5. After the settings are completed, click [Submit].

Click [Back] to return to the previous screen. Click [Cancel] to cancel the settings.

If redundancy check is scheduled, the screen display changes to the schedule list screen. The scheduling just set is added to the list. Message "schedule was created successfully." appears at the top of the tab.
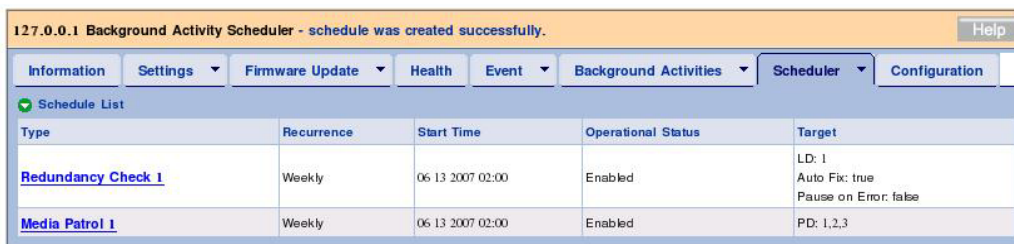
The above procedure can make scheduling.

If the time reaches to the start time having been set, the redundancy check is started. The redundancy check is repeated at the intervals entered in step 3.

> **IMPORTANT:** Redundancy check without Auto Fix of a logical drive not full-initialized or not subject to redundancy check in the Auto Fix mode at all cannot be scheduled.
> If you try, the following message is registered and redundancy check is not done.
> ```
> Failed to create the scheduler: Redundancy
> Check can not be scheduled for logical drive
> x as it is not fully initialized or AutoFix
> is not enabled.
> ```
> In this case, run redundancy check in Auto Fix once.

Changing schedule setting

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the Scheduler tab in the Management Window and then click the link of the redundancy check for which you want to change the schedule setting.

The following procedure is the same as that for creating a schedule.

Suspending (deleting) schedule setting

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the arrow at the right end of the Scheduler tab in the Management Window and then

click Delete Schedules.

3. Check the checkbox of the redundancy check which you want to delete and click [Submit].

The confirmation dialog box asking whether the redundancy check may be deleted appears. Click [OK].

> **NOTE:** You can set a single schedule of redundancy check for a single logical drive.

3.9 Media Patrol

The media patrol feature provides entire reading for the following target HDDs. Because of aged deterioration, it may not be possible to detect faults of HDDs until they are accessed. The media patrol, or routine read and check of data in HDDs, allows such faults to be detected as soon as possible. Therefore, you can take proper measures early.

- HDDs configuring RAID

- Spare HDDs

If accessing to a HDD occurs during media patrol, the media patrol is paused until the completion of the access. Accordingly, media patrol hardly degrades the system performance. Because the media patrol feature checks HDDs in a period of low system load, it may not be able to advance its processing in a system entered in high load status consistently. Therefore, use the feature in system environment of comparatively low load such as in the night.

IMPORTANT:

- Media patrol is scheduled by default to be run at 0:00 a.m. on Wednesday every week just after installation of WebPAM PRO. Change the schedule to be suit to the environment you use.

- The RAID system does not allow media patrol to be set in HDDs individually.

- Media patrol is not done for HDDs having not been used to configure a disk array or for HDDs not specified as spare. Specify unconfigured HDDs to hot spare.

- Media patrol can detect media errors of HDDs early and only repair HDDs being members of redundant RAIDs. However, it does not check whether HDDs are consistent with parity.
- The feature can run media patrol of specified HDDs at the specified time only once (scheduled media patrol is run periodically every specified start time). Media patrol is not run consistently.


Follow the procedure below to provide media patrol.

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the downward arrow at the right end of the Background Activities tab in the Management Window and then click Start Media Patrol.
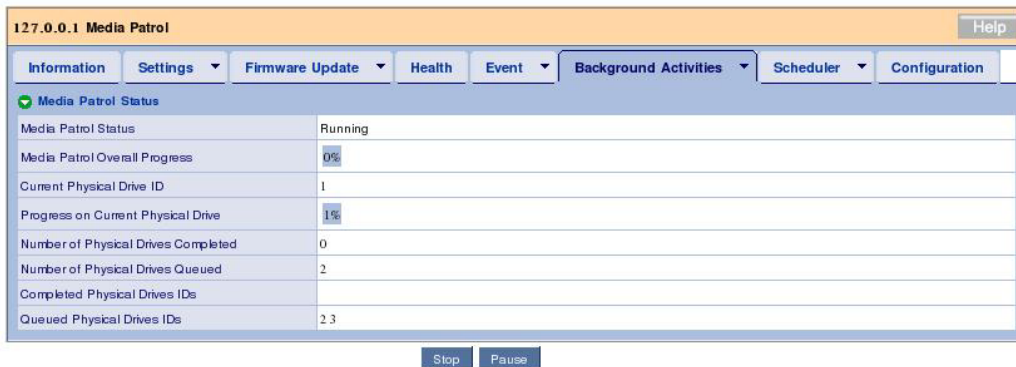
3. Click [Start].

The media patrol is started.

The progress of the media patrol appears in the Background Activities tab. If you click the link of the displayed task being advanced, the current progress status appears. On the screen, you can pause or stop the task.

Click
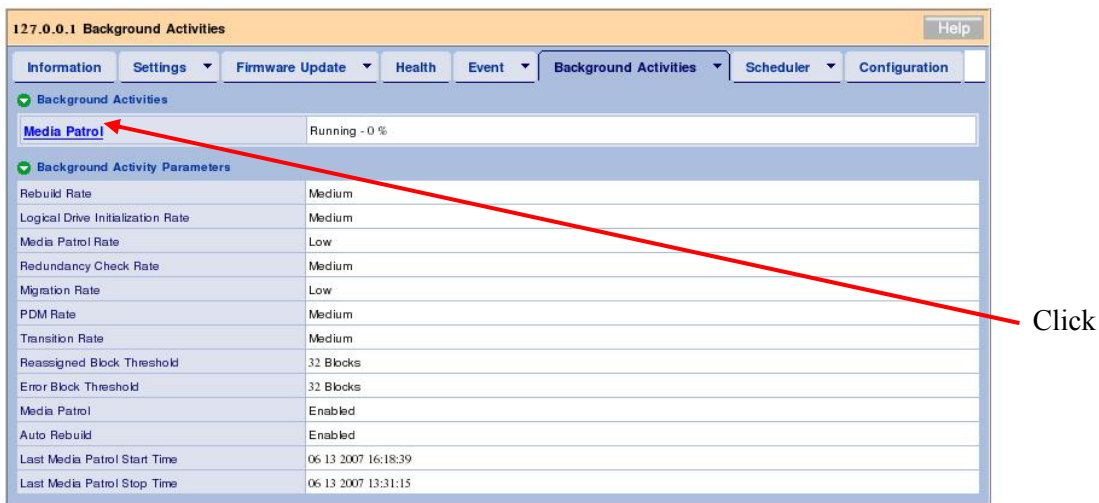
You can see the Progress bar.

The following items appear in the screen indicating the progress of the media patrol.

Media Patrol Status	Indicates the status of media patrol.
Media Patrol Overall Progress	Indicates the progress of media patrol on all connected HDDs.
Current Physical Drive ID	Indicates the ID of the physical drive being subject to media patrol.

Progress on Current Physical Drive	Indicates the progress of the current media patrol on a physical drive.
Number of Physical Drives Completed	Indicates the number of physical drives on which media patrol has already been completed.
Number of Physical Drives Queued	Indicates the number of physical drives on which media patrol is to be done.
Completed Physical Drives IDs	Indicates the IDs of physical drives on which media patrol has already been completed.
Queued Physical Drives IDs	Indicates the IDs of physical drives on which media patrol is to be done.

NOTES:

- During media patrol, "Yielded" may appear in the Media Patrol Status field. The media patrol is set to have the lowest running priority by default. If an access occurs during media patrol, the media patrol is paused until the completion of the access. "Yielded" appears in such a situation.

- After media patrol is completed, be sure to see the event log to check whether one or more errors occur during the media patrol. If a media error occurred, a message indicating the occurrence appears before the message showing that the media patrol is completed without any problem.

- While media patrol is run to a physical device, the time scheduled to another media patrol of the physical device may come. If so, the scheduled media patrol is skipped.

- If the power is off at the time when media patrol is scheduled previously, the scheduled media patrol is skipped.

3.9.1 Scheduling Media Patrol

NOTES:

- Media patrol is scheduled by default to be run at 0:00 a.m. on Wednesday every week just after installation of WebPAM PRO.

- Media patrol is scheduled by default to be run at 0:00 a.m. on Wednesday every week just after installation of WebPAM PRO.

- You can set a single schedule of media patrol for a single controller.

To add schedule setting of media patrol, follow the procedure below.

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the arrow at the right end of the Scheduler tab in the Management Window and then click Add BGA Scheduler.

If media patrol is already set, Media Patrol does not appear in the Scheduler Name option.

3. Set the following values and click [Next].

Scheduler Name	Select the Media Patrol radio button.
Enable This Schedule	Check the checkbox.
Recurrence Pattern	daily: Media patrol is run at the defined time everyday.
	weekly: Media patrol is run on the defined day of every week.
	monthly: Media patrol is run on the defined date every month.

4. Set the following values.

(The figure below appears when you select "weekly" as the Recurrence Pattern.)


Run Time - Start Time	Enter the start time. You can set the hour with the left pull-down menu and the minute in five minutes with the right pull-down menu.

Recurrence Pattern	The display screen varies depending on the Recurrence Pattern selected in the previous screen.
	[daily]
	• [Every–days] (*unavailable)
	[weekly]
	• [Every–weeks] (*unavailable)
	• Check the checkbox of the day of the week on which you want to run media patrol.
	[monthly]
	• [Day of Month] Set the date on which you want to run media patrol every month.
	[The] (*unavailable)
	• Check the checkbox of the month in which you want to run media patrol.
Range of Recurrence	Start from: Start date
	End on–No End Date: Select this option.
	–End After: (*unavailable)
	–Until: (*unavailable)

5. After the settings are completed, click [Submit].

Click [Back] to return to the previous screen. Click [Cancel] to cancel the settings.

If media patrol is scheduled, the screen display changes to the schedule list screen. The scheduling just set is added to the list. Message "schedule was created successfully." appears at the top of the tab.
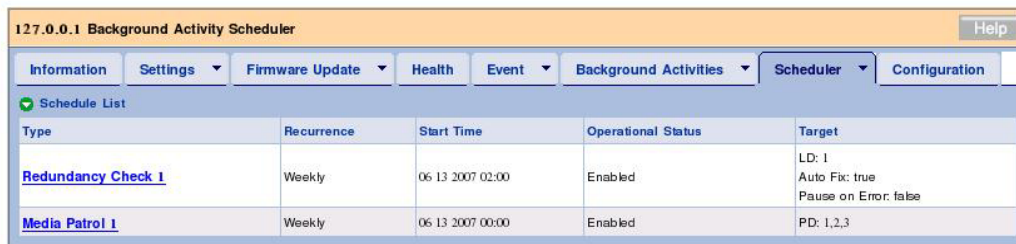
The above procedure can make scheduling.

If the time reaches to the start time having been set, the media patrol is started. The redundancy check is repeated at the interval entered in step 3.

Changing schedule setting

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the Scheduler tab in the Management Window and then click the link of media patrol for which you want to change schedule setting.

The following procedure is the same as that for creating a schedule.

Suspending (deleting) schedule setting

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the arrow at the right end of the Scheduler tab in the Management Window and then click Delete Schedules.

3. Check the checkbox of the media patrol which you want to delete and click [Submit].

The confirmation dialog box asking whether the media patrol may be deleted appears. Click [OK].

	Type	Recurrence	Start Time	Operational Status
☐	Redundancy Check 1	Weekly	06 13 2007 02:00	Enabled
☐	Media Patrol 1	Weekly	06 13 2007 00:00	Enabled

3.10 Rebuild

The rebuild feature can recover redundancy if a single HDD is defected in RAIL level 1, 10 or 5.

During rebuild, data read/write is enabled. However, the redundancy is lost until the rebuild operation is completed.

If an HDD is defected, logical drives are entered into the critical state, of which you are notified.

> **IMPORTANT:** Note that load is applied to the system to decrease its processing rate during rebuild.

3.10.1 Hot Spare Rebuild

If a redundant logical drive is degraded, hot spare rebuild is done under where all the following conditions match.

Spare drives are set.	Spare drives of either of the following types are required:
	• Spare drives set to global
	• Spare drives dedicated for logical drive entered into degraded state
Spare drives have capacity set properly.	Spare drives should have capacities equal to or larger than those of defected physical drives.

When the above conditions are met, host spare rebuild is started automatically. (The physical drives that is not configured to any disk arrays cannot be used as spare drives.)

3.10.2 Hot Swap Rebuild

Hot swap rebuild is done when the following conditions are met.

Auto Rebuild is enabled.	Enable Auto Rebuild should be checked in the Settings screen appearing in the Background Activities tab of subsystem ST EX4650EL. See the description of the Background Activities tab in "3.5.1 Subsystem (ST EX4650EL) icon" for details.
A defected physical drive is replaced with a new HDD on the same slot.	The new HDD should have a capacity equal to or larger than that of the defected physical drive.

If the above conditions are met, hot swap rebuild is started automatically.

3.10.3 Manual Rebuild

For manual rebuild, follow the procedure below.

1. Click a degraded disk array in the Tree View.

2. Click the arrow at the right end of the Background Activities tab in the Management Window and select Start Rebuild

3. Specify source and target HDDs on rebuild.

Source Physical Drive	Specify a normal physical drive used to configure a logical drive in the critical state.
Target Physical Drive	Specify the target HDD on rebuild.

4. Click [Submit].

During the rebuild operation, the progress appears in the Background Activities tab.

As soon as the rebuild is completed, the status display of logical drives is returned to the normal state.

> **NOTES:**
>
> - After rebuild is completed, be sure to see the event log to check whether one or more errors occur during the rebuild. If a media error occurred, a message indicating the occurrence appears before the message showing that the rebuild is completed without any problem.
>
> - To install a new HDD for replacement, wait for 90 sec or longer after the removal of the defected HDD.

■ If Enable Buzzer is checked in controller setting, the buzzer rings with the logical drive being in the critical or offline state or rebuilt. To turn on/off the buzzer, check or uncheck the checkbox of Enable Buzzer in the Controller Settings tab. See the description of the Buzzer tab in "3.5.2 Controller" for details. Buzzer ringing is automatically stopped when the logical drive is recovered to the normal state.

3.11 PDM

The PDM (Predictive Data Migration) feature always monitors HDDs configuring logical drives, previously senses HDDs suspected to be defected and copies data in the HDDs to spare drives. Different from the rebuild feature, PDM can be done without degrading of logical drives. After the data copy, the status display of the source HDDs becomes Stale and they are recognized as PFA error.

IMPORTANT:

- Before the PDM feature can be used, the following must previously be set.
  - Enable PDM is checked in the Settings tab of disk array. (See the description of the Settings tab in "3.5.7 Disk Array.")
  - Spare drives have already been created (if the automatic PDM feature is used).
- If an error occurred in any HDD in logical drive while the PDM feature is being enabled, the data is copied onto the spare drive automatically. Consequently, the slot location initially assigned for a physical drive configuring logical drives may be changed. Consideration must be taken into account to use the PDM feature.

PDM is automatically run under any of the following conditions.
- An S.M.A.R.T. error occurs.
- The number of bad blocks exceeds the threshold (32).
- A fatal error occurs during media patrol.

PDM may also be run manually.

To start PDM manually, follow the procedure below:

1. Select a disk array for which you want to run PDM in the Tree View.

2. Click the arrow at the right end of the Background Activities tab and select Start PDM.

3. Specify the following.

Source Physical Drive	Specify the physical drive which is suspected to be defected and from which data is desired to be copied.
Target Physical Drive	Specify a physical drive to which data is to be copied.

4. Click [Submit].

PDM is started. It may take much time depending on the capacity.

During the execution of PDM, you can check the progress.

5. When the processing is completed, the status display of source HDD becomes "Stale,PFA" and the icon in the Tree View is marked with a red cross (×). It is recommended to replace the HDD with a normal one.

3.12 Transition

At the occurrence of a fault, logical drives may be degraded and recovered by hot spare rebuild. This results in separation of the configured slot positions of the logical drives. However, creating spare drives of revertible type previously (see "3.15 Creating or Deleting Spare Drives") allows logical drives to be returned to the original successive slot positions.

> **IMPORTANT:** In the environment in which your system is always subject to load, the process of transition may take a long time and the performance may cause performance decrement. In this case, the setting of Revertible is recommended to be OFF when creating a spare drive.

The transition is useful in the following situations.

<Example of auto transition>

1. Original state (RAID5)

Create spare drives of revertible type. (See "3.15 Creating or Deleting Spare Drives" for details.)
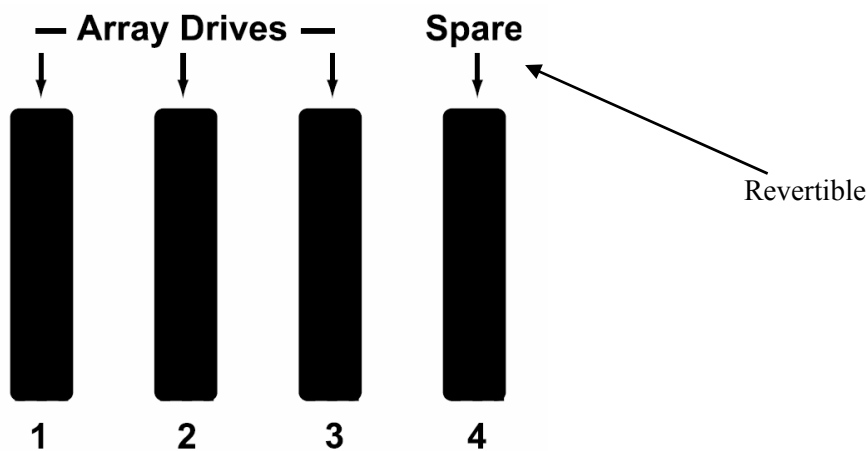
2. Occurrence of fault in PD2

A fault occurs in a physical drive among those configuring a disk array. The disk array is entered into the degraded state (logical drives are entered into the critical state).

Failed Drive

Rebuild to Spare

1   2   3   4

3. Hot spare rebuild is done by using PD4 to create a logical drive having PD1, PD3 and PD4 as configured HDDs.

⎯⎯ Array Drives ⎯⎯

1   2   3   4

4. Replace the defected physical drive with a new physical drive having a capacity equal to or larger than the capacity of the defected drive.

5. Transition is automatically started to move data from the spare drive to the new physical drive.

6. When the transition is completed, the new physical drive becomes a member of the original logical drive. The spare drive having saved the data temporarily returns to the original spare drive.
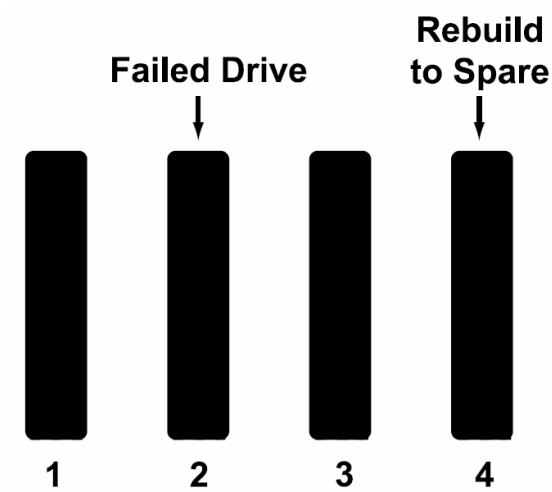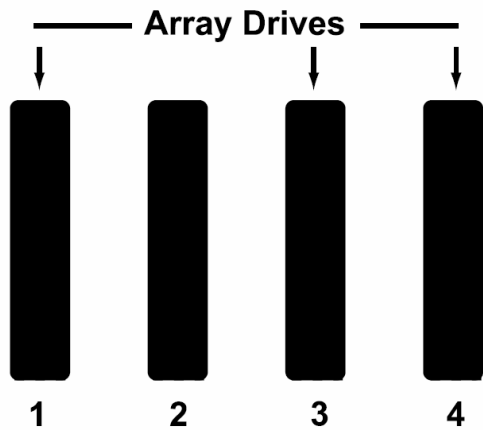
<Example of manual transition>

1. Original state: RAID1

Create spare drives of revertible type. (See "3.15 Creating or Deleting Spare Drives" for details.)
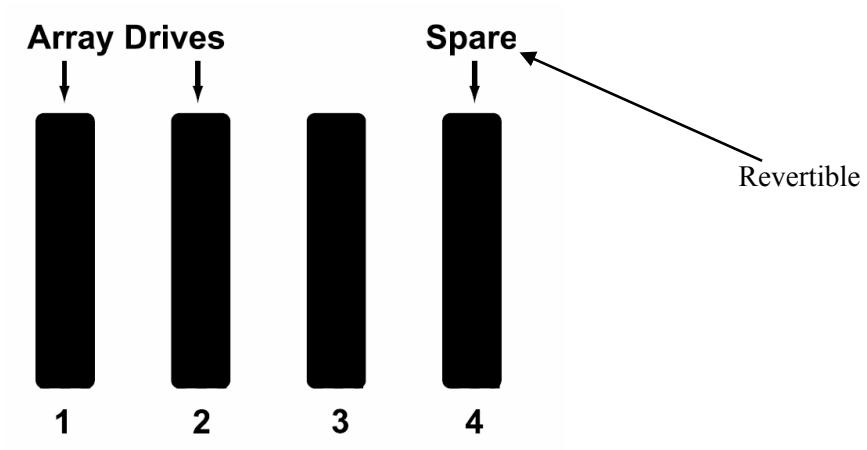
2. Occurrence of a fault in PD2

A fault occurs in a physical drive among those configuring a disk array. The disk array is entered into the degraded state (logical drives are entered into the critical state).
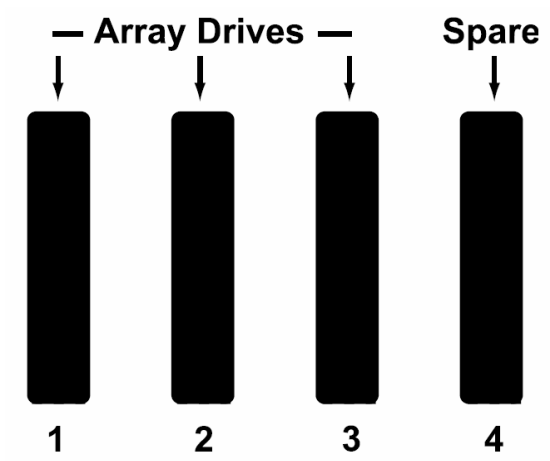
Failed Drive → (PD2) **Rebuild to Spare** → (PD4)

1　　2　　3　　4

3. Hot spare rebuild is done by using PD4 to create a logical drive having PD1 and PD4 as configured HDDs.

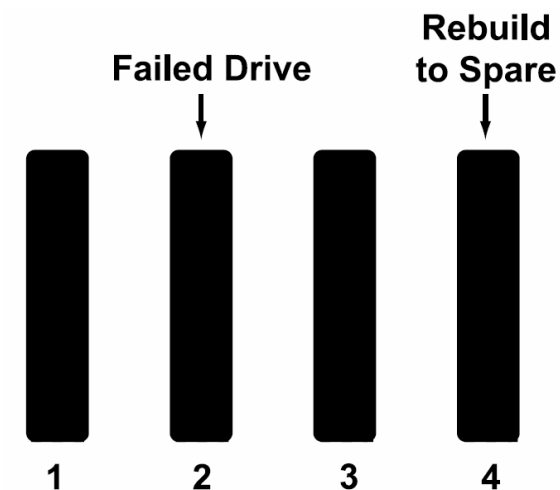4. To make free physical drive PD3 be a configured HDD of the original logical drive, you can select PD3 manually in this state to run transition.

(1) Click the arrow at the right end of the Background Activities tab and select Start Transition.

(2) Select the source and target physical drives as Source Physical Drive and Target Physical Drive, respectively. Click [Submit].

During transition, the progress is displayed in the Background Activities tab.

At the completion of the processing, the spare drive is returned to the normal state.

NOTE: The "Operation Status" field may show "Transition Running" although Transition has finished. Check the messages regarding Transition in the application log to find that the transition processing has finished.

3.13 Transport

The transport feature is used to move a disk array in the online state with its normal status remaining unchanged.

1. Click a disk array for which you want to provide transport in the Tree View and click the Transport tab.
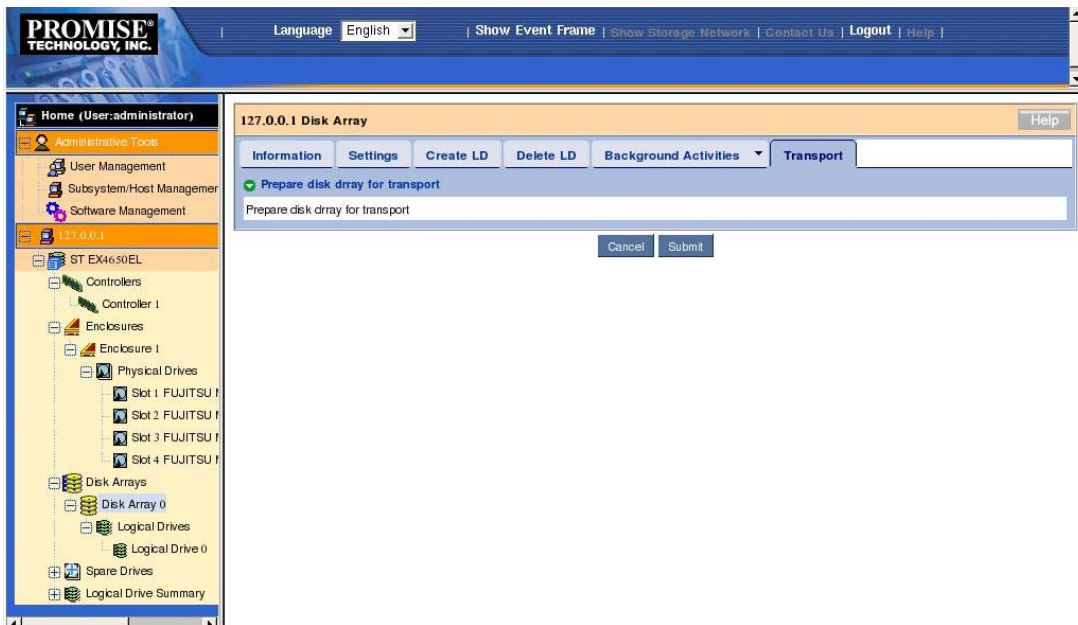
2. Click [Submit].

3. The confirmation dialog box appears. Type "confirm" and click [OK].

Input "confirm".
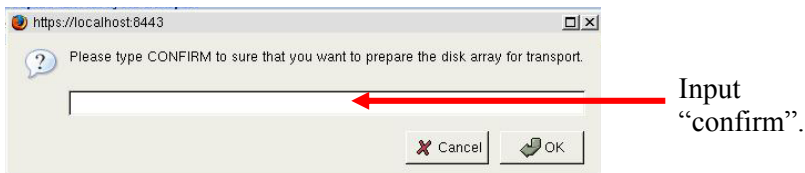
4. Make sure that Operational Status is set to "Offline, Transport Ready." Pull out the HDDs configuring the disk array from the mating slots.

Information	Settings	Create LD	Delete LD	Background Activities ▼	Transport

Disk Array Information

Disk Array ID	1
Alias	
Operational Status	Transport Ready
Total Physical Capacity	67.75GB
Configurable Capacity	67.50GB
Free Capacity	57.50GB
Max Contiguous Free Capacity	57.50GB
Media Patrol	Enabled
PDM	Enabled
Number of Physical Drives	2
Number of Logical Drives	1
Available RAID Levels	0 1

Physical Drives in the Disk Array

Device	Model	Type	Configurable Capacity	Operational Status
PD2	FUJITSU MAX3036RC	SAS	33.75GB	OK
PD3	FUJITSU MAX3036RC	SAS	33.75GB	OK

Logical Drives in the Disk Array

Device	Alias	RAID Level	Capacity	Operational Status
LD1		RAID1	5GB	Offline, Transport Ready

5. Insert the pull-out HDDs into slots in the environment subordinate to a new disk array controller N8103-105 and refresh the HDDs. Then a normal disk array is recognized.

3.14 Initializing Logical Drive

A disk array can be initialized additionally after it is created.

Full initialization set all data bits in logical drives to zero. If logical drives are created, it is recommended to run full initialization first.

IMPORTANT:

- Initialization erases all data completely. Be sure to back up important data before initialization.
- You may select a logical drive which you want to initialize from the disk array menu. However, take the following procedure for initialization to prevent an undesired logical drive from being initialized by mistake.

---

1. Select a logical drive to which full initialization is to be done in the Tree View.

2. Click the arrow at the right end of the Background Activities tab in the Management Window and select Start Initialization.

Quick Initialization	If the checkbox is checked, quick initialization is run. If not checked, full initialization is run.
	Quick Initialization: Initializes master boot sectors only.
	Full Initialization: Initializes the logical drive fully to bring consistency.
Quick Initialization Size	Enabled in quick initialization. Specifies the block size for initialization.
Initialization Patterns in Hex	Enabled in full initialization. Leave default 0 unchanged.

3. Click [Submit].

The confirmation dialog box appears. Type "confirm" and click [OK].

During initialization, the progress is displayed in the Background Activities tab.

3.15 Creating or Deleting Spare Drives

3.15.1 Creating Spare Drives

> **IMPORTANT:** The following HDDs cannot be used for spare drives.
> - HDD that has been configured to any disk array
> - HDD with partitions.

Spare drives are used to protect a redundant logical drive when hard disk drives in the logical drive are defected. That is, if a hard disk drive in a redundant logical drive is defected, rebuild can be done to a spare drive to substitute for the defected hard disk drive for protecting the logical drive. Creating spare drives are required to use the PDM or transition feature.

Follow the procedure below to create spare drives.

1. Click Spare Drives in the Tree View.

2. Click the Create tab in the Management Window.
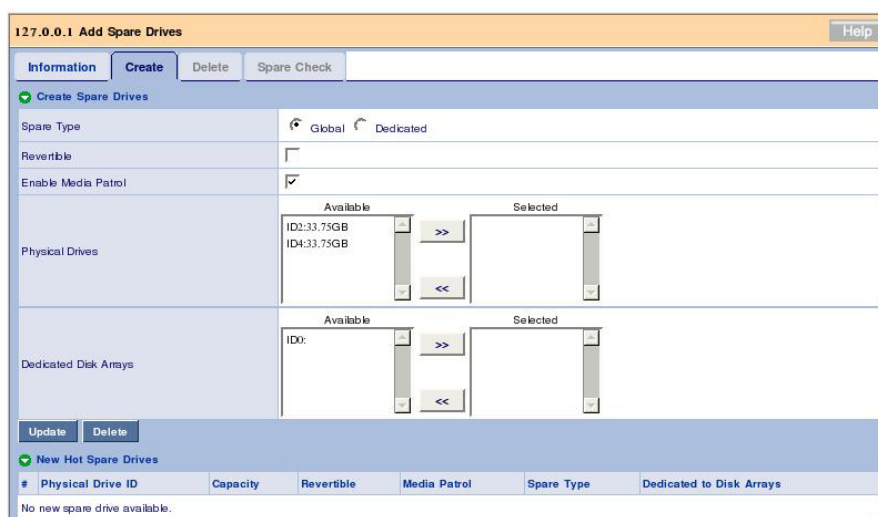
3. Set the following.

Spare Type	Global: Available to any disk arrays
	Dedicated: Available only to specified disk arrays
Revertible	Check the checkbox if the transition feature is used (see "3.12 Transition").
Enable Media Patrol	Check the checkbox.
Physical Drives	Select HDDs to be specified as spare drives from HDDs in the Available frame on the left side and click [>>]. The HDDs are moved to the Selected frame on the right.
Dedicated Disk Arrays	Specify disk arrays if Dedicated is selected as the spare type.
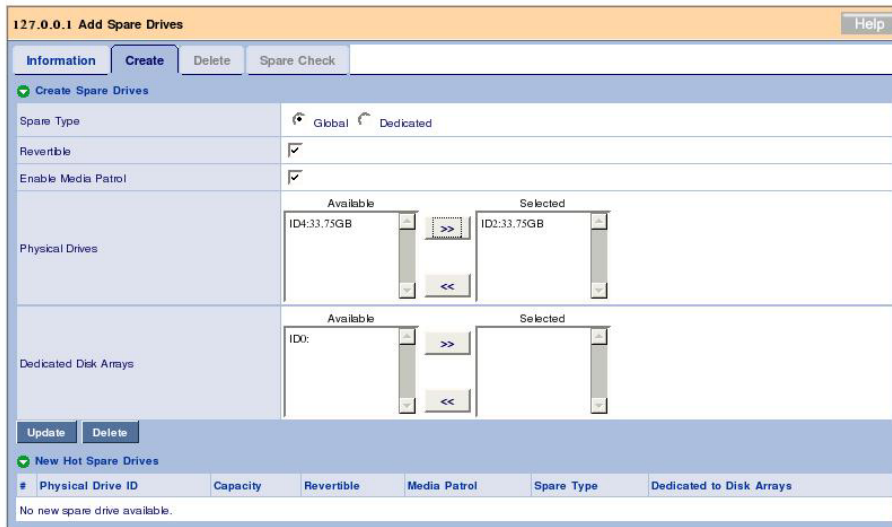
4. Click the Update button.

The specified spare drives are added to the list of New Hot Spare Drives at the bottom.

5. Click [Submit].
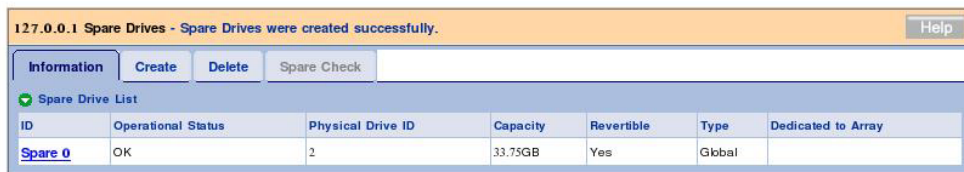
The spare drives are defined. The created spare drives appear additionally in the Information tab.

IMPORTANT:

- The HDDs that are not configured to an logical drive nor set as spare cannot be used as spare drives.

- Media patrol is not done to the HDDs that are not configured to array disk or set as spare. Specify unconfigured disks as spare disks previously.
- Set the capacity of dedicated spare to be the same as that of the dedicated disk array.

3.15.2 Deleting Spare Drives

Follow the procedure below to delete spare drives.

1. Click Spare Drives in the Tree View.

2. Click the Delete tab in the Management Window.

127.0.0.1 Spare Drives							Help

Delete Spare Drives

	Spare ID	Operational Status	Physical Drive ID	Capacity	Revertible	Type	Dedicated to Array
☐	0	OK	2	33.75GB	Yes	Global	

Reset   Submit

Check the checkboxes of spare drives to be deleted and click [Submit].

The following popup appears. Confirm the information and click [OK].

The selected spare drives are deleted.

3.16 Expansion

IMPORTANT:

- Before logical drives are provided with expansion, be sure to back up the data in the disks. If an unexpected error occurs during expansion, data in the disks may be destroyed.

- In this feature, only RAID5 configured with three physical drives can be expanded to that configured with four drives.

- For expansion, all physical drives should have the same capacity.
- This feature can expand the capacity of the logical drive. As seen from OS (Disk Management), the capacity of the HDD looks become larger than before. You can use this portion by newly creating a partition in it. (The capacity of the existence logical drive is not expanded.)
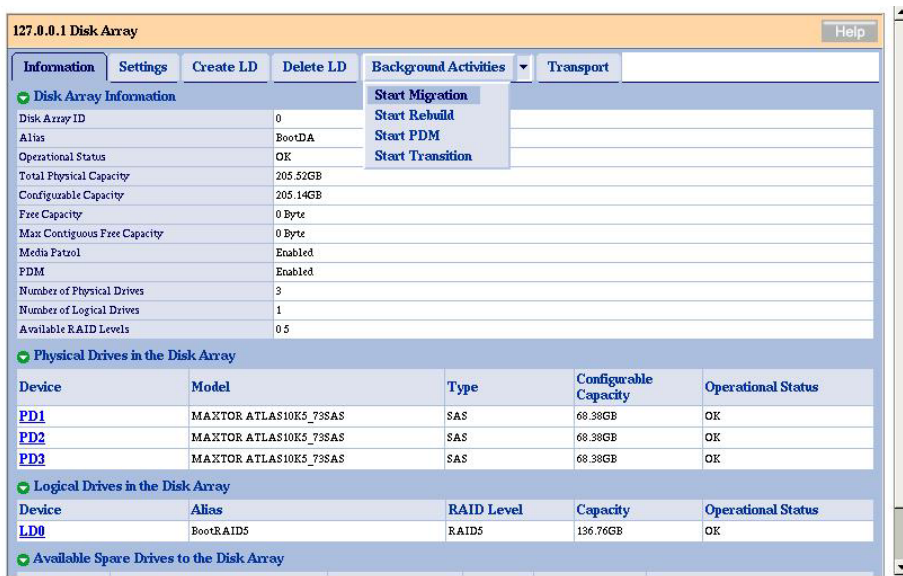
---

1. Click a disk array for which you want to provide expansion in the Tree View.

2. Click the arrow at the right end of the Background Activities tab in the Management Window and select Start Migration.

3. Select physical drives used for the expansion.

Click [>>] to move the physical drives to the Selected frame.

Click [Next].

4. Set detailed information on the disk array.
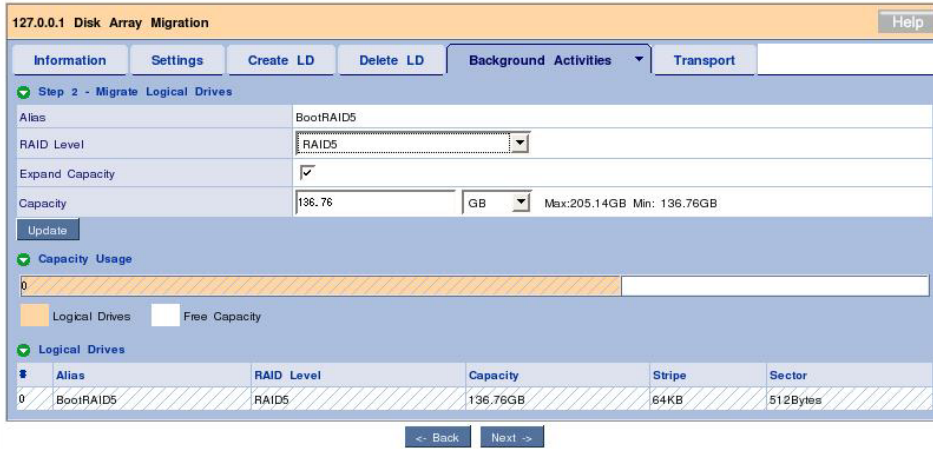
RAID Level	RAID5 only
Expand Capacity	Check the checkbox to increase the capacity. This item is grayed out if the disk array has no empty capacity.
Capacity	To increase the capacity, specify the value.

Click [Update]. The state resulting from expansion is displayed graphically in the Capacity Usage.

Click [Next].

5. The summary of the expansion to be run appears.

Click [Submit].

6. The confirmation dialog box appears. Type "confirm" and click [OK].

The screen indicating the progress of the expansion appears.

Click

You can see the Progress bar.

3.17 Event

WebPAM PRO classifies every event occurred in a RAID system as an error, warning or information to record it. This is effective to diagnose or solve faults occurred in the system.

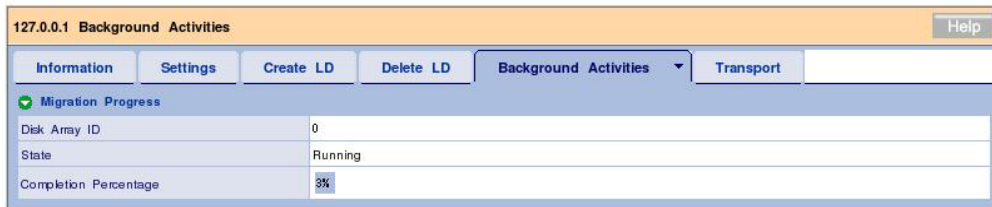> **IMPORTANT:** The log times appearing on the WebPAM PRO screen are later than the times at which the events occur. See the application log of OS to check the event occurrence times.

> **IMPORTANT:**
>
> - The log times appearing on the WebPAM PRO screen are later than the times at which the events occur. See the application log of OS to check the event occurrence times.
> - When you start WebPAM PRO first time, messages with the date of 1970s may be registered. This has no effect on WebPAM PRO operation.

Whether the Event Frame is displayed or not can be alternated by WebPAM PRO Header [Show Event/Hide Event].
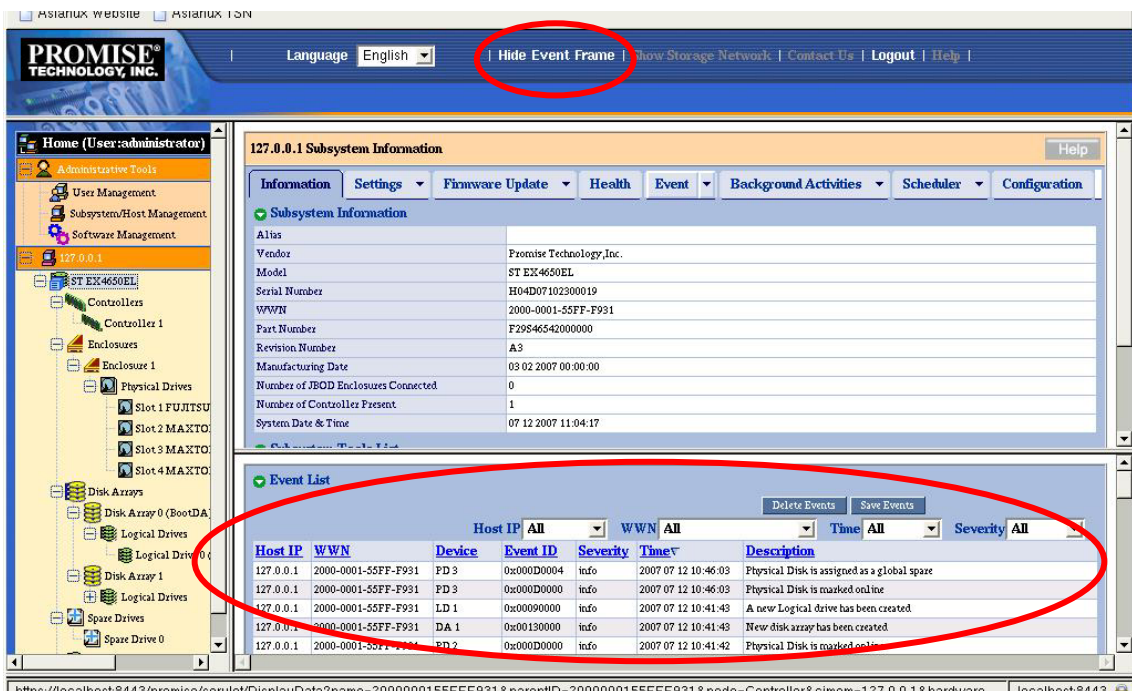
Up to 50 latest events are displayed.

Clicking [Save Events] allows events to be saved in a relevant file. Clicking [Delete Events] causes all registered events to be deleted.

If an event occurs, such a popup as shown below appears at the upper right corner of the WebPAM PRO screen.

New Event   X
Last Event: 127.0.0.1 ,2007 04 09 21:30:50
Physical Disk has been inserted
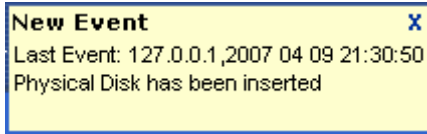
NOTE: Sorting the events is unavailable.

3.18 Collecting Configuration Information

Controller and array configuration information can be saved in a text format by specifying destination. The feature is intended for maintenance. Collect configuration information in the procedure below if you are directed by a maintenance engineer.

1. Click the subsystem (ST EX4650EL) icon in the Tree View.

2. Click the Configuration tab in the Management Window.

3. Scroll the displayed list and click [Save Configuration] at the lower right corner.

The File Download dialog box appears. Save the file to a proper place.

> **IMPORTANT:** In the Microsoft Windows 2000 environment, when you attempt to save the configuration information, message "An error occurred in the page" may appear. Even if it is the case, the configuration file has successfully been saved. This error message can be removed by clicking any place on Management Window.

Appendix A   First Logon

Perform the following procedure to make settings for security:

1.   The security alert dialog box appears.
     Click [Examine Certificate…] to display the certificate.
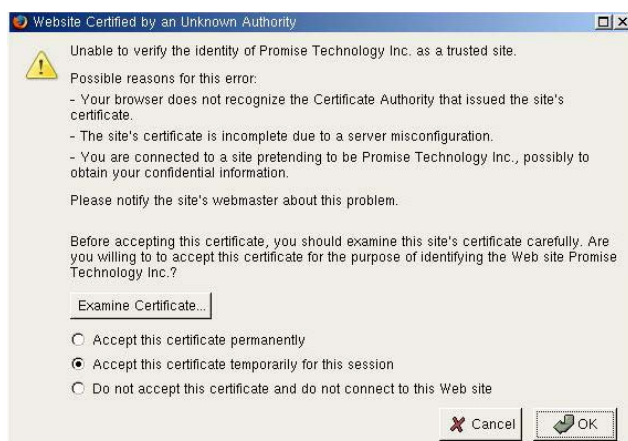
2.   The [Certificate Viewer] dialog box appears.
     After confirming the description, click [Close].
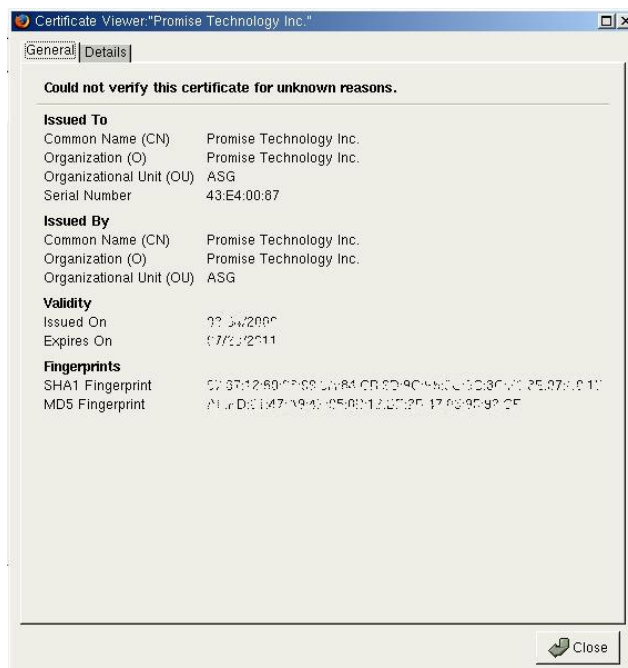
3.   To accept the certificate, click [Accept this certificate permanently] and click [OK].

     To accept the certificate temporarily, click [Accept this certificate temporarily for this session] and click [OK]. If you accept the certificate temporarily, the security alert

window will be displayed at next logon.
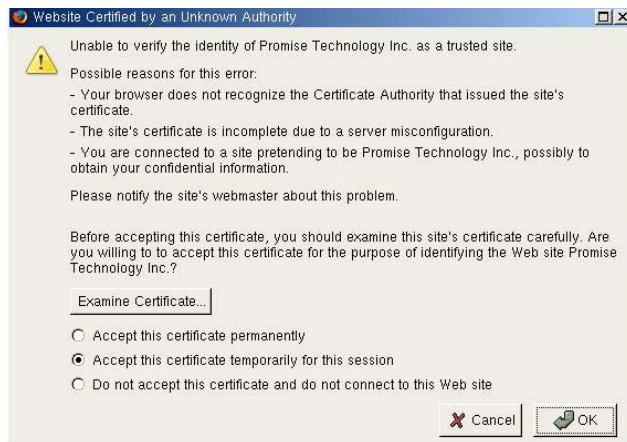
The setting for security is completed.

Appendix B Report Monitoring

To use Alert notification feature after installing NEC ESMPRO Manager, the following settings are required. (This feature can be used only in the Windows environment.)

1. Untar the WebPAM PRO installation module.

Ex.) As the WebPAM PRO installation module is "WPPInst-1.00.tar.gz":
tar -zxvf WPPInst-1.00.tar.gz

2. Start "nec\Linux\WebPAMPR\WPMALERT\WPPMANEN.EXE" in the Windows environment.

3. Click [Yes].

> **NOTE:** If you click [No], the operation terminates without setting.

4. Click [OK].

5. Reboot the system.

Alert report messages and actions

After the installation of WebPAM PRO, the following messages registered with the name "Promise Event Logger" are set as reported sources. To change the setting, redefine it by using the report setting feature of the NEC ESMPRO Agent.

Event ID	Message	Action
512	Battery temperature is above the threshold	No action required if the ID 517 message has not been registered within 8 hours. If there is no ID 517 message, the battery is required to be replaced.
517	Battery is charging	This is for checking the ID 512 message.
526	Battery is not accessible	Failure detected in battery. Check the battery and its life duration and replace it if any failure exists or it has little time left to live.
529	The write policy of writeback logical drive switched from writeback to writethru	Check the battery if any failure exists.
530	The write policy of writeback logical drive switched from writethru to writeback	Check the battery if any failure exists.
4101	Logical drive initialization marks the logical drive offline	An array became offline. Please replace the failed HDD and contact the customer or sales engineer for reconstruction..
4102	Logical Drive Initialization is aborted due to an internal error	Check HDD and cables and replace it if any failure exists.
4108	Quick Logical drive initialization marks the logical drive offline	An array became offline. Please replace the failed HDD and contact your customer engineer for reconstruction..
4109	Quick Logical Drive Initialization is aborted due to an internal error	Check HDD and cables and replace it if any failure exists.
4611	Logical drive has been placed offline. Possible Data Loss	An array became offline. Please replace the failed HDD and contact the customer or sales engineer for reconstruction.
4612	Logical drive has been set to critical	Physical drive became critical. Please replace the failed HDD and execute rebuilding. If array has hot-spare drive, rebuilding will be executed automatically.
5638	Media Patrol is aborted due to an internal error	Check HDD and cables and replace it if any failure exists.
6658	Physical Disk is marked as DEAD	Replace the failed HDD.
6659	Physical Disk has been reset	Check HDD and cables and replace it if any failure exists.
6667	Physical Disk has been removed	Physical driver has been removed. Check HDD and cables and replace it if any failure exists.
6671	Bad sector is found on physical disk	Replace the HDD with bad sectors.
6675	Previously configured disk is no longer found	Replace the failed HDD.
6677	A physical disk has encountered PFA condition	Replace the failed HDD.
6682	Physical Disk is marked as DEAD due to removal	Replace the failed HDD.
6683	Physical Disk is marked as DEAD due to the failure of Reassign	Replace the failed HDD.

Event ID	Message	Action
6684	Physical Disk is marked as DEAD due to PFA condition of the disk	Replace the failed HDD.
6685	Physical Disk is marked as DEAD due to forced offline state	Replace the failed HDD.
6149	RAID migration has encountered a physical disk error	Physical disk error detected. If it cannot be fixed, replace the HDD.
6150	RAID migration has encountered a physical disk error	Migration aborted. Please contact the sales representative for reconstruction of the array.
6154	Array was made Incomplete due to missing NV Watermark	An error occurs during Migration. Please contact the sales representative for reconstruction of the array.
7681	Rebuild is completed	Rebuild is completed. Check the status of the logical drive.
7682	Rebuild is paused	Rebuild is stopped. Restart rebuilding as soon as possible.
7683	Rebuild is resumed	No specific action required.
7684	Rebuild is stopped	Rebuild is stopped. Restart rebuilding as soon as possible.
7687	Rebuild is aborted due to an internal error	Rebuilding aborted. Please contact the sales representative.
7689	Rebuild is queued	No specific action required.
7696	Auto rebuild can not start	The capacity of unconfigured physical drive is not capable of rebuild. Replace a drive with proper capacity.
7697	Rebuild stopped internally	Rebuilding aborted. Please contact the sales representative.
1542	Redundancy check is aborted due to an internal error	Check HDD and cables and replace it if any failure exists.
1543	Redundancy check encountered inconsistent block(s)	If any error occurs in HDD, replace that HDD. If no error occurs in HDDs, back up the system data and replace all the HDDs.
1546	Redundancy check task is stopped internally	Check HDD and cables and replace it if any failure exists.
8192	SMART error is received	Replace the failed HDD.

The above table shows the event IDs in decimal. The events listed in the table are reported to NEC ESMPRO Manager. The symbols such as %1 in messages are padding characters.