PROMISE
TECHNOLOGY

Vess A-Series
Storage Appliance for Video Surveillance
Vess A3340s / Vess A3340d

Vess A3340 PoE

Product Manual

Version 1.2

About this guide

This Product Manual includes instructions for setting up and operating the available hardware versions of the Vess A3340 Storage Appliance for Video Surveillance. These models include the Vess A3340s, Vess A3340d and Vess A3340 PoE. For convenience, these models are referred to as simply Vess A3340 when describing features or operations common to all models. The specific model name is used only when it is necessary to distinguish one model from the other available models.

Please pay special attention to the warnings, cautions, important notices and notes contained throughout this guide. See the explanations of each below.

Also included are four levels of notices:

Warning

A Warning notifies you of probable equipment damage or loss of data, or the possibility of physical injury, and how to avoid them.

Caution

A Caution informs you of possible equipment damage or loss of data and how to avoid them.

Important

An Important message calls attention to an essential step or point required to complete a task, including things often missed.
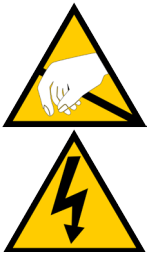
Note

A Note provides helpful information such as hints or alternative ways of doing a task.

Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Warning

The electronic components within the Vess enclosure are sensitive to damage from Electro-Static Discharge (ESD). Observe appropriate precautions at all times when handling the Vess or its subassemblies.

Warning

Turn off the power and disconnect the power cord before servicing this device.

INTRODUCTION

The Vess A-Class Storage Appliance for Video Surveillance is specially engineered for medium to large scale IP video surveillance deployment. The Vess A-Series is ideally suited for continuous surveillance in banks, malls, casinos, factories, warehouses, and similarly sized commercial, residential, governmental or private enterprises. The subsystems are capable of continuous recording and playback operation without dropping frames for networked installations of up to 80 High-Definition IP cameras.

Vess A-Class Storage Appliance for Video Surveillances are available with Windows operating systems, a Video Management Software suite, and disk drives in order to streamline the installation and integration process. The Vess A-Series subsystems are stand-alone devices with internal RAID storage, eliminating need for additional servers, controllers, separate enclosures etc. The Vess A-Series uses the renowned PROMISE RAID engine for maximum reliability, all drive bays are hot-swappable, and models are available with redundant power supplies to ensure data safety and uninterrupted operation.

> **Note**
>
> For convenience, the Vess A3340s, Vess A3340d and Vess A3340 PoE hardware models are referred to as simply Vess A3340 when describing features or operations common to all models. The specific model name is used only when it is necessary to distinguish one hardware model from the other available models.

Vess A-Series Overview

System Management

The Vess A-Series are shipped with either Windows Embedded Standard 7 Runtime (WS7P), or Windows Server 2012 R2 for Embedded System Standard/ Windows 10 IOT Enterprise.

Management Interfaces

- Browser-based management with WebPAM PROe

- Command Line Interface (CLI)

- Command Line Utility (CLU)

Specifications

Model	Vess A3340s	Vess A3340d	Vess A3340 PoE
Form factor	2U, 19" rack mount or desktop		
Function	Storage Appliance for Video Surveillance		
Operating system	Windows		
Drives supported	Eight 3.5" SATA (3Gb/s or 6Gb/s)		
Storage Expansion (iSCSI & JBOD)	Up to 128 HD		
RAID support	0, 1, 1E, 3, 5, 6, 10, 30, 50, 60		
RAID stripe size	64K, 128K, 256K, 512K, 1MB		
Max. LUNs	256/system 32/array		
Controller	Single		
Graphics	Intel® HD 5300		
Memory	8GB DDR		
Processor	Intel® Xeon E3-1275 v5 Quad-core 8-thread		
System fans	Redundant fan		
PSU	350W	350W redundant	400W + 300W PoE
Dimensions	88.2 x 446 x 410 mm	88.2 x 446 x 410 mm	88.2 x 440 x 410 mm
Weight — w/o drives	7.38 kg (16.23 lbs)	9.2 kg (20.24 lbs)	9.4 kg (20.68 lbs)
Weight — w/drives	12.9 kg (28.38 lbs)	14.72 kg (32.38 lbs)	14.92 kg (32.82lbs)

Hardware

The following section provides a summary of the front and rear panel hardware features of the Vess A-Series enclosures.

Front Panel Hardware

The front panel of Vess A-Series enclosures provide access to drives carriers. Some A-Series units are shipped with secure covers to protect the drive carriers from being unintentionally removed.

For all Vess A-Series enclosures, defective drives can be replaced without interruption of data availability to the host computer. If so configured, a hot spare drive will automatically replace a failed drive, securing the fault-tolerant integrity of the logical drive. The self-contained hardware-based RAID logical drive provides maximum performance in a compact external enclosure.

Front Panel LEDs

Descriptions of the LED behavior and function for Vess A-Series enclosures.

Front of Vess A3340

The Vess A3340 is shipped with a lockable front secure cover to provide physical security for installed hard disks and cooling unit module. Use the tubular key shipped with the unit to lock or unlock this cover to access the eight hard drive carrier trays in front.

Front view with bezel security cover

LEDs
visible through bezel

Secure panel tubular lock
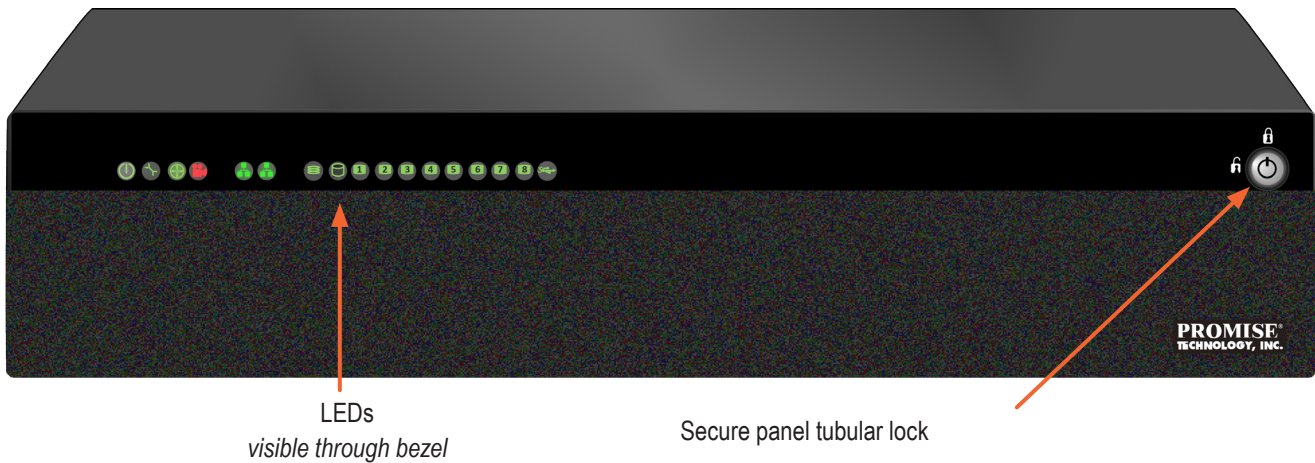
Front with bezel removed

Power button   LEDs   USB ports
two USB 3.0 ports

Drive carriers
eight drive 3.5" carriers
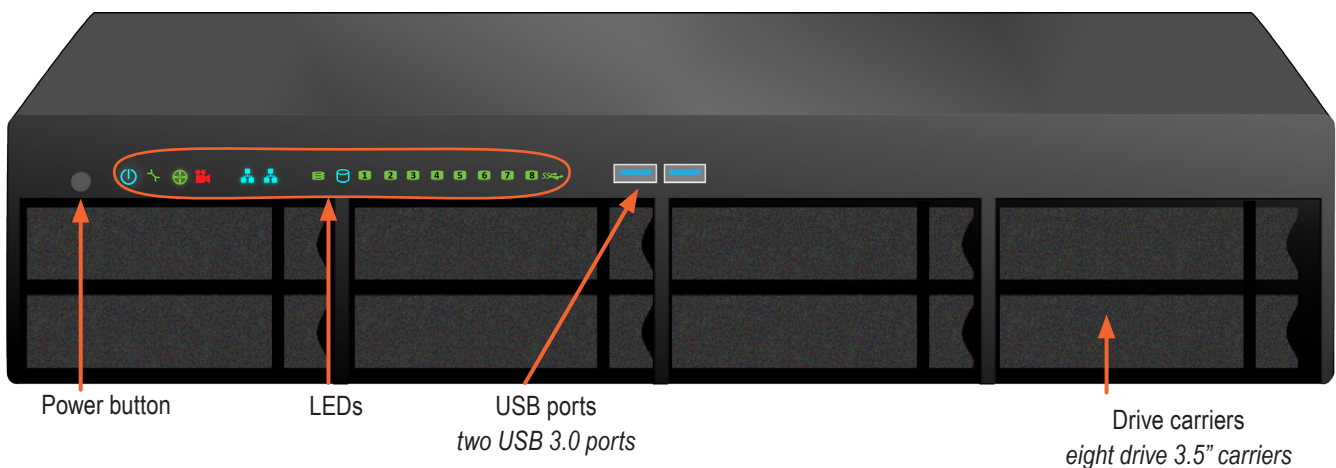
Vess A3340 front panel LED

LED indicators on front of Vess A3340
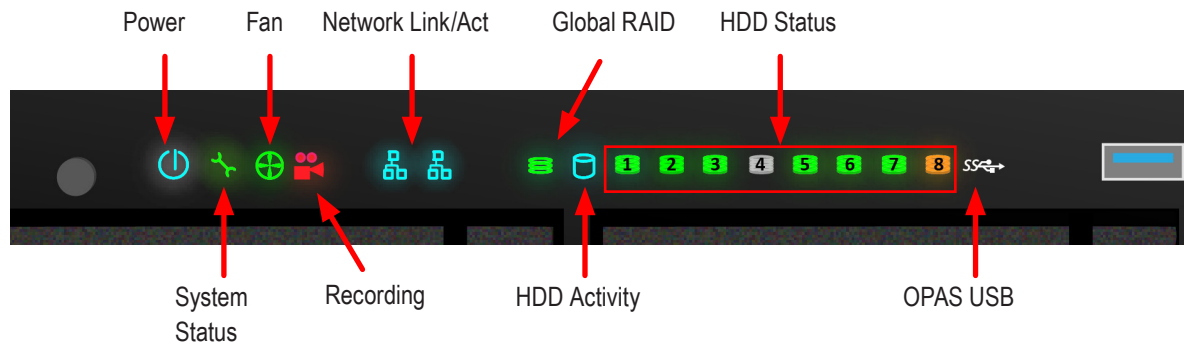
Front panel LED behavior for Vess A3340 system:

LED	Description
Power	Lights BLUE to indicate the system is powered on.
System Status	Lights GREEN when healthy, RED if there is a critical problem (LD offline, fan malfunction, PSU malfunction, voltage out of range, system temperature alert), remains dark when not ready.
Fan Status	Lights GREEN when healthy, RED indicates a fan in the System module is not operating in normal range, ORANGE indicates the CPU fan module is not present.
Recording	RED indicates application running.
Network Link/Activity	One LED for each 1000BASE-T LAN port. Lights BLUE to indicate a valid link, blinks BLUE to indicate activity on the port.
Global RAID Status	Lights GREEN when healthy or RED if any RAID volume is offline, ORANGE for critical state of any logical drive.
Global HDD Activity	Blinks BLUE to indicate one or more drives are being accessed, remains dark when no drives are being accessed.
HDD Status	Lights GREEN when healthy, RED if the RAID member is offline or there is a physical disk error, ORANGE indicates the drive is rebuilding, and a dark LED indicates either no drive is installed or the drive is not configured.
OPAS USB	Lights GREEN if an OPAS device (USB disk) is detected, RED if the OPAS operation has failed, blinks GREEN when an OPAS operation is in progress.

Rear Panel Hardware

The rear panel of the Vess A-Series enclosure provides access to the power supply, local management connection (via USB keyboard and VGA or HDMI monitor port), iSCSI (Ethernet) data ports, and system fan.

Vess A3340s rear panel view

Power insert   System fan   Ports and LEDs   Two PCIe slots
                                               See details on next page
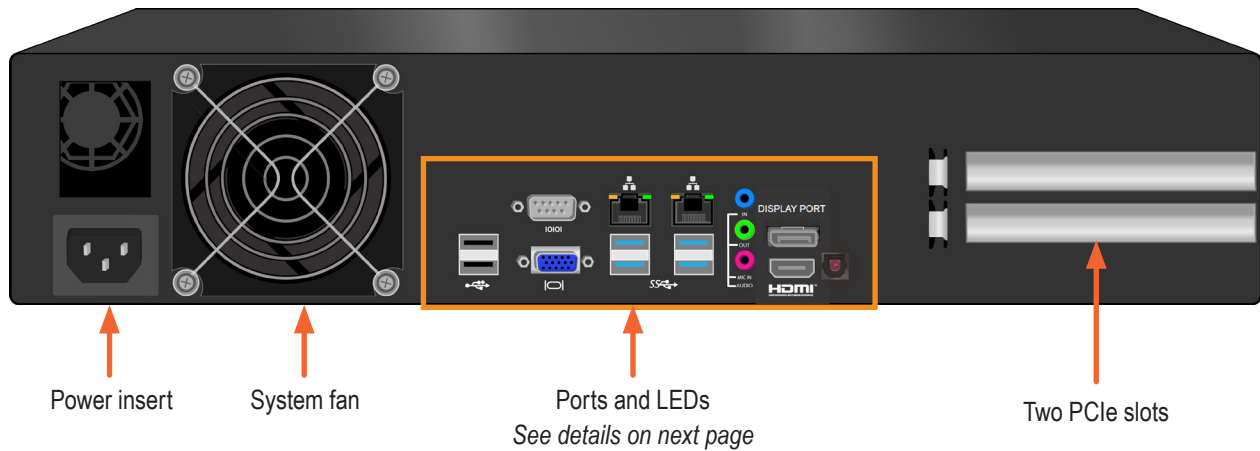
Vess A3340d rear panel view

Power inserts   System fan   Ports and LEDs   Two PCIe slots
Two hot-swappable PSU   *See details on next page*
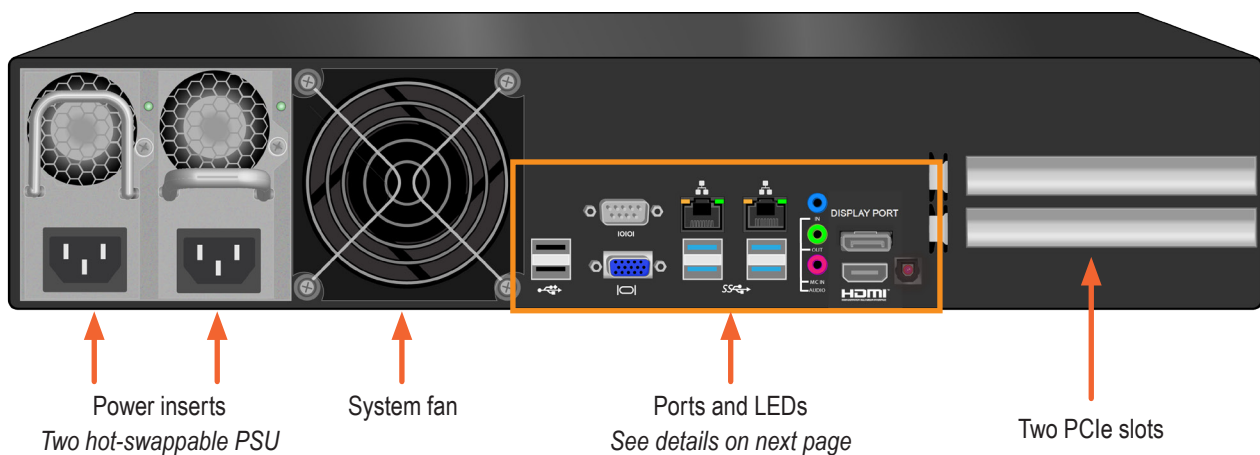
Vess A3340 PoE rear panel view

Power over Ethernet ports

Power inserts
Two hot-swappable PSU

System fan

Ports and LEDs
See details on next page
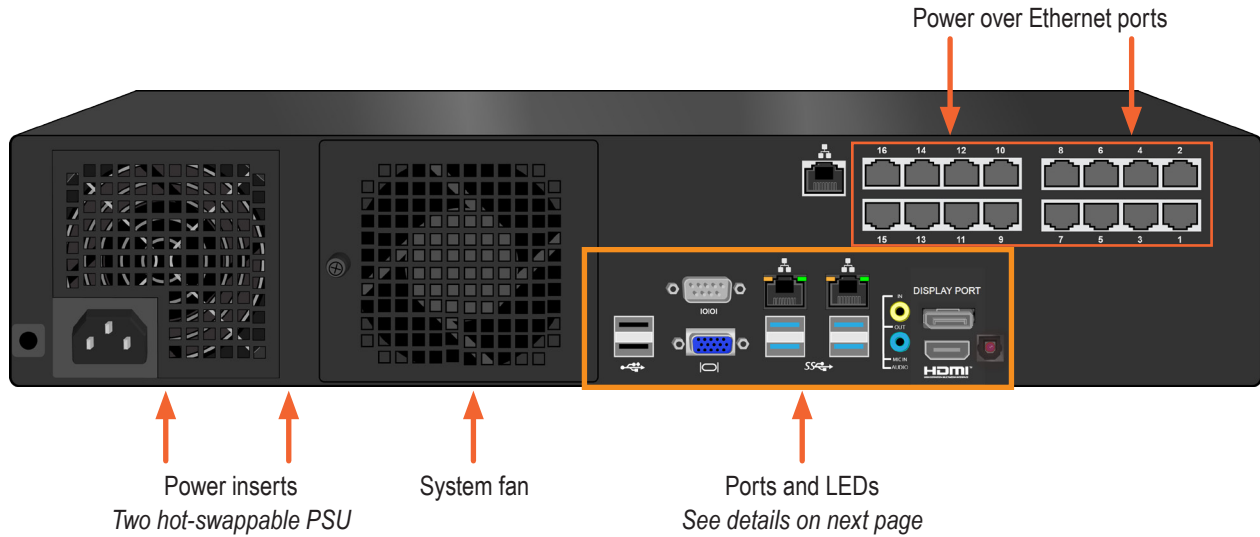
Rear panel LED indicators

The LEDs on the rear panel include LEDs for Ethernet data ports.

LED	Description
Ethernet* *Link/Act and Speed*	The LED located above each port, the LED on the right lights GREEN when the port is connected, flashes GREEN when there is activity on the port and remains dark no connection has been established. The LED on the left indicates connection speed, GREEN is 100 Mbps, ORANGE is 1000 Mbps.

* This LED description does not apply to Power over Ethernet ports.

Rear panel ports

Vess A3340 ports on rear panel
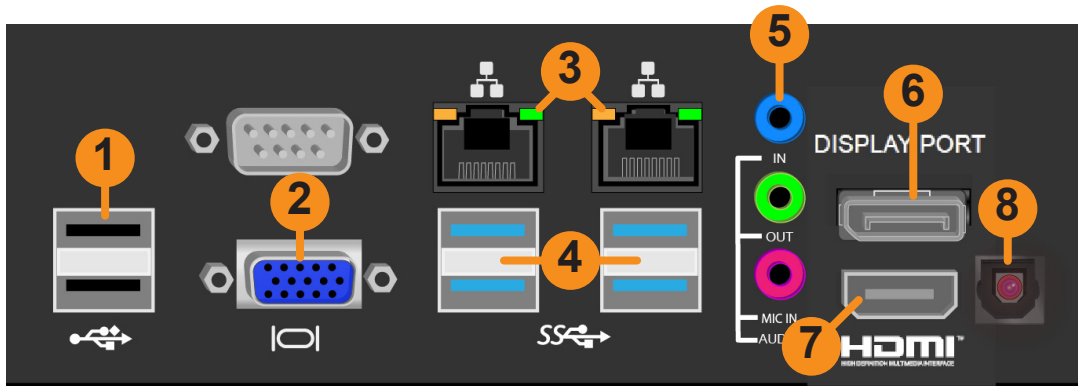
No.	Type
1	USB 2.0 ports
2	VGA port
3	Gigabit Ethernet ports
4	USB 3.0 ports
5	Audio In/Out
6	Display Port
7	HDMI port
8	S/PDIF out

Vess A3340 rear panel connections

Access to physical data and management connections are located on the rear panel of the Vess A3340.

Feature	Description
HDMI	Provides video out connection for HDMI enabled monitors used to view the management interface using CLI, CLU or WebPAM PROe.
VGA	This is also used for a video out connection for VGA monitors, it is also used to view the management interface using CLI, CLU or WebPAM PROe.
USB	The rear panel features two USB 2.0 and two USB 3.0 ports. Use to connect to a USB key-board for managing the Vess A-Series, or use it to transfer data to or from a USB memory device.
RS-232	Serial port can be used for two different functions: 1. Use for the controlling line connection to an uninterruptible power supply (UPS). 2. Use to connect to analog cameras using the analog camera input cable.
Audio In	Use for input from a peripheral audio device, such as a microphone. Plug-In Power micro-phones are supported.
Audio Out	Use for output (line out) peripheral audio device (speakers, for example).

HARDWARE SETUP

This chapter presents the basics on unpacking, setting up hardware for the Vess A3340. Hardware installation includes installing the unit in an equipment rack, connecting the power, making network, data and management connection to the device, and installing hard drives.

The sections in Hardware Setup include the following:

- "Unpacking"

- "Mounting Vess A3340 in a rack"

- "Installing Disk Drives"

    - "Number of Drives Required"

    - "Remove Security Cover"

    - "Drive Slot Numbering"

    - "Drive carriers"

- "Management Path Connections"

- "Connect the Power"

- "Power On Enclosure""

- "Connect to iSCSI Storage Area Network (SAN)"

Unpacking

> **Note**
>
> The Vess A-Series can accommodate SATA (3Gbps/6Gbps) hard drives.

Packing List

The Vess A3340 box contains the following items:

- One Vess A3340s, Vess A3340d or Vess 3340 PoE

- One 1.5m (4.9 ft) Power cord (*Vess A3340s and Vess A3340 PoE*)

- Two 1.5m (4.9 ft) Power cords (*Vess A3340d*)

- Screws for disk drives (40 pieces for 8 bays)

- Sliding rail assembly for rack mounting*

 * These items might be an optional feature in your region. Please contact your sales representative to learn whether this is included or an option for your Vess A-Series enclosure.

Mounting Vess A3340 in a rack

The instructions here apply to the Vess A3340 2U form factor model.

Cautions

- **Do not lift or move the Vess A3340 unit by the handles on the ear brackets in front. Hold the system itself.**

- **Do not install the Vess A3340 unit into a rack without rails to support the system.**

- **Only a qualified technician who is familiar with the installation procedure should mount and install the Vess A3340 unit.**

- **Mount the rails to the rack using the appropriate screws and flange nuts, fully tightened, at each end of the rail.**

- **Do not load the rails unless they are installed with screws as instructed.**

- **The rails available for the Vess A3340 unit are designed to safely support that Vess A3340 unit when properly installed. Additional loading on the rails is at the customer's risk.**

- **The mounting rails will support your Vess A3340 unit only if installed as instructed.**

- **Do not install hard disk drives in the system until after placing the system in the rack.**

The Vess A3340 installs in a 19" equipment rack. Please examine the illustrations in this section to make sure you are using the correct type of rack.

In order to place the system in the rack, first attach the ear brackets to the front of the device. Then install the sliding rail system in the rack. Finally place the device on the sliding rails and secure it to the rack. Use only the screws and fasteners included with the shipment of the sliding rail system, or with the Vess A3340. This procedure is described and illustrated in the sections that follow below.

Attach ear brackets to front

Ear brackets for rack installation are available as an additional purchase. These brackets attach at the front sides of the device housing. Once the brackets are securely attached and the unit has been properly installed in the sliding rail system, these handles can be used to pull or push the device out or into the rack system, while the sliding rails support the weight of the device.

DO NOT lift or attempt to support the weight of the Vess A3340 using the handles on the ear brackets.

Ear brackets (optional)

left side ear bracket
and handle

right side ear bracket
and handle

Attach each ear bracket at the front, on each side of the device housing, and secure with the screws included with the shipment. The handle should protrude in the direction of the front of the device.
The example illustration below shows the right side.

Secure ear bracket to device housing - right side

Cautions

Do not lift or move the Vess A3340 unit by the handles on the ear brackets in front.

Install the sliding rails and place device in rack

Follow these steps to install the sliding rails in the rack system, then place the Vess A3340 onto the rails and secure the device to the rack.

1. Determine what height to place the 2U enclosure in the rack, then place the right and left rack rails at the same height on in the right and left rack position. Choose the mounting holes accordingly for your rack system. Note that three holes are required on each front post, the uppermost of the three to be used for the flange nuts to anchor the enclosure to the rack posts. Adjust the length of the mounting rails as needed.

2. Secure the rails to the rack posts. Make sure the rack rails are properly oriented in the rack.

3. To set the rails into the rack posts and secure the rails, follow these steps:

Determine which holes to use on rack

Notice that each end of the sliding rails have a lever to operate the lock mechanism that grips the rack post.

Lock release lever (back left)

a.   Press the spring lock then insert the studs into the selected square holes on the rack post.

b.   Press the spring lock on the other end of the rail and insert the studs into the selected
Press lever to release lock (front right)
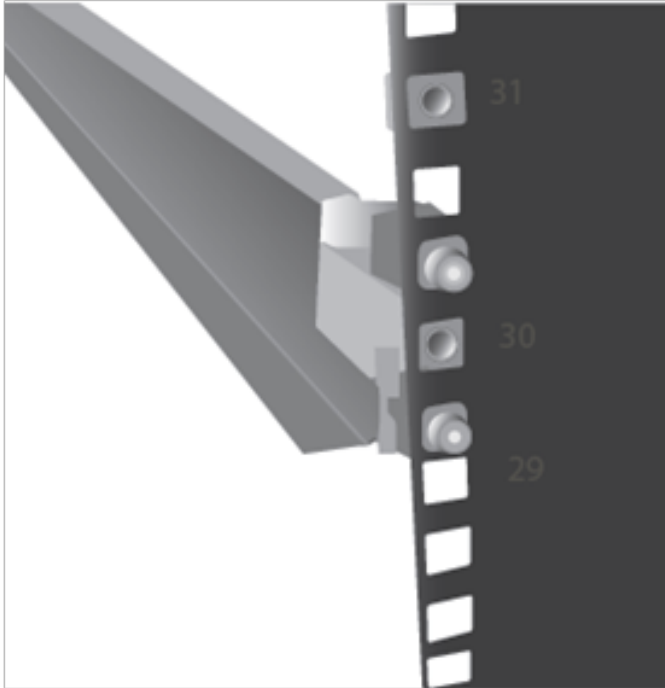
mounting hole on the rack post. If necessary, extend the rail to reach the post.

c.   Use the rail screws and washers to anchor the rack rail to the post.

d.   Make sure the rack rail is aligned, secure, stable and in the correct place.

e.   Perform steps a through c above for the other rail.

f.   Make sure the rack rails are aligned, secure, stable and in place.
See figure on next page.

4.   Use the attaching screws that came with the mounting hardware to secure the enclosure to the rack.

Back left rail secured to post
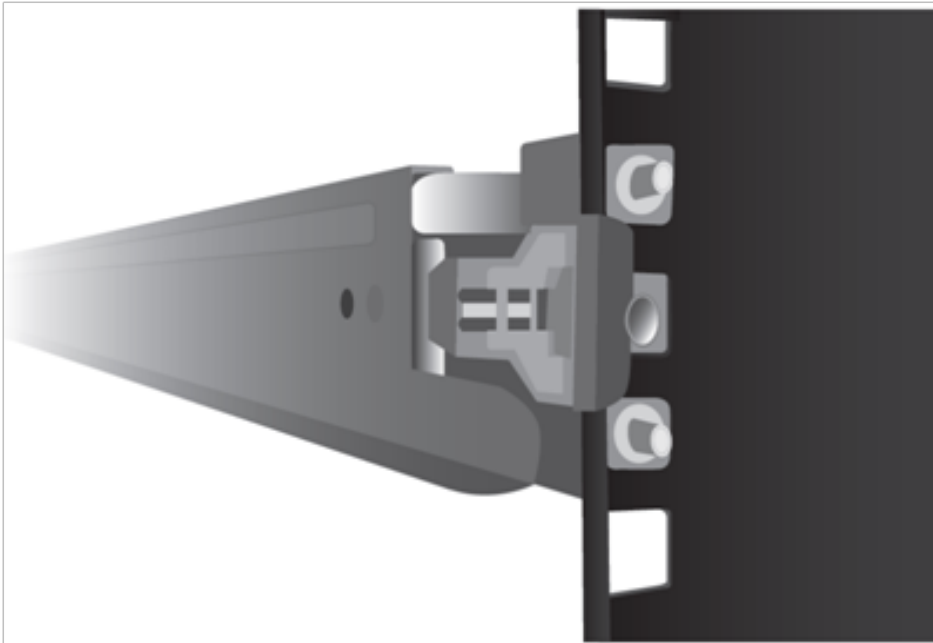
Front view of Vess A3340 secured to rack and placed on rail system

Installing Disk Drives

The Vess A-Series subsystems support:

- SATA hard disks

- 3.5-inch hard disk drives

For a list of supported physical drives, download the latest compatibility list from the PROMISE support website.

Number of Drives Required

The table below shows the number of drives required for each RAID level

Level	Number of Drives		Level	Number of Drives
RAID 0	1 or more		RAID 6	4 to 32
RAID 1	2 only		RAID 10	4 or more*
RAID 1E	2 or more		RAID 30	6 or more
RAID 3	3 to 32		RAID 50	6 or more
RAID 5	3 to 32		RAID 60	8 or more

*Must be an even number of drives.

⚠ **Caution**

The Vess supports disk drive hot-swapping. To avoid hand contact with an electrical hazard, do not remove more than one drive carrier a time.

Remove Security Cover

To remove the security cover:

1.   Use the tubular key to unlock the cover. Turn counterclockwise to unlock.
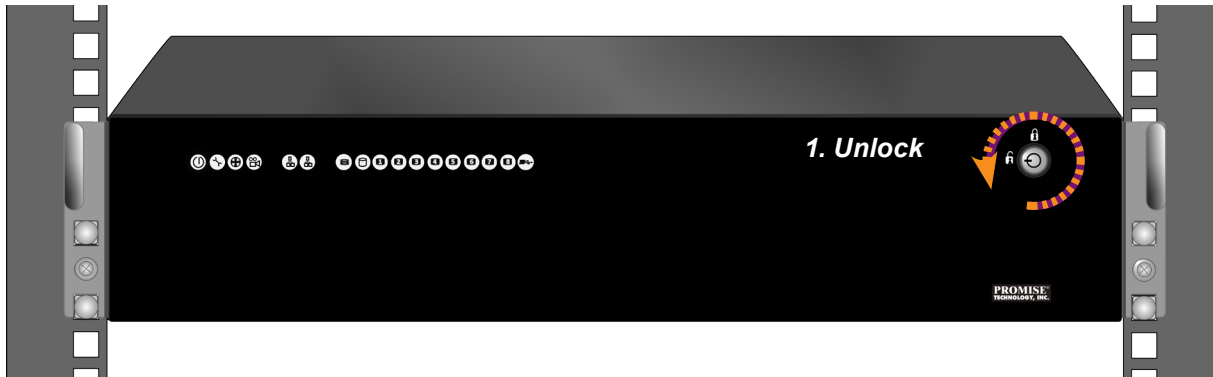
2.   Slide the cover to the right about 4 mm.
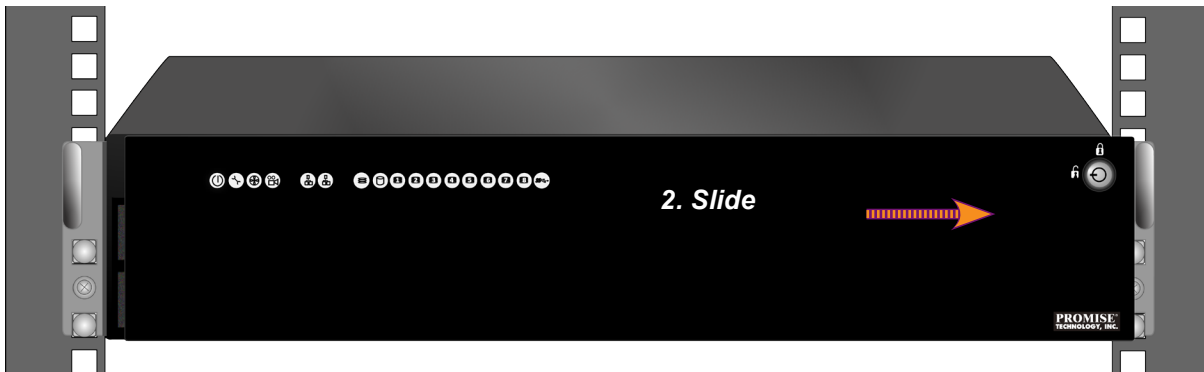
3.   Pull the cover straight back to remove. Be careful not to drop the cover.

Drive Slot Numbering

You can install any suitable disk drive into any slot in the enclosure. The diagram below shows how drive slots are numbered on both the Vess A3340.

Slot numbering is reflected in the web manager GUI and CLI/CLU user interfaces.

Install all of the drive carriers into the enclosure to ensure proper airflow, even if you do not populate all the carriers with disk drives.

Drive slot numbering for Vess A3340
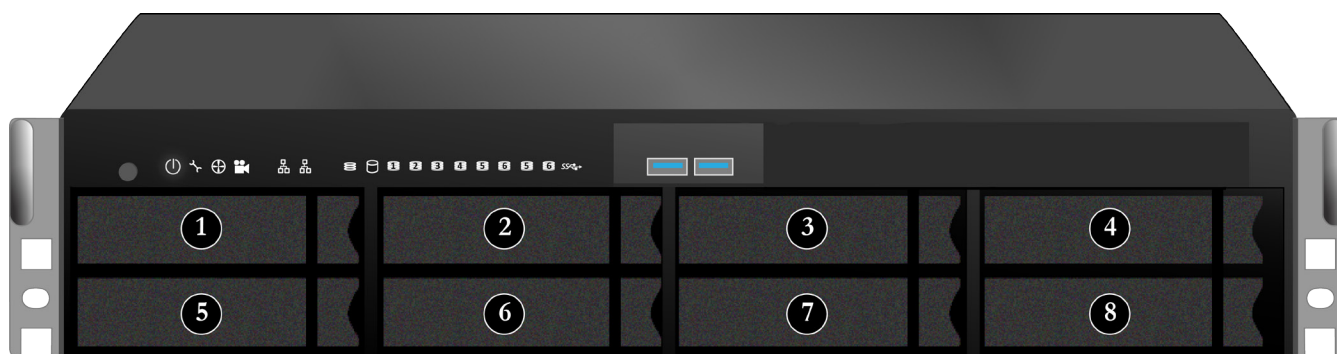
Drive carriers

The instructions below apply to all types of drive carriers intended for use with the Vess A-Series.

1. Remove a disk drive carrier.

2. Carefully lay the disk drive into the drive carrier at the front, so that the screw holes on the sides line up.

3. Insert the screws through the holes in the drive carrier and into the sides of the disk drive.
   See illustration below.

Install only the counter-sink screws supplied with the drive.

• Install four screws per drive.

• Snug each screw. Be careful not to over-tighten.

4. Reinstall the drive carrier into the enclosure.

5. Repeat steps 1 through 3 until all of your disk drives are installed.

Pull handle to release the latch, then pull straight out gripping the handle.
Place your free hand underneath when removing or inserting the carrier containing a hard disk drive, so you do not drop it.
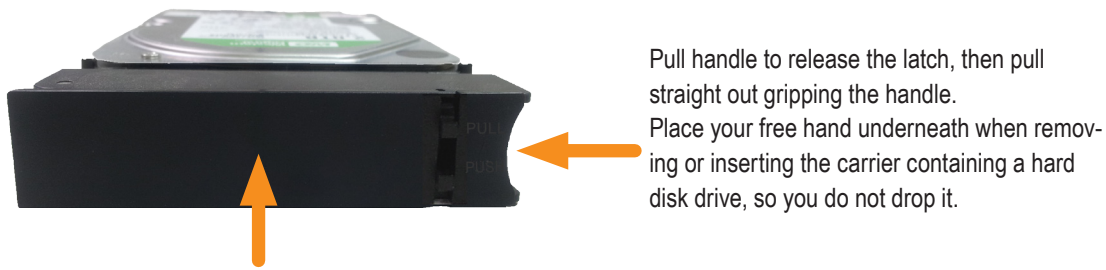
Push in the center to insert the drive carrier into an empty drive bay.

Counter sink screws; two screws on each side.

Vess A3340 disk carrier with HDD installed - front view

Push here when returning or replacing the carrier into an empty drive bay.

Pull here to release the carrier handle latch. Then pull the carrier straight out by the handle. Place your free hand under the carrier. Do not drop the disk carrier, even if it is empty.

Tabs for locking mechanism insert. This piece must be removed to unlatch the carrier. To remove, squeeze the tabs together and pull out. To reinsert, squeeze the tabs together and replace in position. Do not discard the locking mechanisms.

Caution

The Vess A-Series supports disk drive hot-swapping. To avoid hand contact with an electrical hazard, do not remove more than one drive carrier a time.

Management Path Connections

This section describes how to establish a management connection the Vess A3340 subsystem. There are two methods to establish the physical connection used for management of the device. Management through the Gigabit network connection is done using WebPAM PROe, a web browser based GUI. Alternatively you can use an out-of-band connection using a VGA or HDMI monitor and USB keyboard to access the embedded text-based CLI/CLU interface.

Management Path - network connection

Vess A3340 have two Gigabit Ethernet RJ-45 ports on the rear panel for connection to an Ethernet network. Use this connection with WebPAM PROe to login as the device administrator.

To establish the management path:

1. Attach one end of an Ethernet cable to the network connector or standard NIC in the Host PC.

   Attach the other end of the Ethernet cable to one of the ports on the standard network switch.

2. Attach one end of an Ethernet cable to one of the ports on the standard network switch.

   Attach the other end of the Ethernet cable to the Management Port on the Vess system.

   If you have multiple Vess systems, Host PCs or Servers, repeat steps 1 and 2 as required.

3. Follow the instructions for managing the basic settings of the Vess A3340.

Management Path - on site keyboard and monitor

Use a USB keyboard and a VGA or HDMI monitor to establish a local out-of-band connection to the Windows operating system. The VGA port, HDMI and USB ports are also located on the rear panel of the Vess, these are enabled by default upon booting up the system. Connect a VGA or HDMI monitor to the appropriate port on the Vess, and connect a USB keyboard to either USB port on the rear panel.

Vess A3340 rear panel video monitor connections and USB ports

VGA port
Connect to VGA monitor

USB ports
two USB 2.0 and four 3.0 ports; connect to keyboard

Display Port
Connect to Display Port monitor

HDMI port
Connect to HDMI monitor
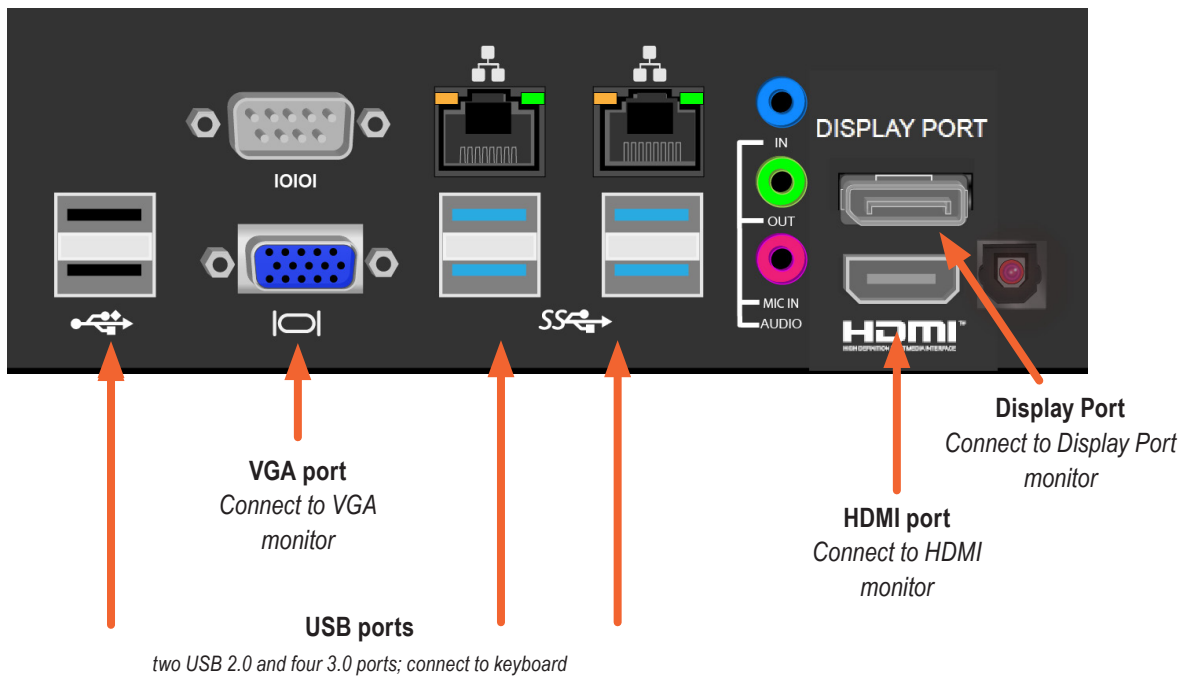
Important

Be sure to place the monitor and keyboard on a stable and secure surface before connecting them.

Connect the Power

Insert a power cable into the power receptacle on each power supply. The Vess A3340d is equipped with two power supplies, the Vess A3340s and Vess A3340PoE have a single power supply.

See diagrams below for locations.

1	Power recep-tacle
2	System fan

Vess A3340d power supply and system fan
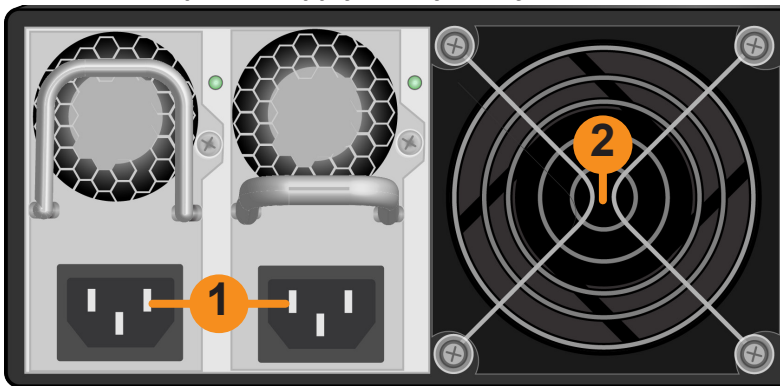
Vess A3340s power supply and system fan
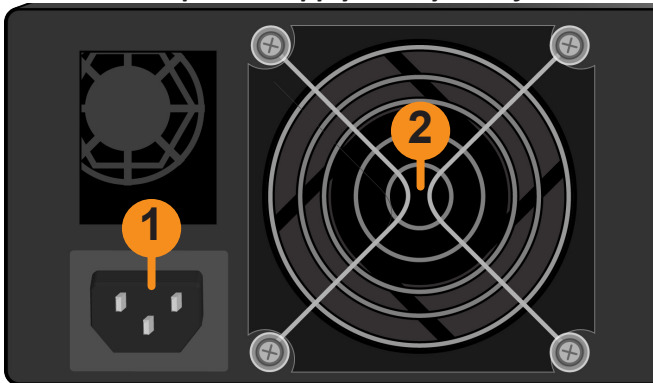
Vess A3340 PoE power supply and system fan
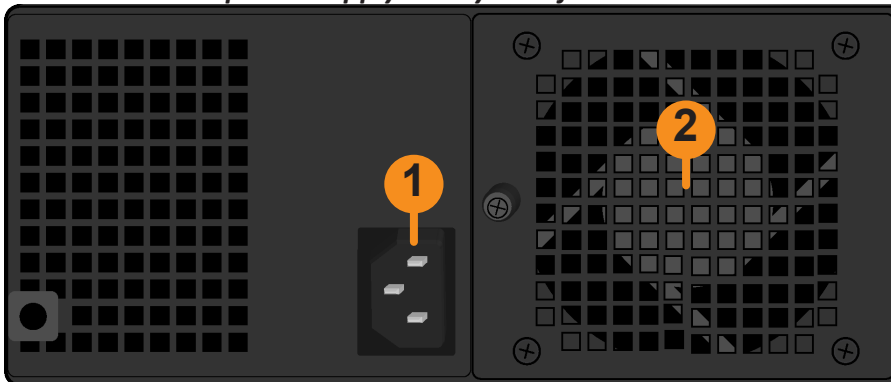
Power On Enclosure

With the power supplies connected, the system can now be powered on.

To power on the Vess A3340, press the Power button in the lower left corner of the front panel (see figure below). Observe the LEDs on the front panel to make certain the boot up proceeds smoothly.

Front panel of Vess A3340

Power button

Front Panel LEDs

When boot-up is finished, check the LEDs on the front panel to make sure the system is functioning properly.

LED	Description
Power	Lights BLUE to indicate the system is powered on.
System Status	Lights GREEN when healthy, RED if there is a critical problem (LD offline, fan malfunction, PSU malfunction, voltage out of range, system temperature alert), remains dark when not ready.
Fan Status	Lights GREEN when healthy, RED indicates a fan in the System module is not operating in normal range, ORANGE indicates the CPU fan module is not present.
Recording	RED indicates application running.
Network Link/Activity	One LED for each 1000BASE-T LAN port. Lights BLUE to indicate a valid link, blinks BLUE to indicate activity on the port.
Global RAID Status	Lights GREEN when healthy or RED if any RAID volume is offline, ORANGE for critical state of any logical drive.
Global HDD Activity	Blinks BLUE to indicate one or more drives are being accessed, remains dark when no drives are being accessed.
HDD Status	Lights GREEN when healthy, RED if the RAID member is offline or there is a physical disk error, ORANGE indicates the drive is rebuilding, and a dark LED indicates either no drive is installed or the drive is not configured.
OPAS USB	Lights GREEN if an OPAS device (USB disk) is detected, RED if the OPAS operation has failed, blinks GREEN when an OPAS operation is in progress.

LED indicators on front panel
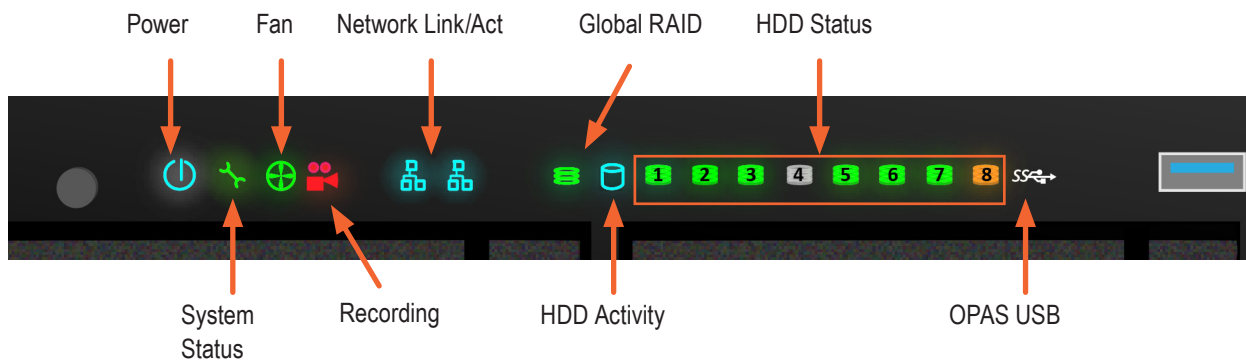
Gigabit Port LEDs

Check the network connection on the rear panel to make sure the system is accessible for configuration. The Gigabit Ethernet ports have Link/Act and Speed LEDs located above each of the two ports.

The LED on the right side above each port lights when connected, flashes when there is activity on the port and remains dark no connection has been established.

Connect to iSCSI Storage Area Network (SAN)

Important

For a list of supported Gigabit Ethernet NICs, HBA NICs and switches, download the latest compatibility list from PROMISE support: http://www.promise.com/support/.

This arrangement requires:

• A GbE network interface card (NIC) or iSCSI HBA NIC in the host PC or server

• A GbE network switch

• A standard network switch

Gigabit ports on the rear panel
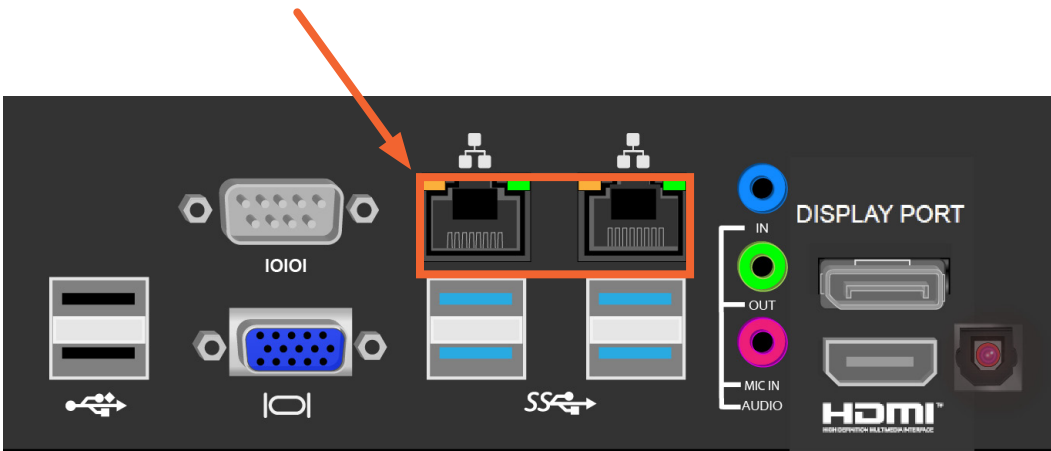
Note

To expand physical capacity available for the Vess A3340, use the onboard iSCSI ports to connect to Vess R2000 Series storage enclosures; and each Vess R2000 can also be connected to Vess J2000 Series JBOD expansion units.

PoE Network Connections (Vess A3340 PoE)

The sixteen PoE ports and the PoE uplink are used for connection to the IP camera network. Use the PoE ports for direct connection for up to sixteen IP camera. The uplink port must connect to a PoE enabled switch.

Vess A3340 PoE IP Camera Network

MANAGING WITH CLU

CLU and CLI management both use a text-based terminal user interface.

In order to access the terminal program interface used for CLI and CLU management on the Vess A-Series subsystem, insert a USB keyboard into any USB port, and connect a monitor using either the VGA or HDMI port.

Vess A3340 rear panel video monitor connections and USB ports

VGA port
Connect to VGA monitor

USB ports
two USB 2.0 and four 3.0 ports; connect to keyboard

HDMI port
Connect to HDMI monitor

Display Port
Connect to Display Port monitor
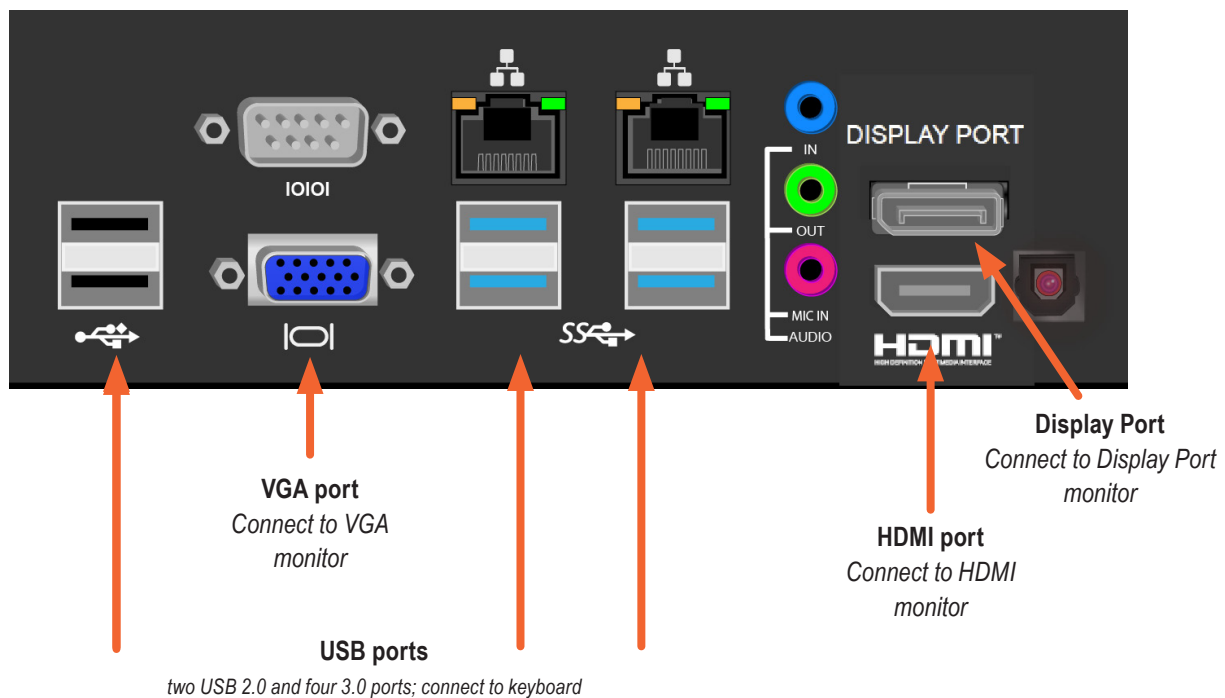
Access CLI in Windows

For Windows installations, once the system has booted up it will be necessary to choose various options to complete the OS setup. You will be prompted to select a default language and other user interface preferences. Follow the instructions on screen to complete your preferences selection and to establish a user name and password for the administrator. After completing these final tasks, the Windows desktop appears.

Important

DO NOT move any files from or copy any files to the PromiseApp folder on the C Drive [C:\PromiseApp] in the Windows OS.

To use the CLU interface, first open the CLI terminal interface:

1. Go to **Start > Run** and click the **Browse** button.

2. Navigate to the **C:\PromiseApp\clitest f**older**.**

3. Click **clitest.exe** file then click the Open button.

4. Click the **OK** button in the **Run** dialog box.

The CLI window opens. See "Using the CLU" below for instructions for instructions on how to access the CLU interface.

Using the CLU

In the CLI terminal interface, login first, then access the CLU interface. Follow the instructions below.

1. At the CLI Login prompt, type the user name and press **Enter**.

    The default user name is ***administrator***.

2. At the Password prompt, type the password and press **Enter**.

    The default password is ***password***.

    The CLI screen appears.

3. At the ***administrator@cli>*** prompt, type `menu` and press **Enter**.

    The CLU **Main Menu** appears.

4. Use the arrow keys or tab key on your keyboard to scroll the highlighted text to a command, then select or activate that command by pressing **Enter**.

CLU Main Menu
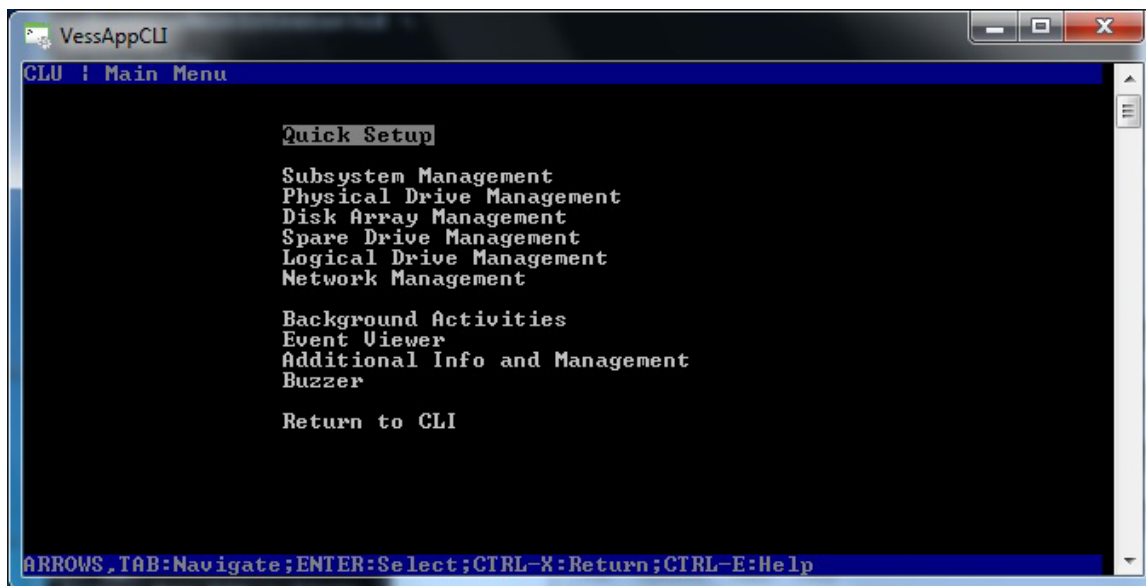
Notice at the bottom of the CLU interface there are on-screen reminders of keyboard actions used for CLU interface. The keyboard inputs to use the CLU are as follows:

- *Arrow Keys* - Use the up and down arrow keys to move the text selector, indicated by the highlighted line of text.

- *Tab Key* - Use the tab key to scroll down the list of text options.

- *Enter Key* - Press the Enter key to select or activate the highlighted text action, command or option.

- *CTRL + X* - Press the Control key and "X" key to return to the previous menu.

- *CTRL + E* - Press the Control key and "E" key to bring up the Help menu

CLU notation used in this guide

The CLU command descriptions in this chapter use abbreviated descriptions of CLU navigation. It is assumed the user will understand that movement from one CLU menu item to another involves using the arrow keys to highlight the given command then pressing enter to view another list of CLU command selections or parameter options. For example, listed below are the steps used to create a new user account. Notice that Step 1 lists the path of CLU menu items to get to the Create New User menu, while Step 2 presents the various parameters to configure for the newly created user. It is implied in Step 1 that the user knows to highlight the menu item and then press the Enter key to move to the next menu item listed. This format is used throughout this chapter.

Example notation from Create New User menu item:

To create a new user account:

1. **Main Menu** >>*Additional Info and Management >> User Management >> Create New User*

2. Highlight each field and type in the appropriate information:

    - *User name* (Maximum 31 characters. Use letters, numbers, and underscore. No spaces.)

    - *Password* (Optional. Maximum 31 characters. Use letters, numbers, and underscore.)

    - *Display name* (Optional)

    - *User's email address*

3. Highlight *Privilege* and press the space bar to toggle though the options.

4. Press **Control-A** to save the user.

Step 1 tells the user to start in the Main Menu, then highlight "Additional Info and Management" and press Enter; this brings up a new list of CLU menu items from which to choose "User Management" and then press Enter again bringing up another list of CLU menu items, and so on.

Use the table below for reference of the CLU interface.

Quick Setup	*A sequence of steps to setup the RAID configuration.*	
Subsystem Management page 36	Alias	
	Media Patrol	*Start, Stop or Pause Media Patrol*
	Lock Management	*Prevent settings changes to controller for set time*
	Controller Management	*Alias, Coercion, Write Back Cache, Forced Read Ahead Cache*
	Enclosure Management	*Enclosure Status Information, Temperature & Voltage Sensor Thresholds,*
Physical Drive Management page 47	Physical Drive Summary	
	Global Physical Drive Settings	*WriteCached, ReadLookAhead, DMAMode, MediumErrorThreshold*
Disk Array Management page 52	Create New Array Delete Array	
Spare Drive Management page 64	Create New Spare Drive	
Logical Drive Management page 68	Logical Drive Summary	
Network Management page 86	Network Port Summary	
Background Activities page 75	Background Activity Settings	*Media Patrol, AutoRebuild, Rebuild Rate, Migration Rate, PDM Rate, Transition Rate, Sync Rate, Initialization Rate, RC Rate, ReAssigned Block Threshold, Error Block Threshold*
Event Viewer page 77	Runtime Events NVRAM Events	*Clear Event Statistics*
Additional Info and Management page 85	Software Management	*Email, Webserver, SNMP*
	Configuration of Logs Clear Statistics Restore Factory Defaults	
Buzzer page 91	*Enable/Disable alarm buzzer*	

Accessing Online Help

To access online help on any CLU screen, press **Control-E**.

To return to the CLU, press **Enter**.

Exiting the CLU

1. Highlight *Return to Previous Menu* and press **Enter**.

    Repeat this action until you arrive at the **Main Menu**.

2. **Main Menu**, highlight *Return to CLI* and press **Enter** to exit

3. Close the terminal emulation, Telnet, SSH, or terminal window.

Logging Out of the CLI

When you shut down or restart the Vess A-Series subsystem, you are automatically logged out of the CLI.

To manually log out of the CLI (no shut down or restart):

At the *username@cli>* prompt, type logout and press **Enter**.

The prompt changes to *cli>*.

Logging Back Into the CLI and CLU

To log into the CLI and CLU after a manual logout:

1. At the *cli:>* prompt, type login followed by your user name and press **Enter**.

2. At the Password: prompt, type your password and press **Enter**.

3. At the *username@cli>* prompt, type `menu` and press **Enter** to open the CLU.

Managing the Subsystem (CLU)

Subsystem Management includes the following functions:

- "Making Subsystem Settings (CLU)" on page 36

- "Locking or Unlocking the Subsystem (CLU)" on page 37

Making Subsystem Settings (CLU)

An alias is optional. To set an Alias for this subsystem:

1. **Main Menu** >> **Subsystem Management** >> **Subsystem Settings**.

2. Make changes as required:

   - Type and alias into the Alias field.

     Maximum of 48 characters. Use letters, numbers, space between words   and underscore

3. Press **Control-A** to save your settings.

Running Media Patrol (CLU)

Media Patrol is a routine maintenance procedure that checks the magnetic media on each disk drive. Media Patrol checks all physical drives assigned to disk arrays and spare drives. It does not check unconfigured drives.

To start, stop, pause or resume Media Patrol - **Main Menu** >> *Subsystem Management >> Media Patrol* >> [*Start, Stop, Pause,* or *Resume*]. If you choose *Stop*, press **Y** to confirm.

Locking or Unlocking the Subsystem (CLU)

The lock prevents other sessions (including sessions with the same user) from making a configuration change to the controller until the lock expires or a forced unlock is done. When the user who locked the controller logs out, the lock is automatically released.

Setting the Lock

To set the lock:

1. **Main Menu** >> **Subsystem Management** >> *Lock Management*

2. In the **Lock Time** field, type a lock time in minutes.

    1440 minutes = 24 hours

3. Highlight *Lock* and press **Enter**.

Resetting the Lock

To reset the lock with a new time:

1. **Main Menu** >> *Subsystem Management* >> *Lock Management*

2. In the **Lock Time** field, type a lock time in minutes.

    1 to 1440 minutes (24 hours)

3. Highlight *Renew* and press **Enter**.

Releasing the Lock

Main Menu >> *Subsystem Management* >> *Lock Management* >> *Unlock*

Releasing a Lock set by another user

To release somebody else's lock:

1. **Main Menu** >> *Subsystem Management* >> *Lock Management* >> *Force Unlock*

2. Press the **Spacebar** to toggle to *Yes* >> **Unlock**

View Subsystem Date and Time (CLU)

This is a display only screen to view current Date and Time:

Main Menu >> *Subsystem Management* >> *System Date & Time*

Managing the RAID Controllers (CLU)

RAID controller management includes the following functions:

- "Viewing Controller Information (CLU)" on page 39

- "Making Controller Settings (CLU)" on page 40

Viewing Controller Information (CLU)

Controller Management includes information, settings and statistics.

To access Controller Management:

1. **Main Menu** >> **Subsystem Management** >> **Controller Management**

   The Controller summary information includes:

   - **Alias** – if assigned

   - **Operational Status** – OK means normal. Might show BGA running.
     Not present indicates a malfunction or no controller is installed

   - **Readiness Status** – Active or Standby is normal. N/A means not accessible

2. Highlight the controller you want and press **Enter**.

To access additional controller information, highlight **Advanced Information** and press **Enter**.

To access controller statistics, highlight **Controller Statistics** and press **Enter**.

Clearing Statistics

To clear controller statistics, see "Clearing Statistics (CLU)" on page 89.

Making Controller Settings (CLU)

If your subsystem has two controllers, any settings you make to one controller automatically apply to the other controller.

To make Controller settings:

1. **Main Menu** >> *Subsystem Management* >> *Controller Management*

2. Highlight the controller you want and press **Enter**.

3. Highlight *Controller Settings* and press **Enter**.

4. Make the following settings as required:

   - Type an alias into the **Alias** field.

     Maximum of 48 characters. Use letters, numbers, space between words   and underscore. An alias is optional.

   - Highlight *Coercion* and press the spacebar to toggle between *Enabled* and *Disabled*.

     For more information, see "Capacity Coercion".

   - Highlight *Coercion Method* and press the spacebar to toggle through:

     GB Truncate – Reduces the capacity to the nearest 1 GB boundary.

     10 GB Truncate – Reduces the capacity to the nearest 10 GB boundary.

     Grp (group) Rounding – Uses an algorithm to determine truncation. Results in the maximum amount of usable drive capacity.

     Table Rounding – Applies a predefined table to determine truncation.

- Highlight *SMART* and press the spacebar to toggle between **Enable** and **Disable**.

- Highlight *SMART Poll Interval* and press the backspace key to erase the current value. Type a new interval value (1 to 1440 minutes).

- Highlight Poll Interval and press the backspace key to erase the current value. Type a new interval value (15 to 255 seconds).

- Highlight Adaptive Writeback Cache and press the spacebar to toggle between Enabled and Disabled.

- Highlight *Forced Read Ahead Cache* and press the spacebar to toggle between **Enabled** and *Disabled*.

- Highlight *HDD Power Saving* and the spacebar to choose a time period. After an HDD has been idle for a set period of time:

  Power Saving Idle Time – Parks the read/write heads

  Power Saving Standby Time – Lowers disk rotation speed

  Power Saving Stopped Time – Spins down the disk (stops rotation)

  You must also enable Power Management on the disk array. See "Creating a Disk Array – Advanced (CLU)" on page 55 and "Enabling Media Patrol, PDM, and Power Management on a Disk Array (CLU)" on page 60.

1. Press **Control-A** to save your settings.

Notes

Power Management must be enabled on the disk array for the HDD Power Saving settings to be effective. See "Making Disk Array Settings (CLU)" on page 59.

Power management is limited to the features your HDDs actually support.

Managing the Enclosure (CLU)

Enclosure Management includes the following functions:

- "Viewing the Enclosures Summary (CLU)" on page 42

- "Viewing Enclosure Information (CLU)" on page 43

- "Making Enclosure Settings (CLU)" on page 43

- "Viewing Power Supply Status (CLU)" on page 44

- "Viewing Cooling Unit Status (CLU)" on page 44

- "Viewing Temperature Sensor Status (CLU)" on page 45

- "Viewing Voltage Sensor Status (CLU)" on page 45

- "Locating an Enclosure (CLU)" on page 46

Viewing the Enclosures Summary (CLU)

Enclosure Management includes information, status, settings and location. To access Enclosure Management:

1. **Main Menu** >> **Subsystem Management** >> *Enclosure Management*

    The following information is shown:

    - **Enclosure ID number**

    - **Enclosure Type**

    - **Operational Status**

    - **Status Description** (specific components in need of attention, if any)

Viewing Enclosure Information (CLU)

To view enclosure information:

1. **Main Menu** >> *Subsystem Management* >> *Enclosure Management*

2. Highlight the enclosure you want and press **Enter**.

    You can monitor power supplies, cooling units, enclosure temperatures and voltages.

Adjustable items

You can set or adjust the following items:

*   Enclosure Warning and Critical temperature thresholds
    See "Making Enclosure Settings" below.

Making Enclosure Settings (CLU)

To make Enclosure settings:

1. **Main Menu** >> *Subsystem Management* >> *Enclosure Management*

2. Highlight the enclosure you want and press **Enter**.

3. Highlight *Enclosure Settings* and press **Enter**.

4. Highlight the **Temperature Warning** threshold you want to change.

5. Press the backspace key to erase the current value.

6. Type a new interval value in degrees C.

7. Press **Control-A** to save your settings.

Viewing Power Supply Status (CLU)

To view the status of the power supplies:

1. **Main Menu** >> *Subsystem Management* >> *Enclosure Management*

2. Highlight the enclosure you want and press **Enter**.

3. Highlight *Power Supplies* and press **Enter**.

   The screen displays the operational and fan status of the power supply or supplies. If any status differs from normal or the fan speed is below the Healthy Threshold value, there is a fan/power supply malfunction.

Viewing Cooling Unit Status (CLU)

To display the status of the power supply fans:

Main Menu >>*Subsystem Management* >> *Enclosure Management*

   This is a read-only menu. The screen displays the status and speed of cooling units. If fan speed is below the Healthy Threshold, there is a malfunction.

Viewing Temperature Sensor Status (CLU)

To display the status of the temperature sensors:

Main Menu >> *Subsystem Management* >> *Enclosure Management*

This is a read-only menu. If any temperature exceeds the Healthy Threshold value, there is an overheat condition in the enclosure.

Viewing Voltage Sensor Status (CLU)

To display the status of the voltage sensors:

Main Menu >>**Subsystem Management** >> E**nclosure Management**

This is a read-only menu. If any voltage is outside the Healthy Threshold values, there is a voltage malfunction in the enclosure.

Locating an Enclosure (CLU)

This feature helps you identify the physical Vess A-Series enclosure you are working with through the CLU.

1. **Main Menu** >> *Subsystem Management* >> *Enclosure Management* and press **Enter**.

2. Highlight the enclosure you want and press **Enter**.

3. Highlight *Locate Enclosure* and press **Enter**.

    The LEDs on the front of the Vess A-Series blink for one minute.

Physical Drive Management (CLU)

Physical Drive Management includes the following functions:

- "Viewing a List of Physical Drives (CLU)" on page 47

- "Making Global Physical Drive Settings (CLU)" on page 48

- "Viewing Physical Drive Information (CLU)" on page 49

- "Setting an Alias (CLU)" on page 50

- "Locating a Physical Drive (CLU)" on page 51

Viewing a List of Physical Drives (CLU)

To view a list of physical drives:

Main Menu >> *Physical Drive Management*

The list of physical drives displays.

Making Global Physical Drive Settings (CLU)

All physical drive settings are made globally, except for setting an alias, which applies to individual drives.

To make global physical drive settings:

1. **Main Menu** >> *Physical Drive Management* >> *Global Physical Drives Settings*

2. Change the following settings as required.

   - Highlight *Write Cache* and press the spacebar to toggle between *Enabled* and *Disabled*.

   - Highlight *Read Look Ahead Cache* and press the spacebar to toggle between *Enabled* and *Disabled*.

   - Highlight *MediumErrorThreshold* and press the backspace key to remove the current value, then type a new smaller value.

   - Highlight *DMA Mode* and press the spacebar to toggle through UDMA 0 to 6 and MDMA 0 to 2.

3. Press **Control-A** to save your settings.

   See "Viewing Physical Drive Information" below to determine which functions your physical drives support.

   Medium Error Threshold is the number of bad blocks tolerated before the controller marks the drive as Dead. The default setting is 64 blocks. A setting of zero disables the function. When disabled, no drives are marked offline even when errors are detected.

Viewing Physical Drive Information (CLU)

To view information about a physical drive:

1. **Main Menu** >> *Physical Drive Management*

2. Highlight the physical drive you want and press **Enter**.

   Basic information displays.

3. Highlight *Advanced Information* and press **Enter**.

   Advanced information displays.

Viewing Physical Drive Statistics (CLU)

To view the statistics for the selected physical drive:

1. **Main Menu** >> *Physical Drive Management*

2. Highlight the physical drive you want and press **Enter**.

3. Highlight *Physical Drive Statistics* and press **Enter**.

Clearing Statistics

To clear physical drive statistics, see "Clearing Statistics (CLU)" on page 89.

Setting an Alias (CLU)

An alias is optional. To set an Alias for a physical drive:

1. **Main Menu** >> *Physical Drive Management*

2. Highlight the physical drive you want and press **Enter**.

3. Type an alias into the field provided.

    Maximum of 32 characters. Use letters, numbers, spaces and underscores.

4. Press **Control-A** to save your settings.

Locating a Physical Drive (CLU)

This feature helps you identify a physical drive within the Vess A-Series enclosure you are working with through the CLU. To locate a physical drive:

1. **Main Menu** >> *Physical Drive Management*

2. Highlight the physical drive you want and press **Enter**.

3. Highlight *Locate Physical Drive* and press **Enter**.

   The drive carrier status LED flashes for one minute. See the illustration below.

LED indicators on front of Vess A3340

HDD Status
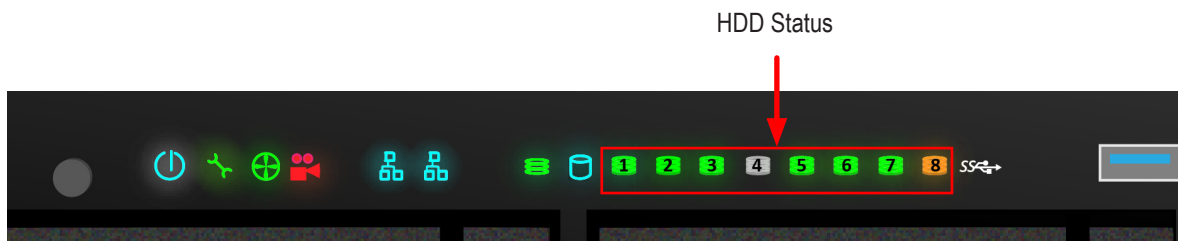
Managing Disk Arrays (CLU)

Disk Array Management includes the following functions:

Viewing a List of Disk Arrays (CLU)

To view a list of disk arrays:

> **Main Menu** >> *Disk Array Management*

The list of disk arrays displays.

Creating a Disk Array (CLU)

The CLU provides three methods of creating a disk array:

- **Automatic** – Creates a new disk array following a default set of parameters. Creates a hot spare drive for all RAID levels except RAID 0, when five or more unconfigured physical drives are available. You can accept or reject the proposed arrangement but you cannot modify it. See "Creating a Disk Array – Automatic"

- **Express** – You choose the parameters for a new disk array by specifying the characteristics you want. You can create multiple logical drives at the same time, however they are all identical. Creates a hot spare drive for all RAID levels except RAID 0. See "Creating a Disk Array – Express"

- **Advanced** – Enables you to specify all parameters for a new disk array, logical drives and spare drives. See "Creating a Disk Array – Advanced"

Creating a Disk Array – Automatic (CLU)

To create a disk array using the Automatic feature:

1. **Main Menu** >> *Disk Array Management* >> *Create New Array* >> *Configuration Method*

2. Press the spacebar to toggle to *Automatic*.

3. Press **Control-A** to save your settings and move to the next screen.

Important

A logical drive cannot be expanded once it has been created. To add capacity, you can either add another logical drive, or, delete the existing logical drive and create a larger one.

4. Review the proposed configuration of disk array and logical drives.

    •   To accept the proposed configuration and create the disk array and logical drives, highlight **Save settings and Continue** and press **Enter**.

    •   To reject the proposed configuration, highlight **Return to previous menu** and press **Enter**. You return to the Disk Arrays Summary screen.

        To create a disk array with different characteristics, repeat the steps above specifying different parameters but choose the **Express** or **Advanced** option.

Creating a Disk Array – Express (CLU)

To create a disk array using the Express feature:

1. **Main Menu** >> **Disk Array Management** >> **Create New Array** >> **Configuration Method** and press the spacebar to toggle to **Express**.

2. Highlight the following options and press to spacebar to choose **Yes** or **No**:

    •   Redundancy

    •   Capacity

> **Important**
>
> A logical drive cannot be expanded once it has been created. To add capacity, you can either add another logical drive, or, delete the existing logical drive and create a larger one.

- Performance

- Spare Drive

3. Highlight **Number of Logical Drives** and press the backspace key to erase the current value, then enter the number of logical drives you want.

4. Highlight **Application Type** and press the spacebar to toggle though the applications and choose the best one for your disk array.

- **File Server**

- **Video Stream**

- **Transaction Data**

- **Transaction Log**

- **Other**

5. Press **Control-A** to save your settings and move to the next screen.

6. Review the proposed configuration of disk array and logical drives.

   To accept the proposed configuration and create the disk array and logical drives, highlight **Save Configuration** and press **Enter**.

   To reject the proposed configuration, highlight **Return to previous menu** and press **Enter**. You return to the Disk Arrays Summary screen.

   To create a disk array with different characteristics, highlight **Create New Array** and press **Enter**. Repeat the steps above specifying different parameters. Or choose the **Advanced** option.

Creating a Disk Array – Advanced (CLU)

To create a disk array using the Advanced feature:

1. **Main Menu** >> **Disk Array Management** >> **Create New Array**

2. Highlight **Configuration Method** and press the spacebar to toggle to **Advanced**.

Step 1 – Disk Array Creation

1. If you want to specify an alias to the disk array, highlight **Alias** and type a name.

   Maximum of 32 characters (letters, numbers, spaces and underscores).

2. Choose whether to enable Media Patrol , PDM, and Power Management.

3. Choose a Media Type, HDD or SSD.

4. Highlight **Save Settings** and Continue and press **Enter**.

Step 2 –Select Physical Drives

1. Highlight a physical drive you want to add to your array and press the spacebar to choose it.

   Repeat this action until you have selected all the physical drives for your array.

2. Highlight **Save Settings and Continue** and press **Enter**.

Step 3 – Logical Drive Creation

1. If you want to specify an alias to the logical drive, highlight **Alias** and type a name.

   Maximum of 32 characters (letters, numbers, spaces and underscores).

2. Highlight **RAID Level** and press the spacebar to toggle though a list of available RAID levels.

3. If you want to create multiple logical drives, highlight **Capacity**, press the backspace key to remove the current value, then type a new smaller value.

4. RAID 30, 50 and 60 only. Highlight **Number of Axles** and press the spacebar to choose the number of axles.

5. For the following items, accept the default value or highlight and press the spacebar to choose a new value:

   • Highlight **Stripe** and press the spacebar to toggle through stripe sizes and choose 64 KB, 128 KB, 256 KB, 512 KB, or 1 MB.

   • Highlight **Sector** and press the spacebar to toggle through sector sizes and choose 512 B, 1 KB, 2 KB, or 4 KB.

   • Highlight **Write Policy** and press the spacebar to toggle write cache policy between **WriteBack** and **WriteThru** (write through).

   • Highlight **Read Policy** and press the spacebar to toggle read cache policy though [**ReadCache**, **ReadAhead**, and **NoCache**].

6. Highlight **Save Logical Drive** and press **Enter**.

Important

A logical drive cannot be expanded once it has been created. To add capacity, you can either add another logical drive, or, delete the existing logical drive and create a larger one.

Step 4 – Summary

Review logical drives you are about to create for your new array. Then do one of the following actions:

- If you agree with the logical drives as specified, highlight **Complete Disk Array Creation** and press **Enter**.

- If you specified less than the full capacity for the logical drive in the previous screen, and you want to add another logical drive now, highlight **Create New Logical Drive** and press **Enter**.

- If you do not agree with the logical drives, highlight **Return to Previous Screen** and press **Enter** to begin the process again.

Deleting a Disk Array (CLU)

Caution

When you delete a disk array, you delete all the logical drives and the data they contain. Back up all important data before deleting a disk array.

1. **Main Menu** >> ***Disk Array Management*** and press **Enter**.

2. Highlight the disk array you want to delete and press the spacebar to mark it.

   The mark is an asterisk (*) to the left of the listing.

3. Highlight ***Delete Marked Arrays*** and press **Enter**.

4. Press Y to confirm the deletion.

5. Press Y again to reconfirm.

Making Disk Array Settings (CLU)

To make disk array settings:

1. **Main Menu** >> *Disk Array Management*

    The list of disk arrays appears.

2. Highlight the disk array you want and press the **Enter**.

3. Make settings changes as required:

    - **Enter**, change or delete the alias in the **Alias** field

      Maximum of 32 characters (letters, numbers, spaces, and underscores).

    - *Media Patrol* – Highlight and press the spacebar to toggle between enable and disable.

    - *PDM* – Highlight and press the spacebar to toggle between enable and disable.

    - *Power Management* – Highlight and press the spacebar to toggle between enable and disable.

4. Press **Control-A** to save your settings.

	Notes
	You can also enable or disable Media Patrol for the entire RAID system.
	Power Management must be enabled on the disk array for the HDD Power Saving settings to be effective.
	Power management is limited to the features your HDDs actually support.

Viewing Disk Array Information (CLU)

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

    The information and settings screen appears.

3. Highlight any of the following and press **Enter** to view a list of:

    • Physical drives in this array

    • Logical drives in this array

    • Spare drives of the disk array

Enabling Media Patrol, PDM, and Power Management on a Disk Array (CLU)

Media Patrol checks the magnetic media on physical drives. Predictive Data Migration (PDM) migrates data from the suspect physical drive to a spare drive **before** the physical drive fails. Power Management parks the heads, spins down, and stops rotation after a set period of time to reduce power consumption.

Media Patrol, PDM, and Power Management are enabled by default. Enabled is the recommended setting for both features.

To enable Media Patrol, PDM, and Power Management on a disk array:

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

3. Highlight *Media Patrol* and press the spacebar to toggle between *Enable* and *Disable*.

4. Highlight *PDM* and press the spacebar to toggle between *Enable* and *Disable*.

5. Highlight *Power Management* and press the spacebar to toggle between *Enable* and *Disable*.
6. Press **Control-A** to save your settings.

Rebuilding a Disk Array (CLU)

Before you can rebuild, you must have a replacement or target physical drive of adequate capacity for your disk array.

To rebuild a disk array:

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

3. Highlight *Background Activities* >> **Rebuild**

   Default source and target drives are shown with possible alternative choices.

4. To choose different drive, highlight the drive, press the backspace key to remove the current number, then type a new number.

5. Highlight **Start** and press **Enter**.

Running Media Patrol on a Disk Array (CLU)

Media Patrol is a routine maintenance procedure that checks the magnetic media on each disk drive. If Media Patrol encounters a critical error, it triggers PDM if PDM is enabled on the disk array.

Running PDM on a Disk Array (CLU)

Predictive Data Migration (PDM) migrates data from the suspect physical drive to a spare drive **before** the physical drive fails.

Before you can run PDM, you must have a replacement or target physical drive of adequate capacity for your disk array.

To run PDM on a disk array:

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

3. Highlight *Background Activities* >> *Predictive Data Migration* and press **Enter**.

    Default source and target drives are shown with possible alternative choices.

4. To choose different drive, highlight the drive, press the backspace key to remove the current number, then type a new number.

5. Highlight *Start* and press **Enter**.

See "Enabling Media Patrol, PDM, and Power Management on a Disk Array (CLU)" on page 60.

For PDM rate, see "Making Background Activity Settings (CLU)" on page 76.

Running Transition on a Disk Array (CLU)

Transition is the process of replacing a revertible spare drive that is currently part of a disk array with an unconfigured physical drive or a non-revertible spare drive.

In order to run Transition:

- The spare drive must be Revertible.

- You must have an unconfigured physical drive of the same or larger capacity to replace the spare drive.

To run Transition on a disk array:

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

3. Highlight *Background Activities* >> *Transition*

   Default source and target drives are shown with possible alternative choices.

4. To choose different drive, highlight the drive, press the backspace key to remove the current number, then type a new number.

5. Highlight *Start* and press **Enter**.

For transition rate, see "Making Background Activity Settings (CLU)" on page 76.

Locating a Disk Array (CLU)

This feature helps you identify the physical drives assigned to the disk array you are working with in the CLU.

To locate a disk array:

1. **Main Menu** >> *Disk Array Management*

2. Highlight the disk array you want and press **Enter**.

3. Highlight *Locate Disk Array* and press **Enter**. The drive carrier status LEDs flash for one minute.

Managing Spare Drives (CLU)

Spare Drive Management includes the following functions:

- "Viewing a list of Spare Drives (CLU)" on page 64

- "Creating a Spare Drive (CLU)" on page 65

- "Running Redundancy Check (CLU)" on page 74

- "Deleting a Spare Drive (CLU)" on page 67

Viewing a list of Spare Drives (CLU)

To view a list of spare drives:

Main Menu >> **Spare Drive Management**

A list of the current spare drives appears, including the following parameters:

- **ID number**

- **Operational Status**

- **Physical Drive ID number**

- **Configured Capacity**

- **Revertible** – The spare drive returns to spare status after you replace the failed drive in the disk array.

- **Type** – Global (all disk arrays) or Dedicated (to specified disk arrays)

- **Dedicated to Array** – The array to which a dedicated spare is assigned

Creating a Spare Drive (CLU)

Only unconfigured physical drives can be used to make spares. Check your available drives under Physical Drive Management. See "Physical Drive Management (CLU)" on page 47.

1. **Main Menu** >> *Spare Drive Management* >> *Create New Spare Drive*

    A default physical drive is shown with possible alternative choices.

2. To choose different drive, highlight the drive, press the backspace key to remove the current number, then type a new number.

3. Highlight R**evertible** and press the spacebar to toggle between *Yes* and *No*.

    A revertible drive can be returned to spare status after you replace the failed drive in a disk array.

4. Highlight *Spare Type* and press the spacebar to toggle between *Dedicated* and *Global*.

    Dedicated means this spare drive can only be used with the specified disk arrays. Global means this spare drive can be used by any disk array.

    If you chose Dedicated, a default disk array is shown with possible alternative choices.

    To choose different array, highlight the array and press the backspace key to erase the current number, then type the new number.

5. Press **Control-A** to save the spare drive.

Making Spare Drive Settings (CLU)

To change spare drive settings:

1. **Main Menu** >> *Spare Drive Management*

    A list of the current spare drives appears, including the following parameters:

2. Highlight the spare drive you want to change and press **Enter**.

3. Highlight the setting you want to change:

    *   *Revertible* – A revertible drive can be returned to spare status after you replace the failed drive in a disk array.

    *   *Type* – Dedicated means this spare drive can only be used with the specified disk arrays. Global means this spare drive can be used by any disk array.

4. Press the spacebar to toggle between the choices.

5. For dedicated spares, type the array number the spare is assigned to.

6. Press **Control-A** to save your settings.

Running Spare Check (CLU)

To run Spare Check:

1. **Main Menu** >> *Spare Drive Management*

    A list of the current spare drives appears.

2. Highlight the spare drive you want to check and press **Enter**.

3. Highlight *Start Spare Check* and press **Enter**.

    The results appear next to Spare Check Status in the same window. Healthy means normal.

Deleting a Spare Drive (CLU)

Caution

If the spare drive you delete is the only spare, the controller does not rebuild a critical array until you provide a new spare drive.

To delete a spare drive:

1. **Main Menu** >> *Spare Drive Management*

   A list of the current spare drives appears.

2. Highlight the spare drive you want to delete and press the spacebar to mark it.

   The mark is an asterisk (*) to the left of the listing.

3. Highlight **Delete Marked Spare Drives** and press **Enter**.

4. Press Y to confirm the deletion.

Managing Logical Drives (CLU)

Logical drive management includes:

Creating a Logical Drive (CLU)

You can create logical drives on existing disk arrays if there is available space in the array.

To create a logical drive from an existing disk array:

1. **Main Menu** >> ***Disk Array Management***

2. Highlight the disk array in which you want to create a logical drive and press **Enter**.

3. ***Logical Drives in the Disk Array*** >> ***Create New Logical Drive***

   The Disk Array ID number and Maximum capacity available for the new logical drive are displayed.

4. Highlight the following parameters and press the backspace key to erase the current value:

   - ***Alias*** – Type an alias into the field, if desired. Maximum of 32 characters (letters, numbers, spaces and underscore).

   - ***RAID Level*** - Press the spacebar to toggle though a list of available RAID levels.

   - ***Capacity*** – Maximum capacity shown. **Enter** a smaller capacity if desired.

5.   Highlight the following parameters and press the spacebar to toggle though the available choices:

- *Stripe size* – Press the spacebar to choose: 64 KB,
   128 KB, 256 KB, 512 KB, or 1 MB.

- *Sector size* – Press the spacebar to choose: 512 B; 1 KB, 2 KB, or 4 KB.

- *Write Policy* – Press spacebar to choose: Write Back or Write Through.

- *Read Policy* – Press spacebar to choose: No Cache,
   Read Cache, or Read Ahead Cache.

6.   RAID 30, 50 and 60 only. Highlight **Number of Axles** and press the spacebar to choose the number of axles.

7.   Highlight **Save Logical Drive** and press **Enter**.

Note

If you did not use all of the available capacity of the disk array, you can create an additional logical drive at this point.

Deleting a Logical Drive (CLU)

> ⚠️ **Caution**
>
> **When you delete a logical drive, you delete all the data it contains. Back up all important data before deleting a logical drive.**

To delete a logical drive from a disk array:

1. **Main Menu** >> ***Disk Array Management***

2. Highlight the disk array that contains the logical drive you want to delete and press **Enter**.

3. Highlight ***Logical Drives in the Disk Array*** and press **Enter**.

4. Highlight the logical drive you want to delete and press the spacebar to mark it.

   The mark is an asterisk (*) to the left of the listing.

5. Highlight ***Delete Marked Logical Drives*** and press **Enter**.

6. Press Y to confirm the deletion.

   Press Y again to re-confirm.

Viewing Logical Drive Information (CLU)

To view logical drive information:

1. **Main Menu** >> *Logical Drive Management*

2. Highlight the logical drive you want and press **Enter**.

    The information and settings screen appears.

3. Highlight any of the following and press **Enter** to view more information:

    *   *Check Table* – Read Check, Write Check, and Inconsistency Check Tables

    *   *Logical Drive Statistics*

    *   *Background Activities*

    *   *Locate Logical Drive*

Viewing Logical Drive Statistics (CLU)

To view logical drive information:

1. **Main Menu** >> *Logical Drive Management*

2. Highlight the logical drive you want and press **Enter**.

    The information and settings screen appears.

3. Highlight *Logical Drive Statistics* and press **Enter**.

    The statistics screen appears.

To clear logical drive statistics, see "Clearing Statistics (CLU)" on page 89.

Viewing the Logical Drive Check Table (CLU)

To view logical drive information:

1. **Main Menu** >> *Logical Drive Management*

2. Highlight the logical drive you want and press **Enter**.

3. Highlight **Check Table** and press **Enter**.

4. Highlight one of the following options and press **Enter**:

   - *Show All Records*

   - *Read Check Table*

   - *Write Check Table*

   - *Inconsistent Check Table*

Making Logical Drive Settings (CLU)

To make Logical Drive settings:

1. **Main Menu** >> *Logical Drive Management*

2. Highlight the logical drive you want and press **Enter**.

3. For the following items, accept the existing setting choose a new one:

   - Highlight *Alias* and type an alias into the field provided.

   - Maximum of 32 characters (letters, numbers, spaces and underscores). An alias is optional.

   - Highlight *WritePolicy* and press the spacebar to toggle between *WriteBack* and *WriteThru* (write though).

   - Highlight *ReadPolicy* and press the spacebar to toggle though *ReadCache*, *ReadAhead* and *None*.

4. Press **Control-A** to save your settings.

Initializing a Logical Drive (CLU)

This function sets all data bits in the logical drive to zero.

<table>
<tr><td>⚠️</td><td>

Warning

When you initialize a logical drive, all the data on the logical drive is lost. Backup any important data before you initialize a logical drive.

</td></tr>
</table>

To initialize a logical drive:

1. **Main Menu** >> *Logical Drive Management* and press **Enter**.

2. Highlight the logical drive you want and press **Enter**.

3. Highlight *Background Activities* >> *Start Initialization*

    The initialization parameters appear.

    • **Initialization pattern** – The default 00000000 is best for most applications

    • **Quick Initialization** – Yes means only the first and last sections of the logical drives are initialized. No means the entire logical drive is initialized.

    To change a parameter, highlight it and press the backspace key to erase the current value, then type the new value.

4. Highlight *Start* and press **Enter**.

    If necessary, you can pause and resume or stop and restart the Initialization. You cannot access the logical drive until Initialization has finished.

For initialization rate, see "Making Background Activity Settings (CLU)" on page 76.

Running Redundancy Check (CLU)

Redundancy Check is a maintenance procedure for logical drives in fault-tolerant disk arrays that ensures all the data matches exactly.

To run Redundancy Check:

1. **Main Menu** >> *Logical Drive Management*

2. Highlight the logical drive you want and press **Enter**.

3. Highlight *Background Activities* >> *Start Redundancy Check*

    The redundancy check parameters appear.

    - **Auto Fix** – Corrects inconsistencies automatically

    - **Pause On Error** – Pauses the Redundancy Check when an error is found

    To change a parameter, highlight it and press the backspace toggle between *Yes* and *No*.

4. Highlight *Start* and press **Enter**.

    If necessary, you can pause and resume or stop and restart the Redundancy Check. You can use the logical drive while Redundancy Check is running.

For Redundancy Check rate, see "Making Background Activity Settings (CLU)" on page 76.

Locating a Logical Drive (CLU)

This feature helps you identify the physical drives assigned to the logical drive you are working with in the CLU. To locate a logical drive:

1. Main Menu >> Logical Drive Management

2. Highlight the logical drive you want and press Enter.

3. Highlight Locate Logical Drive and press Enter.

    The drive carrier status LEDs flash for one minute.

Managing Background Activity (CLU)

Background activity refers to any of several functions that take place in the background while normal operation of the Vess A-Series continues.

Background activities work in conjunction with disk arrays and logical drives. See "Managing Disk Arrays (CLU)" on page 52 and "Managing Logical Drives (CLU)" on page 68for more information about how and when to use background activities.

Background Activity Management includes the following functions:

- "Viewing Current Background Activities (CLU)" on page 75

- "Making Background Activity Settings (CLU)" on page 76

Viewing Current Background Activities (CLU)

Main Menu >> ***Background Activities***

A count of current background activities appears, including:

- **Rebuild**

- **PDM (Predictive Data Migration)**

- **Synchronization**

- **Redundancy Check**

- **Transition**

- **Initialization**

- **Media Patrol**

Making Background Activity Settings (CLU)

1. **Main Menu** >> **Background Activities** >> ***Background Activity Settings***

2. Highlight following and press the spacebar to toggle between ***Enabled*** and ***Disabled***.

   - ***Media Patrol*** – Checks the magnetic media on physical drives

   - ***Auto Rebuild*** – When enabled and no spare drive is available, the disk array begins to rebuild as soon as you replace the failed physical drive with an unconfigured physical drive of equal or greater size

3. Highlight following and press the spacebar to toggle through ***Low***, ***Medium***, and ***High*** rates:

   - ***Rebuild*** – Rebuilds data to a replacement physical drive in a disk array
   - ***PDM*** – Migrates data from a suspect physical drive to a replacement drive in a disk array
   - ***Transition*** – Returns a revertible spare drive to spare status
   - ***Synchronization*** – Checks the data integrity on disk arrays
   - ***Initialization*** – Full initialization sets all data bits in the logical drive to a specified pattern, such as all zeros
   - ***Redundancy Check*** – Checks, reports and can correct data inconsistencies in logical drives

   The rates are defined as follows:

   - **Low** – Fewer resources to activity, more to data read/write.

   - **Medium** – Balance of resources to activity and data read/write.

   - **High** – More resources to activity, fewer to data read/write.

4. Press **Control-A** to save your settings.

Working with the Event Viewer (CLU)

Working with the Event Viewer includes the following functions:

• "Clearing Runtime Events (CLU)" on page 78

• "Clearing NVRAM Events (CLU)" on page 79

The Event Viewer displays log of subsystem events. Events are classified as:

• **Runtime Events** – A list of and information about the 1023 most recent runtime events recorded since the subsystem was started

• **NVRAM Events** – A list of and information about the most important events over multiple subsystem startups. NVRAM events are stored in non-volatile memory

Event Severity Levels	
Level	**Description**
Fatal	Non-recoverable error or failure has occurred.
Critical	Action is needed now and the implications of the condition are serious.
Major	Action is needed now.
Minor	Action is needed but the condition is not a serious at this time.
Warning	User can decide whether or not action is required.
Information	Information only, no action is required.

Viewing Runtime Events (CLU)

To display Runtime Events:

1. **Main Menu** >> *Event Viewer*

    The log of Runtime Events appears. Events are added to the top of the list. Each item includes:

    - **Sequence number** – Begins with 0 at system startup.

    - **Device** – Disk Array, Logical Drive, Physical Drive by its ID number.

    - **Severity** – See the table above.

    - **Timestamp** – Date and time the event happened.

    - **Description** – A description of the event in plain language.

2. Press the up and down arrow keys to scroll through the log.

Clearing Runtime Events (CLU)

To clear the Runtime Event log:

1. **Main Menu** >> *Event Viewer* >> *Clear Runtime Event Log*

2. Press Y to confirm.

Viewing NVRAM Events (CLU)

This screen displays a list of and information about the most important events over multiple subsystem startups.

To display NVRAM events:

1. **Main Menu** >> *Event Viewer* >> *NVRAM Events*

    The log of NVRAM Events appears. Events are added to the top of the list. Each item includes:

    - **Sequence number** – Begins with 0 at system startup.

    - **Device** – Disk Array, Logical Drive, Physical Drive by its ID number.

    - **Severity** – See the table on the previous page.

    - **Timestamp** – Date and time the event happened.

    - **Description** – A description of the event in plain language.

2. Press the up and down arrow keys to scroll through the log.

Clearing NVRAM Events (CLU)

To clear the Runtime Event log:

1. **Main Menu** >> *Event Viewer* >> *NVRAM Events* >> *Clear NVRAM Event Log*

2. Press Y to confirm.

Managing Users (CLU)

User Management includes the following functions:

- "Viewing User Information (CLU)" on page 80
- "Creating a User (CLU)" on page 81
- "Changing User Settings (CLU)" on page 82
- "Changing User Password (CLU)" on page 83
- "Deleting a User (CLU)" on page 84

Viewing User Information (CLU)

Each user types their user name and password to log into the CLI.

To view a list of current user accounts:

1. **Main Menu** >> *Additional Info and Management* >> *User Management*

   A list of the current users appears.

Creating a User (CLU)

To create a new user account:

1. **Main Menu** >> *Additional Info and Management* >> *User Management* >> *Create New User*

2. Highlight each field and type in the appropriate information:

   - **User name** (Maximum 31 characters; use letters, numbers, and underscores. No spaces.)

   - **Password** (Optional. Maximum 31 characters. Use letters, numbers, and underscore.)

   - **Display name** (Optional)

   - **User's email address**

3. Highlight **Privilege** and press the space bar to toggle though the options.

   See the Table on the next page.

4. Press **Control-A** to save the user.

User Privileges	
Level	**Meaning**
View	Allows the user to see all status and settings but not to make any changes
Maintenance	Allows the user to perform maintenance tasks including Rebuilding, PDM, Media Patrol, and Redundancy Check
Power	Allows the user to create (but not delete) disk arrays and logical drives, change RAID levels, change stripe size; change settings of components such as disk arrays, logical drives, physical drives, and the controller
Super	Allows the user full access to all functions including create and delete users and changing the settings of other users, and delete disk arrays and logical drives. The default "administrator" account is a Super User

Changing User Settings (CLU)

The Administrator or a **Super User** can change other users' settings.

To change user settings:

1. **Main Menu** >> *Additional Info and Management* >> *User Management*
2. Highlight the User whose settings you want to change and press **Enter**.
3. Highlight **Privilege** and press the space bar to toggle though the options.

    See the Table above.

4. Highlight **Status** and press the space bar to toggle between *Enabled* and *Disabled*.
5. Highlight the items you want and press the backspace key to erase the current value, then type the new value:

    • **User name**

    • **Email address**

6. Press **Control-A** to save the settings.

> Important
>
> If a user is logged-in when his account is disabled, the user is immediately logged-out.

Changing User Password (CLU)

The Administrator or a **Super User** can change other users' passwords.

To change a password:

1. **Main Menu** >> **Additional Info and Management** >> **User Management**
2. Highlight the User whose password you want to change and press **Enter**.
3. Highlight **Change Password...** and press **Enter**.
4. Highlight **New Password** and type a new password.

    Maximum 31 characters. Use letters, numbers, and underscore.
5. Highlight **Retype Password** and type the new password again to verify.
6. Press **Control-A** to save the new password.

	Note
	To reset the Administrator's password to the factory default, see "Restoring Factory Defaults (CLU)" on page 90.

Deleting a User (CLU)

The Administrator or a **Super User** can delete other users. You cannot delete the account you used to log in. There must always be one **Super User** account.

Rather than deleting a user, consider disabling a user account.

To delete a user:

1. Log in under a user name other than the one you want to delete.

2. **Main Menu** >> *Additional Info and Management* >> **User Management**

3. Highlight the user you want to delete and press the spacebar to mark it.

    The mark is an asterisk (*) to the left of the listing.

4. Highlight **Delete Marked Users** and press **Enter**.

5. Press Y to confirm the deletion.

Software Management (CLU)

Software Management includes the following functions:

- "Email Settings (CLU)" on page 85

- "Web Server Settings (CLU)" on page 85

Email Settings (CLU)

By default, Email service is set to Automatic and its normal status is Started.

To make Email service settings:

1. **Main Menu** >> *Additional Info and Management* >> **Software Management** >> *Email >> Startup Type*

2. Press the spacebar to toggle between **Automatic** and **Manual**.

3. Highlight the following and press the backspace key to erase the current value, then type the new value:

    - SMTP server IP address or server name

    - Server Port number (25 is the default)

4. Highlight **Authentication** and press the spacebar to toggle between **Yes** and **No**.

    If you selected Yes, type in a User name and Password in the fields provided.

5. The following items are optional but recommended. Highlight and press the backspace key to erase the current value, then type the new value:

    - Sender's email address

    - Subject Line for the email message

6. Press **Control-A** to save your settings.

To start, stop or restart the Email service, highlight **Start**, **Stop** or **Restart** and press **Enter**.

Web Server Settings (CLU)

By default, Web Server service is set to Automatic and its normal status is Started.

To make Web Server service settings:

1. **Main Menu** >> *Additional Info and Management* >> *Software Management* >> *Startup Type*

2. Press the spacebar to toggle between ***Automatic*** and ***Manual***.

3. Highlight the following and press the backspace key to erase the current value, then type the new value:

    - HTTP Port (8090 is the default)

    - Session Time Out (24 minutes is the default. 1440 minutes = 24 hours)

4. Highlight ***SSL*** and press the spacebar to toggle between ***Enabled*** and ***Disabled***.

5. Highlight ***HTTPS Port*** and press the backspace key to erase the current value, then type the new value. 8443 is the default.

6. Press **Control-A** to save your settings.

To start, stop or restart the service, highlight ***Start***, ***Stop***, or ***Restart*** and press **Enter**.

SNMP Settings (CLU)

By default, Simple Network Management Protocol (SNMP) service is set to Automatic and its normal status is Started.

To make SNMP service settings:

1. **Main Menu** >> ***Additional Info and Management*** >> ***Software Management*** >> ***SNMP*** >> **Startup Type**

2. Press the spacebar to toggle between **Automatic** and **Manual**.

3. Highlight the following and press the backspace key to erase the current value, then type the new value:

    - ***Port Number*** – 161 is the default

- ***System Name*** – (optional) Type a system name in this field

- ***System Location*** – Type a country name in this field

- ***System Contact*** – Type the email address of your system administrator in this field

- ***Read Community*** – Type a community name in this field

4. Press **Control-A** to save your settings.

To start, stop or restart the SNMP service, highlight ***Start***, ***Stop***, or ***Restart*** and press **Enter**.

Managing SNMP Trap Sinks (CLU)

Viewing a List of Trap Sinks

To create a trap sink:

1. **Main Menu** >> *Additional Info and Management* >> *Software Management* >> *SNMP* >> *Trap Sinks*

   A list of the current trap sinks appears.

Adding a Trap Sink

To add a trap sink:

1. **Main Menu** >> *Additional Info and Management* >> *Software Management* >> *SNMP* >> *Trap Sinks* >> *Create New Trap Sink* >> *Trap Sink IP address*

2. Press the backspace key to erase the current value, then type the new IP address in this field.

3. Highlight **Trap Filter** and press the spacebar to toggle through the severity levels.

   See the Table below.

4. Press **Control-A** to save the Trap Sink.

Event Severity Levels	
Level	**Description**
Fatal	Non-recoverable error or failure has occurred.
Critical	Action is needed now and the implications of the condition are serious.
Major	Action is needed now.
Minor	Action is needed but the condition is not a serious at this time.
Warning	User can decide whether or not action is required.
Information	Information only, no action is required.

Deleting a Trap Sink

To delete a trap sink:

1. **Main Menu** >> *Additional Info and Management* >> *Software Management* >> *SNMP* >> *Trap Sinks*

Clearing Statistics (CLU)

This function clears the statistical counts for the RAID controller, iSCSI ports, physical drives, and logical drives. To clear statistics:

1. **Main Menu** >> *Additional Info and Management* >> *Clear Statistics*

2. Press Y to confirm the deletion.

Restoring Factory Defaults (CLU)

This function restores the factory default settings to the firmware and software items you select.
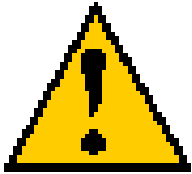
Caution

Restoring default settings can disrupt your Vess A-Series functions. Use this feature only when necessary

1. **Main Menu** >> *Additional Info and Management* >> *Restore Factory Defaults*

2. Highlight the setting groups you want to restore and press the spacebar to toggle between **Yes** and **No**.

   "Yes" means this setting is restored to the default value.

   "No" means the current setting remains untouched.

3. Highlight *Restore Factory Defaults* and press **Enter**.

4. Press Y to confirm the reset.

Buzzer

Making Buzzer Settings

The buzzer sounds to inform you that the Vess A-Series needs attention.

To make buzzer settings:

1. **Main Menu** >> *Buzzer*

    A list of Controllers appears with the current buzzer setting and status.

2. Highlight *Enabled* and press the spacebar to toggle between *Yes* and *No*.

3. Press **Control-A** to save your settings.

Silencing the Buzzer

> ⚠️ **Caution**
>
> **This action disables the buzzer for all events.**

To silence the buzzer, follow the procedure above for disabling the buzzer.

MANAGING WITH WEBPAM PROE

This chapter describes using WebPAM PROe to monitor and manage your RAID system.

Logging into WebPAM PROe

You can log into WebPAM PROe in either of two ways:

- "Logging in at the Enclosure" on page 92

- "Logging in over the Network" on page 93

Logging in at the Enclosure

At the Vess enclosure to log into WebPAM PROe, do one of the following actions:

- Double-click the WebPAM PROe desktop icon.

- Choose WebPAM PROe in the Windows Programs menu.

- Follow the steps under "Logging in over the Network" on page 93.

Note

The default IP settings for the Gigabit Ethernet ports are:

Port 1 = 192.168.0.1

Port 2 = 192.168.1.1
IP settings for the ports are controlled by the OS. Use the normal IP settings configuration procedure for the OS you are using if you want to change the default settings.

Logging in over the Network

	Important
✔	For Vess A-Series running Windows OS, it is necessary to disable the Windows Firewall in order to allow access to WebPAM PROe through the network interface. If the Firewall is running, no management access is permitted from the network.

You can log into WebPAM PROe from any PC with a network connection to the Vess A-Series enclosure.

1.　Launch your Browser.

2.　In the Browser address field, type the information provided below. Then press Enter. Note that this example uses the default IP address for Port 1

If you chose External SSL Security during installation, use the Secure Connection. Otherwise, use the Regular Connection.

Regular Connection

• 　WebPAM PROe uses an HTTP connection. . . . . .http://

• 　Enter the Subsystem IP address 192.168.0.1

• 　Enter the Port number . . . . :8090

Together, your entry looks like this:

　　　http://192.168.0.1:8090

Secure Connection

- WebPAM PROe uses a secure HTTP connection . . . . .https://

- Enter the Subsystem IP address 192.168.0.1

- Enter the Port number . . . . :8443

Together, your entry looks like this:

https://192.168.0.1:8443/
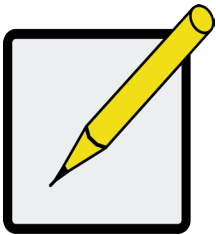
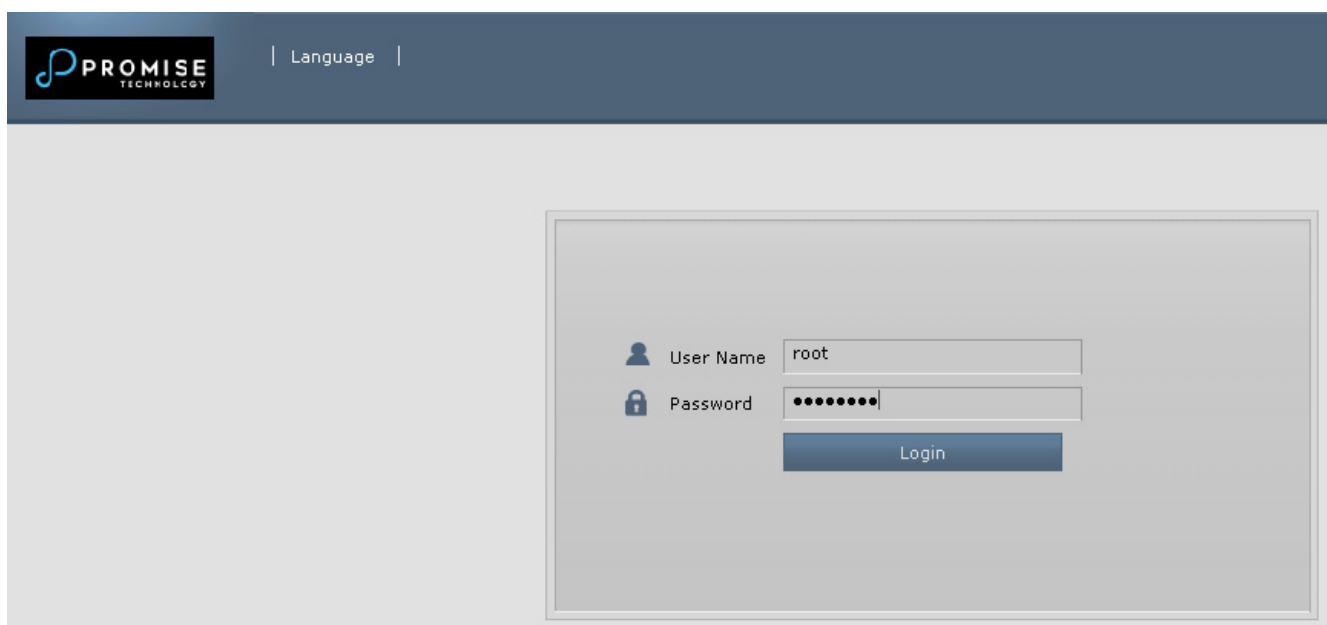| Note |
| --- |
| • You can enter the Host PC's network name in place of the IP address. |
| • If you are logging in at the Host PC, you can enter local Host in place of the IP address. |
| • Whether you select a regular or a secure connection, your login to WebPAM PROe and your user password are always secure. |

Login Screen

When the opening screen appears:

1. Type **administrator** in the User Name field.

2. Type **password** in the Password field.

3. Click the **Login** button.

The User Name and Password are case sensitive. See Figure 1.
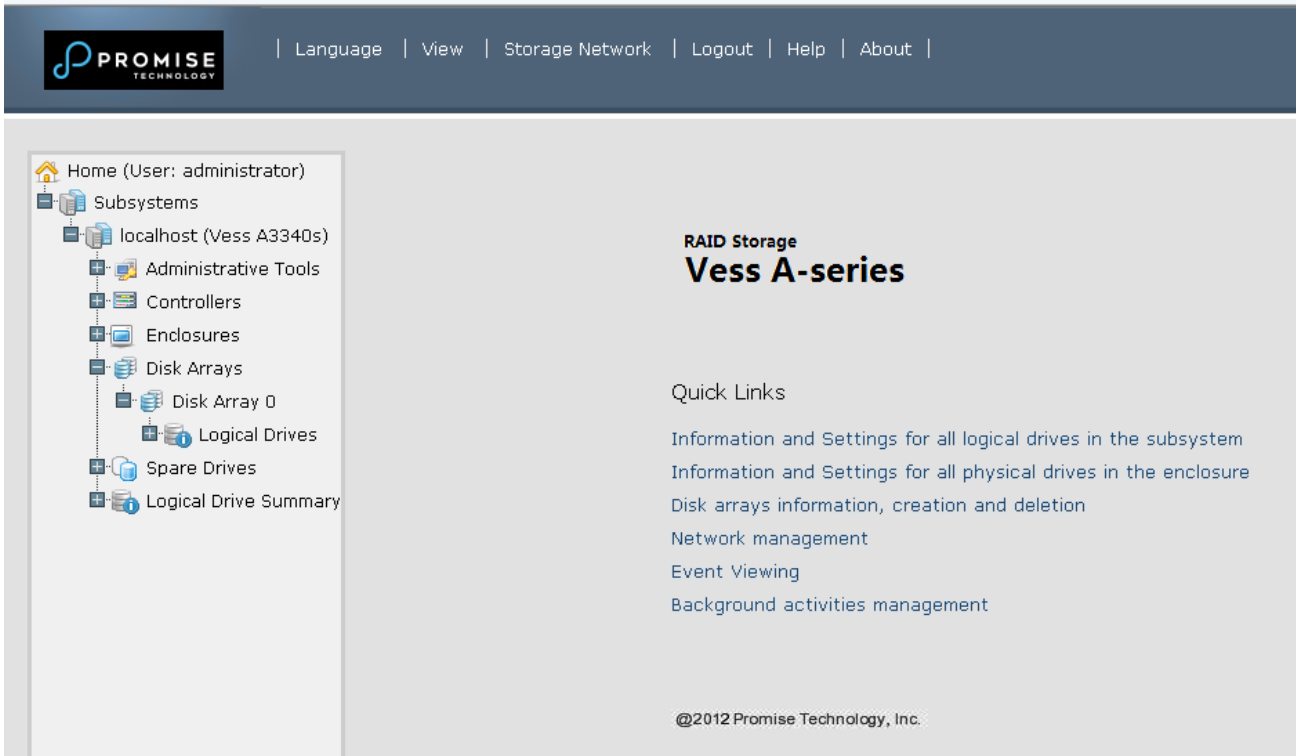
The WebPAM PROe login screen

Quick Links menu

The Quick Links menu is the administrator's Home page for WebPAM PROe. Here you will find links to menus to view setting and manage logical drives, physical drives, and disk arrays. Also links to view network settings and event logs, as well as the background activities management menu.

Quick Links menu - User's Home page

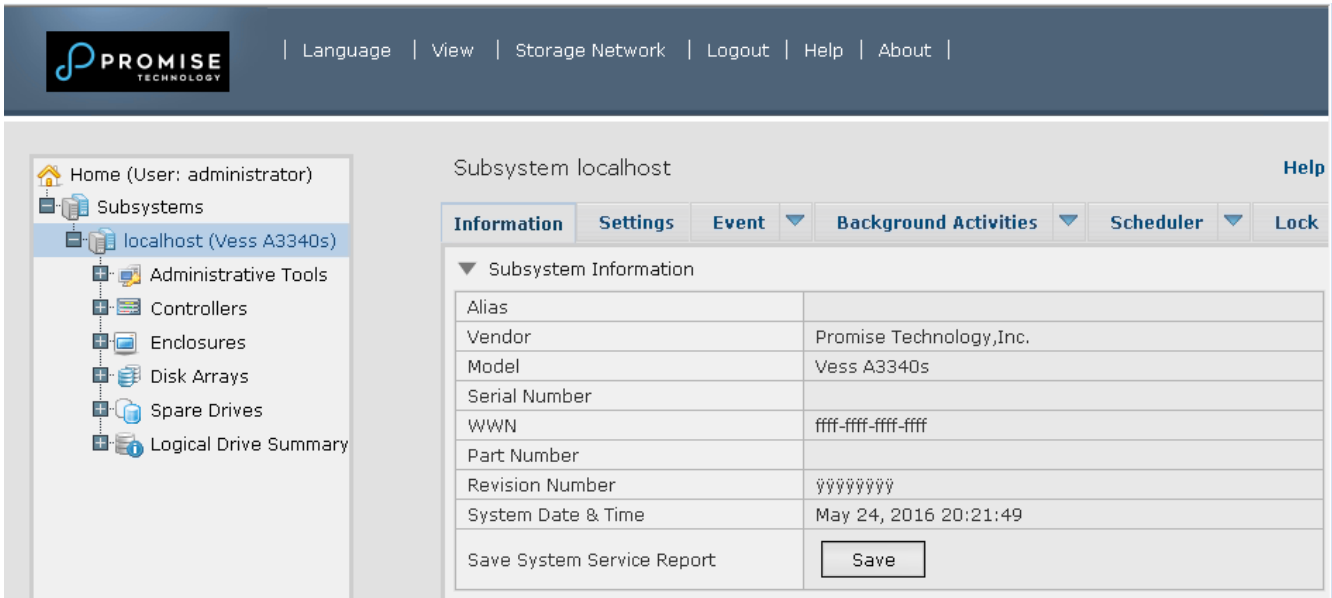# Using the WebPAM PROe Interface

WebPAM PROe is browser-based RAID management software with a graphic user interface. Basic user interface components and functions include:

WebPAM PROe interface - Subsystem home page

- Tree View
- Event Frame

Using the Header

The Header contains the following items:

Language – Choose a display language

View – To view the Event Frame,

Logout – To logout

Using Tree View

Tree View enables you to navigate around all components of the Vess enclosure, software management, RAID controller, enclosure, physical drives, disk arrays, logical drives, and spare drives. The figure below shows the components of Tree View.

WebPAM PROe Tree View

Logged-in User

Vess Class A3340s enclosure

ferent for the Administrator and Super Users than for other users. The
users.
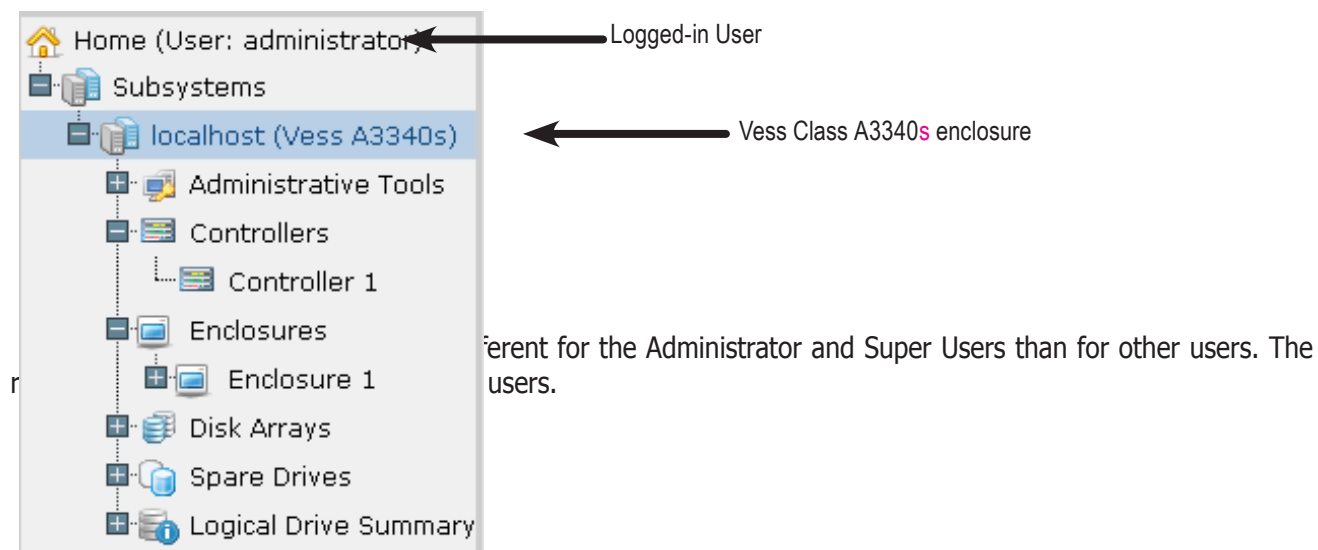
Using Management View

Management View displays information and settings menus according to the item you choose in Tree View. It presents the user interface for the Vess enclosure, including creation, maintenance, deletion, and monitoring of disk arrays and logical drives. Function tabs access menus to control specific actions and processes.

Click the **Help** link to the right of the tabs in Management View to access online help for the function currently displayed.

Choosing a Display Language

WebPAM PROe displays in the following languages:

• English	• Italian
• Simplified Chinese	• Japanese
• Traditional Chinese	• Korean
• French	• Spanish
• German	• Russian

To change the display language:

1. Click the **Language** drop-down menu in the Header.

2. Highlight the language you prefer.

   WebPAM PROe displays in the chosen language.

Viewing the Event Frame

To view the Event Frame, click Show Event Frame in the Header. To hide the Event Frame, click Hide Event Frame in the Header.

In the event frame, events are listed and sorted by:

• **Device** – Disk array, logical drive, physical drive, controller, etc.

• **Event ID** – The hexadecimal number that identifies the specific type of event

• **Severity** – See below:

       • Information – Information only, no action is required

       • Warning – User can decide whether or not action is required

       • Minor – Action is needed but the condition is not serious at this time

       • Major – Action is needed now

       • Critical – Action is needed now and the implications of the condition are serious

       • Fatal – Non-Recoverable error or failure has occurred

• **Time** – Time and date of the occurrence

• **Description** – A brief description of the event

You can also view events by clicking the Subsystems icon in Tree View, then clicking the Event tab in Management View.

Logging out of WebPAM PROe

There are two ways to log out of WebPAM PROe:

- Close your browser window

- Click **Logout** in the WebPAM PROe Header

Clicking **Logout** brings you back to the Login Screen. After logging out, you must enter your user name and password in order to log in again.

Subsystem Management

The menus listed under Subsystems are all the menus used for device management. Click on the Subsystems icon to view read-only information for the Vess including the management IP address, Alias, Model and WWN.

To view the menus used for system management, click the **+** symbol of the Subsystems icon to reveal the child menu icons for the following:

- **Administrative Tools** (includes links for User Management, View Network Settings, Performance Monitoring and Software Management)

- **Controllers** (view controller information and manage settings)

- **Enclosures** (view device information and virtual enclosure, set temperature thresholds for warnings and enable/disable warning buzzer)

- **Disk Arrays** (manage disk arrays)

- **Spare Drives** (manage spare drives)

- **Logical Drives Summary** (read-only logical drive information display)

Click on the subsystem IP address and model name listed under the Subsystems top-level menu icon in Tree View. In the Information tab, the following information for the subsystem appears:

- *Alias*
- *Model*
- *World Wide Number*
- *Revision Number*

- *Vendor*
- *Serial Number*
- *Part Number*
- *System Date & Time*

Here you can also save a *System Service Report* (useful for troubleshooting) in the form of an HTML file to the computer you are using by clicking on the **Save** button. See "Saving a Service Report".

The Subsystem home menu includes the following function tabs:

- **Information** (described above)
- **Background Activities**
- **Event** (list runtime and NVRAM events)

- **Settings** (assign an Alias)
- **Scheduler** (schedule background activities)
- **Lock** (lock/unlock subsystem)

Background Activities

Background activities perform a variety of preventive and remedial functions on your physical drives, disk arrays, logical drives, and other components.

You can run a background activity immediately or schedule it to run at a later time.

Setting options for each activity are listed after the scheduling options. These settings determine how the background activity affects I/O performance.

View Current Background Activities

To view current background activities:

1. Click the Subsystem icon of the subsystem on which you want to view Background Activities.

2. In the Subsystem menu, click the Background Activities tab. Background Activities currently running are displayed in the top portion of the menu. You can also view the current Background Activities parameter settings in the lower part of the menu. Click the Background Activity Parameters menu expander to view the current parameter settings.

View Background Activities Parameters settings

To view current background parameter settings:

1. Click the Subsystem icon of the subsystem on which you want to view Background Activities.

2. Click the Background Activity Parameters menu expander to view the current parameter settings. The parameters listed are as follows:

- Rebuild Rate
- Background Synchronization Rate
- Logical Drive Initialization Rate
- Redundancy Check Rate
- Migration Rate
- PDM Rate

- Transition Rate
- Reassigned Block Threshold
- Error Block Threshold
- Enable Media Patrol
- Enable Auto Rebuild

Manage Background Activities Settings

The parameters listed in the Background Activities menu are configured in the Background Activities Settings menu. To change Background Activities settings

1. Click the Subsystem icon of the subsystem on which you want to view Background Activities.

2. Click the menu expander between the Background Activities tab and the Scheduler tab and select the *Settings* option. The following settings can be configured:

    • Rebuild Rate *High, Medium, Low*

    • Background Synchronization Rate *High, Medium, Low*

    • Logical Drive Initialization Rate *High, Medium, Low*

    • Redundancy Check Rate *High, Medium, Low*

    • Migration Rate *High, Medium, Low*

    • PDM Rate *High, Medium, Low*

    • Transition Rate *High, Medium, Low*

    • Reassigned Block Threshold

    • Error Block Threshold

    • Enable Media Patrol

    • Enable Auto Rebuild

These settings can be also scheduled using the Scheduler. See the instructions for using schedules following the parameters descriptions below.

Rebuild Settings

To change Rebuild setting the in Background Activities Settings menu:

1. Use the **Rebuild Rate** drop-down menu to choose a rate:

    - **Low** – Fewer system resources to the Rebuild, more to data read/write operations.

    - **Medium** – Balances system resources between the Rebuild and data read/write operations.

    - **High** – More system resources to the Rebuild, fewer to data read/write operations.

2. To enable Auto Rebuild (rebuilds when you swap out the failed drive with a new one) Check the **Enable Auto Rebuild** box.

3. Click the **Submit** button.

Rebuild Rate

When you rebuild a disk array, you are actually rebuilding the data on one physical drive.

- When a physical drive in a disk array fails and a spare drive of adequate capacity is available, the disk array begins to rebuild automatically using the spare drive.

- If there is no spare drive of adequate capacity, but the Auto Rebuild function is ENABLED, the disk array begins to rebuild automatically as soon as you remove the failed physical drive and install an unconfigured physical drive in the same slot.

- If there is no spare drive of adequate capacity and the Auto Rebuild function is DISABLED, you must replace the failed drive with an unconfigured physical drive, then perform a **Manual Rebuild**.

Background Synchronization

Synchronization is automatically applied to redundant logical drives when they are created. Synchronization recalculates the redundancy data to ensure that the working data on the physical drives is properly in sync.

<u>Background Synchronization Rate</u>

1. To change Background Synchronization Rate setting the in Background Activities Settings menu: Click the Synchronization Rate drop-down menu and choose a rate:

   - **Low** – Fewer system resources to Synchronization, more to data read/write operations.

   - **Medium** – Balances system resources between Synchronization and data read/write operations.

   - **High** – More system resources to Synchronization, fewer to data read/write operations.

2. Click the **Submit** button.

Logical Drive Initialization

Technically speaking, **Initialization** is a foreground activity, as you cannot access a logical drive while it is initiating.

Initialization is normally done to logical drives after they are created from a disk array. Initialization sets all data bits in the logical drive to zero. The action is useful because there may be residual data on the logical drives left behind from earlier configurations. For this reason, Initialization is recommended whenever you create a logical drive.

<u>Logical Drive Initialization Rate</u>

To change Logical Drive Initialization Rate setting the in Background Activities Settings menu:

1. Click the Logical Drive Initialization Rate drop-down menu and choose a rate:

   - **Low** – Fewer system resources to Initialization, more to data read/write operations.

   - **Medium** – Balances system resources between Initialization and data read/write operations.

   - **High** – More system resources to Initialization, fewer to data read/write operations.

2. Click the **Submit** button.

Redundancy Check

Redundancy Check is a routine maintenance procedure for fault-tolerant disk arrays (those with redundancy) that ensures all the data matches exactly. Redundancy Check can also correct inconsistencies.

> **Note**
>
> You can use the scheduler to set up a Redundancy Check Schedule.
> To set up a schedule, click the menu expander to the right of the **Scheduler** tab and select *Redundancy Check Schedule.*

Redundancy Check Rate

To change Redundancy Check Rate setting the in Background Activities Settings menu:

1. Click the Redundancy Check Rate drop-down menu and choose a rate:

    *   **Low** – Fewer system resources to Redundancy Check, more to data read/write operations.

    *   **Medium** – Balances system resources between Redundancy Check and data read/write operations.

    *   **High** – More system resources to Redundancy Check, fewer to data read/write operations.

2. Click the **Submit** button.

PDM

Predictive Data Migration (PDM) is the migration of data from the suspect physical drive to a spare drive, similar to rebuilding a logical drive. But unlike Rebuilding, PDM constantly monitors your physical drives and automatically copies your data to a spare drive before the physical drive fails and your logical drive goes Critical.

PDM Settings

To change PDM setting the in Background Activities Settings menu:

1. Click the PDM Rate drop-down menu and choose a rate:

    - **Low** – Fewer system resources to PDM, more to data read/write operations.
    - **Medium** – Balances system resources between PDM and data read/write operations.
    - **High** – More system resources to PDM, fewer to data read/write operations.

2. Highlight the current values in the block threshold fields and input new values.

    Reassigned Block Threshold range is 1 to 512 blocks.

    Error Block Threshold range is 1 to 2048 blocks.

3. Click the **Submit** button.

Transition

Transition is the process of replacing a revertible spare drive that is currently part of a disk array with an unconfigured physical drive or a non-revertible spare drive.

Transition Rate

To change Transition Rate setting the in Background Activities Settings menu:

1. Click the Transition Rate drop-down menu and choose a rate:

    - **Low** – Fewer system resources to Transition, more to data read/write operations.
    - **Medium** – Balances system resources between Transition and data read/write operations.
    - **High** – More system resources to Transition, fewer to data read/write operations.

2. Click the **Confirm** button.

Media Patrol

Media Patrol is a routine maintenance procedure that checks the magnetic media on each disk drive. Media Patrol checks are enabled by default on all disk arrays and spare drives. Media Patrol is concerned with the media itself, not the data recorded on the media. If Media Patrol encounters a critical error, it triggers PDM if PDM is enabled on the disk array.

Media Patrol Settings

Media Patrol is enabled or disabled using the Background Activities menu or you can create a schedule to run Media Patrol.

- To enable Media Patrol, click on the Subsystem in Tree View then click on the Background Activities menu tab. Click to check the *Enable Media Patrol* option. Notice also that the *Auto Rebuild* option is here as well. If you want to automatically begin rebuilding a logical drive as soon as a faulty drive is replaced, make sure this option is enabled.

- To begin Media Patrol manually, click on the menu expander to the right of the Background Activities tab and scroll down and select *Start Media Patrol* to see the Start Media Patrol menu. Then click on the **Start** button.

- To schedule Media Patrol, click on the menu expander to the right of the Scheduler tab and scroll down and select *Add Media Patrol Schedule* to open the schedule menu. Use this menu to add a Media Patrol schedule.

Managing Activity Schedules

Schedules for **Media Patrol**, **Redundancy Check** and **Spare Drive Check** can be created to run during off peak times.

Add or delete an activity schedule

To add, enable or delete an activity schedule, click on the Subsystem in Tree View, then click on the Scheduler menu expander to the right of the Scheduler tab. Scroll down to the schedule option you want to view that menu. Schedule options are *Add Media Patrol Schedule*, *Add Redundancy Check Schedule*, *Add Spare Check Schedule* and *Delete Schedule*.

View or modify an existing activity schedule

To view existing schedules including the recurrence, start time and status of existing schedules, click on the Scheduler tab. Here you can then modify any listed schedule by clicking on the name of the schedule in the list.

Event Logs

Event logs are useful for troubleshooting, tracking functions and monitoring subsystems. To view, save or clear subsystem event logs, click on the subsystem in Tree View, then click on the Event menu expander. Choose to display *Runtime Events* or *NVRAM Events*. Event logs can be saved as a simple text file by clicking the **Save** button in either menu. To clear the log and start fresh, click the **Clear Event Log** button.

Administrative Tools

Click the **+** symbol of the Administrative Tools icon reveal subsystem administrative tools menu links for User Management, View Network Settings, Performance Monitoring and Software Management. The Administrative Tools menu lists text hyperlinks to these same menus, plus links to menus to Restore Factory Default settings, Clear Statistics and Save System Service Report.

Restore factory default settings

To restore any firmware or software settings to the default values:

1. Click on the Administrative Tools icon.

2. Click on the *Restore Factory Defaults* link to reveal a new menu.

3. Check mark the option boxes for the settings you want to return to the factory default values. Default Settings options include:

Firmware Default Settings	**Software Default Settings**
• Background Activities	• Service Settings
• Controller Settings	• Web Server Settings
• Enclosure Settings	• Email Settings
• Physical Drive Settings	
• Subsystem Settings	

4. Click the **Submit** button to return the selected settings to default values. To deselect all options and start over, click the **Reset** button.

Clear Statistics

To clear all subsystem statistics for controllers, ports physical drives and logical drives:

1. Click on the Administrative Tools icon.

2. Click on the *Clear Statistics* link to reveal a new menu.

3. Click on the **Submit** button to clear all device statistics.

User Management

User Management deals with user accounts.

Viewing User Information

The view a list of users, their status, access privileges, display name, and email address:

1. Click the Administrative Tools icon.

2. Click the User Management icon.

The Information tab appears in Management View.

Making User Settings

To change settings of other users:

1. Log into WebPAM PROe as the Administrator or a Super User.

2. Click the Administrative Tools icon.

3. Click the User Management icon.

4. Click the **Information** tab.

5. In the list of users, click the link of the user whose settings you want to change.

   The Settings screen for the chosen user displays.

6. Enter or change the settings for this user.

   - Enable/disable this user
   - Display name
   - Privilege.

7. Click the **Submit** button.

The Administrator or Super User can change another user's password.

Making Your Own User Settings

To change your own user settings:

1. Log into WebPAM PROe under your own user name.

2.   Click the Administrative Tools icon.

3.   Click the User Management icon.

4.   Click the **Settings** tab in Management View.

5.   Enter or change the display name or mail address.

6.   Click the **Submit** button.

Changing Your Own Password

To set or change your own password:

1.   Log into WebPAM PROe under your own user name.

2.   Click the Administrative Tools icon.

3.   Click the User Management icon.

4.   Click the **Password** tab in Management View.

5.   Enter the current password in the Old Password field.

6.   If you do not have a password, leave this field blank.

7.   Enter the new password in the New Password field.

8.   Enter the new password in the Retype Password field.

9.   Click the **Submit** button.

Creating a User

To create a user:

1. Log into WebPAM PROe as the Administrator or a Super User.

2. Click the Administrative Tools icon.

3. Click the User Management icon.

4. Click the **Create** tab in Management View.

5. Enter a user name in the User Name field.

6. Enter a password for this user in the New Password and Retype Password fields.

A password is optional. If you do not assign password, tell this user to leave the password field blank when he/she logs into to WebPAM PROe.

7. Check the *Enabled* box to enable this user on this subsystem.

8. Enter a display name in the Display Name field.

A display name is optional but recommended.

9. Choose a privilege level from the Privilege drop-down menu.

For definitions of each privilege level, see the List of User Privileges below.

10. Click the **Submit** button.

List of User Privileges

- **View** – Allows the user to see all status and settings but not to make any changes

- **Maintenance** – Allows the user to perform maintenance tasks including

- Rebuilding, PDM, Media Patrol, and Redundancy Check.

- **Power** – Allows the user to create (but not delete) disk arrays and logical drives, change RAID levels, change stripe size; change settings of components such as disk arrays, logical drives, physical drives, and the controller.

- **Super** – Allows the user full access to all functions including create and delete users and changing the settings of other users, and delete disk arrays and logical drives. The default "administrator" account is a Super User.

Deleting a User

There is always at least one Super User account. You cannot delete the user account you used to log in. To delete a user:

1. Log into WebPAM PROe as the Administrator or a Super User.

2. Click the Administrative Tools icon.

3. Click the User Management icon.

4. Click the **Delete** tab in Management View.

5. Check the box to the left of the user you want to delete.

6. Click the **Submit** button.

7. Click **OK** in the confirmation box.

View Network Settings

To view network settings for the Ethernet ports, including the port used for access to WebPAM PROe, click on the View Network Settings icon under Administrative Tools. Information listed for each port includes:

- If the port is enabled/disabled
- If the link is up/down
- IP type IPv4/IPv6

- IP address
- Subnet mask
- MAC address
- Maximum port speed

Software Management

The Software Management menu is used to manage settings for Email, SNMP settings and Web services. The Email function is used for sending notifications of events. The Web service is used for remote network connection to the WebPAM PROe management interface. This is also where you can export and import configuration script files and user database files.

Importing a Configuration Script

You can write a CLI configuration script to automatically configure your Vess subsystem. The script must be a plain, non-encrypted text file. From there, you can import the script from the Host PC and perform the configuration automatically.

Cautions

Do NOT attempt to write or modify a configuration script until you receive guidance from Technical Support.

Importing a configuration script overwrites the current settings on your Vess subsystem.

Or you can save the configuration from one Vess subsystem, export it, and then import it to automatically configure your other Vess subsystems. To import a configuration script:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click the **Import** tab in the Service Management menu.

4. Choose *Configuration Script* from the **Type** drop-down menu.

5. Click the **Choose File** button and select the configuration script on the Host PC. The file will be listed in the Local File Name row of the menu.

   The system verifies that the file is a valid configuration script and displays any errors or warnings.

6. Click the **Submit** button to continue.

7. In the **Confirmation** box, type the word "**confirm**" in the field provided and click the **Confirm** button.

   The configuration script is imported and applied automatically.

Exporting a Configuration Script

You can save the configuration from one Vess subsystem, export it, and then import it to automatically configure your other Vess subsystems.

To export a configuration script:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click the **Export** tab in the Service Management menu.

4. Choose *Configuration Script* from the **Type** drop-down menu.

5. Click the **Export** button.

6. Select a location on the Host PC for the downloaded file and save the file.

   The file is saved to your PC as "Configscript.txt".

> ⚠️ **Cautions**
>
> **Do NOT attempt to write or modify a configuration script until you receive guidance from Technical Support.**

Saving a Service Report

A Service Report is a detailed report covering the configuration and status of all components in your RAID system. A support technician or field engineer might request a service report for the purpose of diagnosis and troubleshooting.

To save a system configuration file:

1. Click on the Subsystem icon (IP address and device name) in Tree View to open the Subsystem Information display.

2. Click the **Save** button in the Save System Service Report row of the information display.

   Information for the report is gathered and compiled. This action takes up to a few minutes, depending on the size of your RAID system.

3. Determine where you want to store the file on the Host PC, then click the **Save** button in the pop-up menu.

   The report saves to your Host PC as a compressed HTML file.

4. Double-click the downloaded file to decompress it.

5. Double-click the report to open it in your default browser.

The Service Report includes the following topics:

- About – Report utility

- BBM Info – Bad Block Manager

- BGA Summary – Status and settings

- Buzzer Info

- Controller Info

- Disk Array Info

- Disk Array Dump info

- Disk Array Verbose Info

- Enclosure Info

- Error Table Info

- Event Info - NVRAM

- Event Info - Runtime

- LogDrive Info – Basic logical drive information

- LogDrive Dump Info – Diagnostic information

- Logical Drive Verbose Info – Full logical drive information

- Network Info – Virtual port

- Phydriv Info – Basic physical drive information

- Phydriv Verbose Info – Full physical drive

- SWMGT Info – Software management

- Service Setting – Email

- Service Setting – Webserver

- Spare Info – Basic spare drive information

- Spare Dump Info – Diagnostic information

- Spare Verbose Info – Full spare Drive information

- Statistic Info

- Subsystem info

- User Info

Email Service

Email service enables the RAID subsystem to send you Email messages about events and status changes. By default, Email service is set to Automatic.

Stop Email Service

To stop the Email service:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click on **Email** in the Service List of the Service Management menu.

4. Click the **Stop** button under *Service Status -- Email*.

5. Click the **Confirm** button.

To start the Email service after stopping it:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click on **Email** in the Service List of the Service Management menu.

4. Click the **Start** button under *Service Status -- Email*.

5. Click the **Confirm** button.

Restarting Email Service

To restart the Email service:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click on **Email** in the Service List of the Service Management menu.

4. Click the **Restart** button under *Service Status -- Email*.

5. Click the **Confirm** button.

Email Settings

To change Email service settings:

1. Click the **Administrative Tools** icon.

2. Click the **Software Management** icon.

3. Click on **Email** in the Service List of the Service Management menu.

4. Make settings changes as required:

    Under *Service Setting -- Email* choose a startup type:

    -   *Automatic* – (default) Starts and runs with the subsystem.

    -   *Manual* – You start the service when you need it.

    Under *Email Server Settings*

    -   SMTP Server IP address

    -   SMTP Authentication under *Email Server Settings*
        The Yes option enables authentication.
        The No option disables.

    -   SMTP Authentication under *Email Server Settings*
        Username – Required if SMTP authentication is enabled.
        SMTP Authentication Password – Required if SMTP authentication is enabled.

    Under *Email Content Customization*

    -   Email Sender (From) Address – The sender's name shown on notification messages.

    -   Email Subject – The subject line of the notification message.
5. Click the **Submit** button.
6. Click the **Confirm** button.

Sending A Test Email Message

After email settings are completed, you can send a test email.

To send a test email message, complete email settings as described above and check the *Send a test email* option box, then click the **Submit** button. A test email message is sent to the address you specified.

Performance Monitoring

The Performance Monitor displays real-time performance statistics for logical drives and physical drives. The vertical scale adjusts dynamically to accommodate the statistical data.

Because it reports performance in real-time, to see data in the monitor, there must be I/O data activity taking place between the subsystem and the Host.

To monitor performance:

1. Click the **Administrative Tools** icon.

2. Click the Performance Monitoring icon.

3. Click the Information tab for aggregated statistics; or choose the Read/Write tab to view specific Read and Write performances separately.

4. Under Logical Drive, choose the metric you want to see from the Measurement drop-down menu.

Information

- Bandwidth in MB/s
- Cache usage by %
- Dirty cache usage by %

5. Check the boxes for the logical drives you want to see.
   - Maximum latency in ms
     - Total of all logical drives
   - Average latency in ms
     - Up to 4 devices
   - Minimum latency in ms
   - I/Os per second

Read/Write

- Read bandwidth
- Write bandwidth
- Maximum Read latency in ms
- Maximum Write latency in ms
- Average Read latency in ms
- Average Write latency in ms
- Minimum Read latency in ms
- Minimum Write latency in ms

6. Under Physical Drive, choose the metric you want to see from the Measurement drop-down menu.

Information

- Bandwidth in MB/s

- Maximum latency in ms

- Average latency in ms

- Minimum latency in ms

- I/Os per second

7. Check the boxes for the physical drives you want to see.

- Total of all physical drives

- Up to 4 devices

- I/Os per second

Read/Write

- Read bandwidth

- Write bandwidth

- Maximum Read latency in ms

- Maximum Write latency in ms

- Average Read latency in ms

- Average Write latency in ms

- Minimum Read latency in ms

- Minimum Write latency in ms

Since the performance monitor is a real-time display, it does not accumulate information and there is no clear or save function.

To save performance statistics for analysis or troubleshooting, save a Service Report. See "Saving a Service Report".

Controllers

Click on a specific controller in Tree view to display information or statistics for a controller. Or to change controller settings. See the following sections:

- "View Controller Information"
- "Viewing Controller Statistics"
- "Controller Settings"

View Controller Information

To view controller information:

1. Click the **Controllers** icon.

2. Click the specific **Controller** icon of the controller for which you want to view information.

3. The Information tab will present basic controller information.

Controller information includes:

- Cache Usage
- Dirty Cache Usage
- Part Number
- Serial Number
- Hardware Revision
- WWN

- Install Package Version
- Install Package Build Date

1. Click the **Advanced Information** menu expander to view advanced information.

Advanced controller information includes:

- Memory Type
- Memory Size
- Flash Type
- Flash Size
- Preferred Cache Line Size
- Cache Line Size
- Coercion   *Enabled/Disabled**
- Coercion Method*
- SMART Log *Enabled/Disabled**
- SMART Polling Interval   *

- Write Back Cache Flush Interval*
- Enclosure Polling interval
- Host Cache Flushing   *Enabled/Disabled**
- Forced Read Ahead   *Enabled/Disabled**
- Spin Down Type
- HDD Power Levels*
- HDD Idle Time*
- HDD Standby Time*
- HDD Stopped Time*
- Physical Drive Temperature Threshold*
- Physical Drive Critical Temperature Threshold*

Items with an asterisk (*) are adjustable under Controller Settings.

Viewing Controller Statistics

To view controller statistics:

1. Click the **Controllers** icon.

2. Click the specific **Controller** icon of the controller for which you want to view statistics.

3. At the top of the Information display menu, between the Information and Settings tabs, click on the menu expander to reveal the Statistics link.

Reveal Statistics link
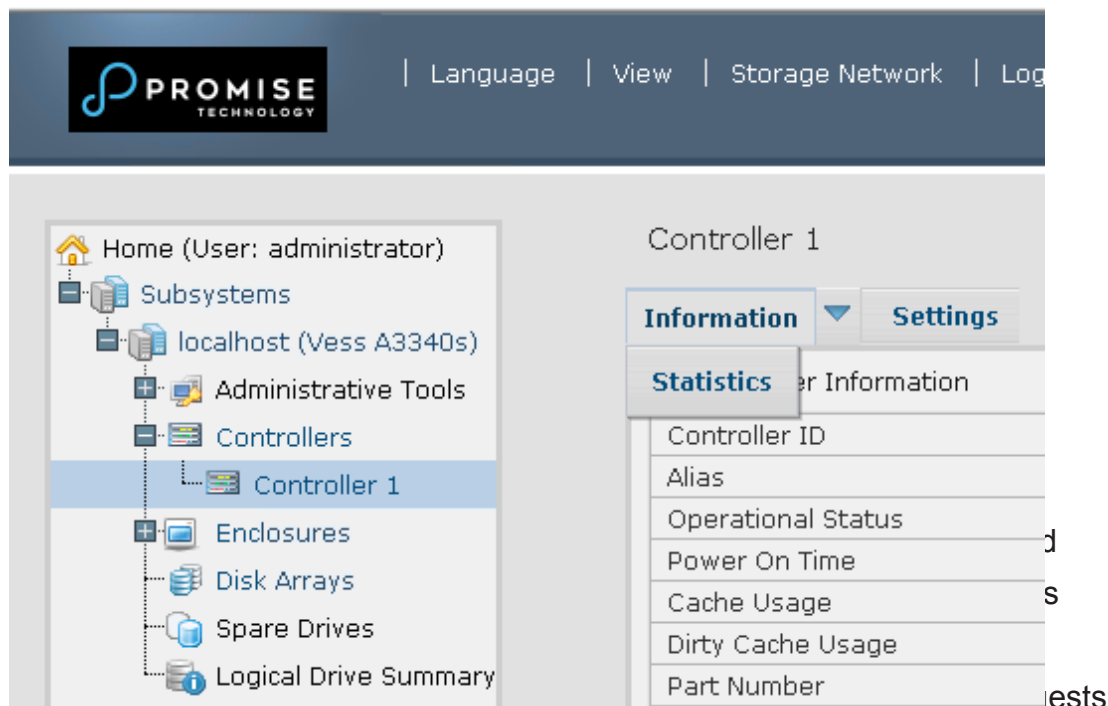
- • I/O Requests
- • Read IO Requests
- • Statistics Start Time
- • Write I/O Requests
- • Statistics Collection Time

Controller Settings

To make controller settings:

1. Click the **Controllers** icon.

2. Click the specific **Controller** icon of the controller you want to manage.

3. Click the **Settings** tab.

4. Make settings changes as required:

   • Enter, change or delete the alias in the **Alias** field.

   • **SMART Log** – Check the box to enable or uncheck to disable.

   • **SMART Polling Interval** – **Enter** a value into the field, 1 to 1440 minutes

   • **Coercion** – Check the box to enable or uncheck to disable.

   • **Coercion Method** – Choose a method from the drop-down menu:

             GBTruncate

             10GBTruncate

             GrpRounding

             TableRounding

   • **Write Back Cache Flush Interval** – **Enter** a value into the field, 1 to 12 seconds.

   • **HDD Power Saving** – Choose time periods from the drop-down menus.
     After an HDD has been idle for the set period of time:

             Power Saving Idle Time – Parks the read/write heads.

             Power Saving Standby Time – Lowers disk rotation speed.

             Power Saving Stopped Time – Spins down the disk (stops rotation).

   • **Host Cache Flushing** – Check the box to enable or uncheck to disable.

   • **Forced Read Ahead** (cache) – Check the box to enable or uncheck to disable.

   • Physical Drive Temperature Threshold - Type a temperature
     (50-55 ºC) to trigger an event notice and email alert.

   • Physical Drive Critical Temperature Threshold - Type a
     temperature (58-65 ºC) to trigger system shutdown.

5. Click the **Submit** button.

Enclosures

The Enclosure menus are used to provide information for and monitor the status about the various components of the enclosure unit. Click on a specific enclosure in Tree view or in the Enclosures list to display information or settings menus for an enclosure. See the following sections:

- "Enclosure Information"
- "Enclosure temperature sensor settings"
- "Buzzer Settings"
- "Physical Drives"

Locate an enclosure

To locate an enclosure in the list, click the Locate button. The LED indicators on the front panel of the enclosure will blink for one minute.

Enclosure Information

The Enclosure Information read-only display menu provides key real-time information about current hardware status of the enclosure. Click on the expanders buttons to reveal current conditions and status of the enclosure, power supplies, fans, blowers, temperature sensors and voltage sensors. Move the cursor over the icons in the virtual enclosure displayed at the top of the menu to see current status and relevant conditional statistics for the fans, power supplies, and temperature sensors.

Enclosure Information display

The temperature threshold settings are used to send event notices when the internal temperature reaches a high level. To set enclosure temperature thresholds, click on the enclosure in Tree View, then click on the **Settings** tab to view the Enclosure Settings menu. There are two thresholds to configure:

- *Controller Warning Temperature Threshold [90-95 C°]* — If the enclosure temperature reaches this threshold, a warning message is sent and an event is recorded in the event log.

- *Controller Critical Temperature Threshold [100-105 C°]* — If the enclosure temperature reaches this threshold, a warning message is sent, an event recorded is recorded in the event log.

Buzzer Settings

The audible enclosure alarm buzzer can be enabled or disabled.

To enable or disable the buzzer, click on the enclosure in Tree View, then click on the Buzzer menu expander, scroll to *Settings* and click the check **Enable Buzzer** option box. Click the **Subm**it button.

Physical Drives

The Physical Drives menus are used to view information and statistics about physical hard drives installed in the enclosure and to set Global Settings for hard drives. To see the Physical Drives List, expand the individual Enclosure icon in Tree View to see the Physical Drives icon for the enclosure. To display the information for any populated slot, you can expand the Physical Drives icon in Tree View to reveal links to each slot, or click on the slot in the Physical Drives List, or click on the populated slot in the virtual enclosure displayed in the menu.

View individual physical drive information

Physical Drive Information	
Physical Drive ID	1
Location	Enclosure 1 Slot 1
Alias	
Physical Capacity	1.82TB
Configurable Capacity	1.82TB
Used Capacity	1.82TB
Block Size	512 Bytes
Operational Status	OK
Configuration Status	Array0 SeqNo0
Model	Hitachi HUA723020ALA640
Drive Interface	SATA 6Gb/s
Serial Number	MK0171YFHPS9BA
Firmware Version	MK7OAA10
Protocol Version	ATA/ATAPI-8
Visible To	Controller 1

The information listed for individual physical drives includes:

Physical Drive Information

- Physical Drive ID
- Location [Enclosure # Slot #]
- Alias
- Physical Capacity
- Configurable Capacity
- Used Capacity
- Block Size [Bytes]
- Operational Status

- Configuration Status
- Model
- Drive Interface
- Serial Number
- Firmware Version
- Protocol Version
- Visible To [Controller #]

Advanced Physical Drive Information

- Write Cache [*Enabled/Disabled*]
- Read Look Ahead Cache [*Enabled/Disabled*]
- SMART Feature Set
- SMART Self Test
- SMART Error Logging
- Command Queuing Support

- Command Queuing [*Enabled/Disabled*]
- Queue Depth
- Maximum Multiple DMA Mode Supported
- Maximum Ultra DMA Mode Supported
- DMA Mode
- Drive Temperature [C°/F°]
- Reference Drive Temperature
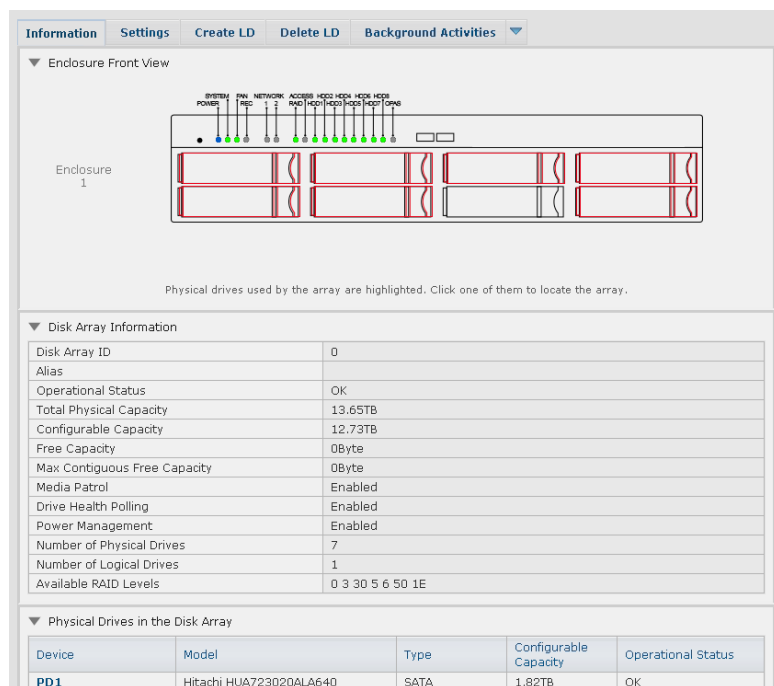- Power Saving Mode

Disk Arrays and Logical Drives

Disk arrays and logical drives are created and managed using the **Disk Arrays** menu. Use the Array Configuration menu to view the Disk Array List, and to create and delete disk arrays on the enclosure. Expand the Disk Arrays icon in Tree View to view menu links for existing arrays. Each array icon can be expanded again to see the Logical Drives icon, and this can be expanded to see each logical drive icon.

For a detailed description of how to create disk arrays and logical drives using WebPAM PROe, please refer to the Quick Start Guide.

Use the top-level Disk Arrays menu to view the **Disk Array List**, to delete existing arrays, and to create new disk arrays using the Automatic, Express, or Advanced disk array creation menus. Note that there must be physical drives available in order to use any of the disk array creation menus.

View information for existing disk arrays by clicking on the icon in Tree View or the array name in the Disk Array List. Each individual array menu is used to create and delete logical drives, to change settings (Alias and enable/disable PDM, Media Patrol and Power Management) for the array, or to start Background Activities including PDM, Rebuild and Transition.

Individual Disk Array menu

Information	Settings	Create LD	Delete LD	Background Activities ▼

▼ Enclosure Front View

Enclosure 1

Physical drives used by the array are highlighted. Click one of them to locate the array.

▼ Disk Array Information

Disk Array ID	0
Alias	
Operational Status	OK
Total Physical Capacity	13.65TB
Configurable Capacity	12.73TB
Free Capacity	0Byte
Max Contiguous Free Capacity	0Byte
Media Patrol	Enabled
Drive Health Polling	Enabled
Power Management	Enabled
Number of Physical Drives	7
Number of Logical Drives	1
Available RAID Levels	0 3 30 5 6 50 1E

▼ Physical Drives in the Disk Array

Device	Model	Type	Configurable Capacity	Operational Status
PD1	Hitachi HUA723020ALA640	SATA	1.82TB	OK

Information in the Disk Array menu includes:

- Disk Array ID [#]
- Alias
- Operational Status (see below)
- Total Physical Capacity
- Configurable Capacity
- Free Capacity [Bytes]
- Max Contiguous Free Capacity [Bytes]

- Media Patrol [*Enabled/Disabled*]
- PDM　　[*Enabled/Disabled*]
- Power Management [*Enabled/Disabled*]
- Number of Physical Drives
- Number of Logical Drives
- Available RAID Levels

Other lists in this menu:

- Physical Drives in the Disk Array
- Logical Drives in the Disk Array
- Available Spare Drives to the Disk Array

Disk Array Operational Status

OK – This is the normal state of a logical drive. When a logical drive is Functional, it is ready for immediate use. For RAID Levels other than RAID 0, the logical drive has full redundancy.

Synchronizing – This condition is temporary. Synchronizing is a maintenance function that verifies the integrity of data and redundancy in the logical drive. When a logical drive is Synchronizing, it will function and your data is available. However, access will be slower due to the synchronizing operation.

Critical / Degraded – This condition arises as the result of a physical drive failure. A degraded logical drive will still function and your data is still available. However, the logical drive has lost redundancy (fault tolerance). You must determine the cause of the problem and correct it.

Rebuilding – This condition is temporary. When a physical drive has been replaced, the logical drive automatically begins rebuilding in order to restore redundancy (fault tolerance). When a logical drive is rebuilding, it will function and your data is available. However, access will be slower due to the rebuilding operation.

Logical drive management

Logical drives are made from disk arrays. In the Tree, you can see a graphic representation of the logical drives that belong to each array. The Logical Drive List can be accessed in Tree View by expanding the under Disk Arrays and clicking on the Logical Drives icon for any existing disk array, or simply click on the **Logical Drive Summary** icon for the Subsystem.

Click on any Logical Drive (LD) in the list to view Information and Statistics, to change Settings (Alias, Read Policy,Write Policy), to start Background Activities (Initialization, Redundancy Check), or to view the Check Table for the LD.

Information displayed in the menu includes:

- Logical Drive ID
- Alias
- Raid Level
- Operational Status
- Capacity
- Physical Capacity
- Number of Axles [#]
- Number of Used Physical Drives [#]
- Stripe Size
- Sector Size [Bytes]
- Disk Array ID

- Read Policy
- Write Policy
- Current Write Policy
- Serial Number
- WWN
- Synchronized [Yes/No]
- Tolerable Number of Dead Drives Per Axle
- Parity Pace
- Codec Scheme

Spare Drives

When a physical drive in a disk array fails and a spare drive of the same type and adequate capacity is available, the disk array will begin to rebuild automatically using the spare drive.

In Tree View, click on the Spar Drive icon to see the Spare Drives List, or to create or delete an existing spare drive. Click on any spare drive in the list to information about the drive. Spare Drive Information includes:

- Spare Drive ID

- Operational Status

- Physical Drive ID

- Capacity

- Revertible [*Yes/No*]

- Type

- Dedicated to Disk Arrays

Running Spare Check

A Spare Check verifies the operational status of your spare drives. You can also schedule a Spare Check.

To check a spare drive:

1. Click the Spare Drives icon.

2. Click the Spare Check tab.

3. From the Physical Drive drop-down menu, choose the spare drive you want to check. Or choose All to check all the spare drives at the same time.

4. Click the **Submit** button.

The results of the Spare Check appear under Spare Check Status in the Information tab. "Healthy" means normal condition.

Logical Drive Summary

The Logical Drive Summary displays a list of all logical drives in the Subsystem. This list does not arrange the logical drives under the disk array to which they belong nor under the enclosure in which they are located. The menu functions in the same way as the Logical Drives menu discussed in "Logical drive management" on page 136

MANAGING WITH THE CLI

- Opening the CLI on Windows (below)

- Table of Supported Commands

- Notes and Conventions

- List of Supported Commands

The Command Line Interface (CLI) provides rapid setup of disk arrays and logical drives. You can also manage your system using the CLI. However, ongoing management is much easier with the CLU or WebPAM PROe.

> **Important**
>
> DO NOT move any files from or copy any files to the PromiseApp folder on the C Drive [C:\PromiseApp] in the Windows OS.

Opening the CLI on Windows

To open the CLI, click the CLI icon on the desktop or:

1. Go to **Start > Run** and click the **Browse** button.

2. Navigate to the **C:\PromiseApp\clitest** folder.

3. Click **clitest.exe** file then click the Open button.

4. Click the **OK** button in the **Run** dialog box.

The CLI window opens.

Use the default user name, **administrator**, and default password, **password**, to login.

Table of Supported Commands

Command	Action
about	View utility information.
array	View or edit array information. Create, edit, or delete logical drives in an existing array. To physically locate an array in an enclosure. Accept an incomplete array condition.
bbm	View or clear the BBM defect list of the specified configured physical drive.
bga	View status of all current background activities. Enable or disable relevant background activities. Modify the background task rate for each of the background tasks.
buzz	View buzzer status, enable/disable and turn on/off buzzer.
checktable	View logical drive error tables.
config	For express or automatic configuration. For advanced configuration please see the 'array' command.
ctrl	View or edit controller information and settings.
enclosure	View or edit enclosure and SEP information and settings. Locate an enclosure via LEDs.
event	View or clear events logs.
export	Subsystems only. Export files to remote tftp host.
factorydefaults	Restore settings to factory defaults.
import	Import files from remote tftp host
init	View logical drive initialization status and progress. Start, stop, pause, or resume an initialization or a quick initialization.
logdrv	View or edit logical drive information and settings. Locate a logical drive via LEDs.
logout	Logout session for the current user.
menu	Enter menu driven Command Line Utility.
Note: Commands are NOT case sensitive.	

Table of Supported Commands (Continued)

Command	Action
mp	View media patrol status and progress. Start, stop, pause, or resume media patrol.
net	View or edit ethernet network information and settings.
password	Modify a user's password.
pdm	View PDM status and progress. Start, stop, pause, or resume PDM process.
phydrv	View or edit physical drive information and settings. Locate a physical drive via LEDs.
rc	View redundancy check status and progress. Start, stop, pause or resume redundancy check.
rb	View rebuild status and progress. Start, stop, pause, or resume a rebuild process.
sc	View spare check status. Start spare check.
spare	Create or modify hot spare drives.
spath	Discover and change subsystem path.
stats	View or reset statistics.
subsys	View or edit subsystem information and settings.
swmgt	View, start or stop software component.
sync	View logical drive synchronization status and progress.
transit	View transition status and progress. Start, stop, pause, or resume a transition process.
user	List, modify, create and delete user accounts on subsystem.
help	When used alone will display this menu. When used in conjunction with a command (example: help array) it will display help information for that particular command.
?	This can be used in place of the help command or optionally can be used as a switch for a command (example: array -?) to provide command usage.
Note: Commands are NOT case sensitive.	

Notes and Conventions

Commands and options are NOT case sensitive.

Not all extended keys are supported. However, you can use the backspace and the left and right arrow keys for command line editing. In addition, the up and down arrow keys allow scrolling through the command history buffer.

If you need context-sensitive help, type one of the following commands:

- <command> -h

- <command> -?

- help <command>

That action will display full context-sensitive help for the specific command. Each command when used alone, such as "array" will display a summary of relevant information. If more information is desired, the -v verbose mode can be used. This will provide information for all relevant aspects of that command.

Usage terminology is as follows:

- [square braces] depict an optional switch

- <arrow braces> depict user input

- Type " | more" at the end of each command, to display info page by page

about

Usage

about

Summary

Displays utility information.

array

Usage

array [-a <action>] [-d <DaId>] [-c <array count>] [-v] array -a add [-s "<list of array params>"] [-d <DaId>] -p <PdId list> [-c <Ld count>] [-l "<list of Ld params>"] array -a mod -d <DaId> [-s "<list of array settings>"]

array -a del -d <DaId list>

array -a locate -d <DaId>

array -a accept -d <DaId> [-t <condition type>]

array -a addld -d <DaId> [-c <Ld count>] -l "<list of ld settings>"

array -a delld -l <LdId list>

Summary

The array command is the main command for performing advanced configuration and maintenance tasks on disk arrays.

This command lists, creates, modifies, deletes, and locates disk arrays. It also adds and deletes logical drives.

Note that you cannot mix Hard Disk Drives (HDD) and Solid State Drives (SSD) in the same disk array.

Options

-a <action>   Specifies the action to perform.

list   (Default) Displays a summary of all arrays, a specified number of arrays, or a specific
   array.

add   Adds/creates an array. This action might also create logical drives at the same time.

addld   Adds/creates a logical drive to an existing array.

delld   Deletes a logical drive from an array.

mod   Modifies array settings.

del   Deletes an array and all its associated logical drives.

locate   Locates an array.

accept   Accepts the condition of an incomplete array. The condition that can cause an array
   to be incomplete is:

   • Missing Drive: one or more drives missing in the array
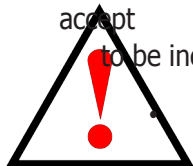
> ⚠️ **Warning**
>
> **When you delete a disk array, you also delete any logical drives that belong to it, along with the data they contain.**
>
> **When you initialize a logical drive, you delete all data on the logical drive.**
>
> **Back up any important data before deleting a disk array or logical drive.**

> ✔️ Important
>
> A logical drive cannot be expanded once it has been created. To add capacity, you can either add another logical drive, or, delete the existing logical drive and create a larger one.

-p <PD ID list>   Specifies physical drives to be used in an array, with -a add option. PD IDs are specified individually or separated by comma. Sequential group of physical drives are specified by placing a ~ between numbers such as 1~6. This will include physical drives 1, 2, 3, 4, 5, and 6.

-s "<option>=<value>   Specifies array settings when creating (add) or modifying (mod) an array. Options are comma separated.

alias= A user-specified array name. Up to 32 characters, alpha-numeric characters, blank spaces and underscores. Beginning and ending blank spaces are discarded.

mediapatrol= Enables or disables Media Patrol for this array.

enable	The default is enable.
disable	

pdm=   Enables or disables PDM for this array.

enable	The default is enable.
disable	

-l "<option>=<value>"   Specifies logical drive settings when adding a logical drive to an existing array (addld) or during array creation (add). **Options** are comma separated.

<LD ID list>   Specifies a list of Logical Drive IDs. Requires the -a delld option.

ID=   Assigns a specific ID to an array. Overrides automatic ID assignment. Valid values are 0-255.

Alias=   A user-specified name for the logical drive. Raid=   Specifies logical drive RAID level.

0	Striping.
1	Mirroring on two drives.
5	Parity, requiring 3 or more drives.
10	Mirroring on even number of drives.
1e	Extended mirroring, requiring 2 or more drives.
50	Striping on multiple RAID 5, requiring 6 or more drives.
6	Allow two drive failure, requiring 4 or more drives.
60	Striping on multiple RAID 6, requiring 8 or more drives.

Capacity=   Specifies logical drive capacity. Can be specified in megabytes (mb), gigabytes (gb) or terabytes (tb), up to 2 decimal places. If not specified, all available capacity is used for this logical drive.

Stripe=   Specifies logical drive stripe size. Options include 64KB,128 KB, 256 KB, 512 KB, and 1024 KB. If not specified, the default 64KB is used.

Sector=   Specifies logical drive sector size. Options include 512 B, 1 KB, 2 KB, and 4 KB. Sector size cannot exceed Stripe size. Auto-adjusted not to exceed the maximum supported sector size of the controller. If not specified, the default 512 B is used.

WritePolicy=   Specifies logical drive write policy.

        writethru   Writes are not cached

        writeback   Writes are cached

ReadPolicy=   Specifies logical drive read policy.

        readahead   Reads extra data to help reduce read times of sequential data.

        readcache   Caches reads the data in case the same request is made again.

        nocacheNo caching algorithm.

Axle=   A member element when creating a RAID10 or RAID50 or RAID60.
RAID10 have 2 axles, RAID50 and RAID60 may have up to 16 axles with up to 16 drives per axle.

PreferredCtrlId=   Subsystems only. Specifies which controller the LD is preferred for LUN affinity. Valid value is 1 or 2. If value is not specified, LUN affinity is auto balanced.

-c <array count>   Specifies the number of arrays to give a summary of when used with the -a list option. For example 'array -a list -c3' will give a summary for the first 3 arrays on that controller.

<Ld count>   Specifies the number of logical drives to be created with the -a add option. With the -c option, all the logical drives have same settings but only one -l option=value can be specified.

-t <condition type> Specifies the type of incomplete condition to accept. If not specified, it will accept the current incomplete condition by default.

missingdrive   The condition of missing drive in the array.

-v Verbose mode. Displays all array properties, requires -a list option.

Examples

array -v -c 1

array -a add -s "alias=MyArray,mediapatrol=enable" -p 1,3,5~9

    -l "raid=5,capacity=50gb,stripe=256kb,sector=1kb"

array -a add -p 1,3,5~9 -l "raid=5,capacity=50gb,stripe=256kb"

array -a mod -d 1 -s "alias=YourArray,mediapatrol=disable"

array -a del -d 3

array -a locate -d 0

array -a addld -d 0 -l "raid=1e,capacity=125gb,stripe=64kb"

array -a delld -l 1

bbm

Usage

bbm [-a <action>] [-p <PdId>]

bbm -a clear -p <PdId>

Summary

The bbm command displays and clears the Bad Block Map (BBM) for all configured SATA drives.

Options

-a <action>　　　　Specifies the action to perform.

list　　　(Default) List the BBM information.

clear　　　Clears the BBM list. For configured SATA drives only.

-p <PdId> Specifies the physical drive id. For the -a list option, the default is all physical drives. For the -a clear option, you must specify a physical drive id.

Examples

bbm -p 1

bbm -a clear -p 3

bga

Usage

bga [-a <action>]

bga -a mod -s "<list of settings>"

Summary

The bga command displays all current background activities and makes settings each background activity.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Lists current background activities.

        mod   Makes changes to one of the settings.

-s "<option>=<value>"

        Specifies which background activity settings to change.

autorebuild=   Enable or disables auto-rebuild and auto-transition.

    Auto-rebuild will rebuild an array when an unconfigured drive is inserted into the slot of a dead drive.

    Auto-transition will start transitioning on a used revertible spare in the following condition:

1. When the rebuild has completed using the revertible spare, and

2. When an unconfigured drive is inserted into the slot of the dead drive which the was part of the array.

When a non-revertible spare has been inserted or created, and is applicable to the array. This option affects all arrays on the subsystem.

> enable

> disable

mediapatrol=   Verifies the media of the array and/or spares to find bad blocks on physical disks before you use that block. This feature is enabled and disabled on an array basis.

> enable

> disable

ReassignedBlock=   (1-512) Threshold value to trigger PDM, when re-assign map exceeds the threshold value.

ErrorBlock=   (1-2048) Threshold value to trigger PDM, when number of medium error on the PD exceeds the threshold value.

<bg task>=<rate> Background task rates determine what percentage of the IO load on the controller should be dedicated to the background task. A lower number will mean the task takes longer to complete, a higher number will cause the task to complete faster, all other things being equal.

rebuildrate=   Rebuild rate determines the rate at which rebuild will run.
               (low=25, medium=50, high=75)

> low

> medium

> high

pdmrate=   PDM rate determines the rate at which PDM will run.
                    (low=25, medium=50, high=75)

      low

      medium

      high

transitionrate=   Transition rate determines the rate at which transition will run.
                    (low=25, medium=50, high=75)

      low

      medium

      high

syncrate=   Synchronization rate determines the rate at which synchronization will run.
    (low=25, medium=50, high=75)

      low

      medium

      high

initrate=   Initialization rate determines the rate at which initialization will run.
    (low=25, medium=50, high=75)

      low

      medium

      high

rcrate=   Redundancy check rate determines the rate at which redundancy check will run.
    (low=25, medium=50, high=75)

      low

      medium

      high

Examples

bga

bga -a mod -s "autorebuild=enable,rebuildrate=high,syncrate=low"

buzz

Usage

buzz [-a <action>]

buzz -a list

buzz -a enable

buzz -a disable

buzz -a on

buzz -a off

Summary

The buzz command displays the status of the buzzer, and enables, disables, turns on or turns off the buzzer.

Options

-a <action>   Specifies the action to perform.

          list   (Default) List the status of the buzzer.

          enable   Enable the buzzer.

          disable   Disable the buzzer.

          on   Turn on the buzzer.

          off   Turn off the buzzer.

checktable

Usage

checktable [-t <tableType>] -l <LdId>

Summary

The checktable command displays the error check tables of a logical drive.

Options

-t <tableType>   Specifies which error table to display. The default displays all tables.

          rct   Displays the read check table.

          wct   Displays the write check table.

          ibt   Displays the inconsistent block table.

-l <LdId>   Specifies the logical drive ID.

Examples

checktable -l 10 -t rct

checktable -l 10

config

Usage

config -a auto

config -a expr [-r y|n] [-c y|n] [-p y|n] [-m y|n] [-s y|n] [-t <AppType>] [-l <NumLd>]

Summary

The config command has two options: Automatic and Express.

Automatic configuration takes all available unconfigured physical drives to create an optimized disk array following a default set of parameters. There are no options.

Express configuration takes your input, creates one or two arrays, and spreads their capacity evenly over all of the logical drives that you specify.

The redundancy option creates redundant logical drives (RAID 1, 10, 1E, 5, 50, 6, or 60).

The capacity option enables optimizes the logical drives for capacity. The performance option optimizes the logical drives for performance.

If you choose all three options, redundancy gets highest priority and capacity gets lowest priority.

Note that you cannot combine HDDs and SSDs in the same disk array. If your system has both type of drives, it will create separate disk array/logical drive sets for each type of physical drive.

Options

-a <action>   Specifies the action to perform.

        auto   Automatic configuration with no options. Creates an optimized disk array. One or more logical drives are created automatically.

        expr   Express configuration. RAID level is dependant on the options chosen.

-r <y|n>   Selects the redundancy option.

-p <y|n>   Selects the performance option.

-c <y|n>   Selects the capacity option.

-s <y|n>   Includes a spare drive in the array.

Note: Requires 5 or more unconfigured physical drives.

-t <AppType>   Specifies the intended application for this array.

      video   Sequential large block reads.

      data   Random read/write mix, small to medium sized IO.

      log   Sequential small block write.

      other   Random read/write mix, small to medium sized IO.

      fileserver   Random read/write mix, small to medium sized IO.

-l <num of LDs>   Specifies how many logical drives to include in the configuration. Array capacity is divided evenly among the logical drives.

Examples

config -a auto

config -a expr -ry -p y -c n -sy -t data -l2

ctrl

Usage

ctrl [-a <action>] [-i <ctrlId>] [-c <ctrl count>] [-v]

ctrl -a mod [-i <ctrlId>] -s "<list of settings>"

ctrl -a clear [-i <ctrlId>] [-t <condition type>]

Summary

The ctrl command displays controller information and changes controller settings.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Lists controller information.

        mod   Changes controller settings.

        clear   Clears controller conditions.

-i <ctrl ID> Specifies the controller ID.

-c <ctrl count>   Controller count. Required for information on multiple controllers.

-s "<option>=<value>" Specifies which settings to change.

        alias=   A user-specified name for the controller.

        Up to 48 characters long, alpha- numeric characters, blank spaces and underscores
The beginning and ending blank spaces are discarded.

coercion=   Enables or disables disk coercion. Disk coercion will truncate the size of the physical drives. Makes different size drives appear to be the same size. For example, a 90.1 GB drive would appear as the same size as an 89.8 GB drive. Important when using drives of different manufacturers for rebuilds or as hot spares.

        enable

        disable

coercionmethod=   The method of coercion.

        GBTruncate   Truncates the drive to the nearest 1-billion byte boundary.

| | 10GBTruncate | Truncates the drive to the nearest 10-billion byte boundary. |

| | GrpRounding | Truncates the drive using an intelligent algorithm. Allows the maximum amount of usable space. |

| | TableRounding | Truncates the drive using a pre-defined coercion table. |

smart=   Enables or disables polling drive SMART status.

     enable

     disable

smartpollinginterval=   (1 - 1440) Sets the time interval in number of minutes to poll the drive SMART status.

cacheflushinterval= (1-12) Sets the time interval in seconds to flush the controller writeback cache.

     ddf   Uses the DDF area on the physical drives of the disk array.

     nvram   Uses the NVRAM on the controller.

     enable

     disable

pollinterval=   Sets interval in seconds to poll enclosure SEP information.

adaptivewbcache= Enables or disables adaptive writeback cache.

     enable   Writeback logical drives will change the write policy based on the availability of protection. If BBU or UPS is available, the write policy is retained as Writeback, otherwise the policy is switched to Writethru.

disable   The write policy of the writeback logical drives are not changed irrespective of the availability of BBU or UPS.

hostcacheflushing= Subsystems only. To enable or disable host cache flushing.

For high availability products only.

enable

disable

forcedreadahead= Enables or disables forced read ahead caching.

enable

disable

commonwwnn=   Enables or disables common WWNN. For high availability products only.

enable   All controllers report one common WWNN.

disable   Each controller reports its own WWNN.

alua=   Subsystems only. Enables or disables asymmetric logical unit access. Enabling ALUA will enable LUN affinity automatically.

enable

disable

-t <condition type> Specifies the type of condition to clear.

Valid only when the command action is "clear".

-l   Displays the id of the controller on whose serial port the CLI is running.

-v Verbose mode. Used with the -a list option.

Examples

ctrl

ctrl -v

ctrl -l

ctrl -a mod -i 1 -s "alias=ctrl1, coercion=enable"

enclosure

Usage

enclosure [-a <action>] -v

enclosure -a mod [-e <encl id>] -s <list of settings>

enclosure -a locate [-e <encl id>] [-t <FRU type> -f <FRU id>]

Summary

The enclosure command provides status and information about the various components of the enclosure unit. It is also sets temperature threshold values for JBOD enclosures and displays Vendor Provided Data (VPD).

-f <FRU id>　　　　Specifies id of FRU to locate. Requires -a locate option. Valid values are 1 and 2.

-v　　　　Verbose mode. Requires -a list option. VPD information is displayed.

Examples

enclosure

enclosure -v

enclosure -a mod -e 10 -s "tempwarning=35, tempcritical=45"

event

Usage

event [-a <action>] [-l <location>] [-i <SeqNo>] [-c <event count>] [-v]

event -a clear [-l <location>]

Summary

The event command displays and clears the RAM and NVRAM event logs.

Options

-a <action>   Specified the action to perform.

        list   Displays the events for the specified location. RAM events are displayed if no location is specified.

        clear   Clear events for a specified location.

-l <location>   Specifies the location from which to display or clear events.

        ram   All events are stored in RAM. These events are lost after rebooting.

        nvram   Some events are also stored in NVRAM. These events remain after rebooting and are a subset of the RAM events.

-i <sequence ID>   Specifies a specific event by its sequence number. This is a starting point. Requires the -a list option. You can use the -c option.

-c <event count>   Specifies the number of events to retrieve when displaying events.

-v   Verbose mode. Requires the -a list option.

Examples

event

event -v

event -l nvram

event -a clear -lnvram

event -c 200

event -a list -i852 -c200

Options

-a \<action\>   Specifies the action to perform.

        list   (Default) Displays information and status of the enclosure.

        mod   Modifies settings. Requires the -s option.

        locate   Locates an enclosure by flashing its LEDs.

-e \<encl id\>   Enclosure ID. The default value is 1 if unspecified.

        For list action, the default is for all enclosures if unspecified.

-s "\<option\>=\<value\>" Specifies the settings to change. Applies to the JBOD enclosures only.

tempwarning=   (25-45) Enclosure warning theshold temperature, in degrees Celsius.

tempcritical=   (30-51) Enclosure critical theshold temperature, in degrees Celsius.

ctrltempwarning= (90-95) Controller warning theshold temperature, in degrees Celsius.

ctrltempcritical= (100-105) Controller critical threshold temperature, in degrees Celsius.

-t \<FRU type\>   Specifies which type of FRU to locate. Requires -a locate option.

        ctrl   Locates the controller.

        cooling Locates the cooling unit.

export

Usage

export -t <fileType> [-s <tftpServer>] [-p <port>] -f <fileName>

Summary

The export command exports certain types of configuration files to a remote or local host.

This command only affects subsystems.

Options

-t <file type>   Specifies the type of file to export.

         userdb   User database file. This file type is not applicable for in-band and can only be exported to a remote host.

        servicereport   System service report file. This file is exported to remote host for embedded and local host for in-band.

-f <file name>   Specifies the name of the file to be exported.

-s <TFTP server>   Specifies TFTP server's IP or host name. Do not specify TFTP server for in-band.

-p <port num>   The port number of the TFTP server. Default is 69. Do not specify port number for in-band.

Examples

export -t userdb -s 192.168.1.1 -f userdb.bin

export -t servicereport -s 192.168.1.1 -f servicereport # for embedded

export -t servicereport -f servicereport # for in-band

factorydefaults

Usage

factorydefaults -a <action> -t <type>

Summary

The factorydefaults command restores factory default settings.

Options

-a <action>   Specifies the action to perform.

    restore   Restore the factory default settings.

-t <type> Specifies the type of settings to restore.

        all   All settings.

        allfw   All firmware settings.

        allsw   Subsystems only. All software settings.

Following are individual Firmware settings:

        bga   Background activity settings.

        ctrl   Controller settings.

        encl   Enclosure settings, including temperature thresholds.

        netiscsi   Subsystems only. Network settings of iSCSI ports.

        netmgmt   Subsystems only. Network settings of management ports.

        phydrv   Physical drive settings.

        subsys   Subsystem settings.

Following are individual Software settings, which only apply to Subsystems:

bgascheduler   Background activity scheduler settings.

service   Service startup type settings.

webserver   Web server settings.

snmp   SNMP settings. (Linux only)

telnet   Telnet settings. (Linux only)

email   Email settings.

user   User settings.

Examples

factorydefaults -a restore -t phydrv

factorydefaults -a restore -t all

import

Usage

import -t <file type> -s <TFTP server> -f <file name> -p <port num> -i

Summary

The import command is used to import files from a remoter TFTP host.

Options

-t <file type>

   userdb   User database file.

   configscript Configuration script.

-s <TFTP server> Specifies tftp server's IP or host name.

 -f <file name>   Specifies the name of the file to import.

-p <port num>   The port number of the TFTP server. Default is 69.

-i   Get format validation information about imported file only. File is not really applied to subsystem yet.

init

Usage

init [-a <action>] [-l <LdId>]

init -a start -l <LdId> [-q <size>] [-p <pattern>]

init -a stop -l <LdId>

init -a pause -l <LdId>

init -a resume -l <LdId>

Summary

The init command starts, stops, pauses, and resumes a logical drive initialization. A full initialization writes to the entire logical drive space and takes several minutes, depending on the size of the logical drive.

A quick initialization writes to the first and last few megabytes of the logical drive. Typically, a quick initialization is completed in moments.

> ⚠️ **Warning**
>
> **When you initialize a logical drive, you delete all data on the logical drive. Backup any important data before you initialize a logical drive!**

Options

-a <action>   Specifies the action to perform.

    list   Displays a list of the initialization processes in progress or paused and their status. The default action.

    start   Start an initialization.

    stop   Stop an initialization.

    pause   Pause an initialization.

    resume   Resume an initialization.

-l <LD ID>   Specifies the logical drive to be initialized.

-q <size>   (1-1024) Specifies the amount of data in megabytes (MB) for a quick initialization.

-p <pattern>   Specifies the pattern for a full initialization. The pattern can range from 1 to 128 bytes (HEX string), and is padded to even number of bytes, such as, fff padded to 0fff.

    Pattern is not supported for quick initialization.

Examples

init

init -a stop -l0

init -a start -l0 -p5a5a0101

logdrv

Usage

logdrv [-a <action>] [-l <LdId>] [-c <Ld count>] [-v]

logdrv -a locate -l <LdID>

logdrv -a mod -l <LdId> -s "<list of ld settings>"

Summary

The logdrv command displays information about the logical drives and changes logical drive settings.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Displays a summary of one or more logical drives.

        mod   Changes logical drive settings.

        locate Locates a logical drive within the enclosure by flashing drive carrier LEDs.

-l [<LD ID>]   Logical drive ID.

-c [<LD count>]   Logical drive count. Requires the -a list option.

-s ["<option>=<value>"]

        Specifies the logical drive settings to change.

        alias=   A user-specified name for the logical drive. Up to 32 characters, containing alpha-numeric characters, blank spaces and underscores. Beginning and ending blank spaces are discarded.

WritePolicy=   Specifies logical drive write policy.

        writethru   Writes are not cached.

        writeback   Writes are cached. Note: Cannot be set if ReadPolicy is set to "nocache."

ReadPolicy=   Specifies logical drive read policy.

        readahead   Reads extra data to help reduce read times of sequential data.

        readcache   Caches reads in the case the same request is made again.

        nocache   No caching algorithm.

    PreferredCtrlId=Specifies which controller the LD is prefers for LUN affinity. Valid value is 1 or 2.

-v   Verbose mode. Used with -a list.

Examples

logdrv

logdrv -v

logdrv -a mod -l0 -s "readpolicy=readahead"

logdrv -a locate -l2

logout

Usage

logout

Summary

The logout command is used to logout the current user from the session.

Examples

logout

menu

Usage

menu

Summary

Use this to switch the user interface to CLU mode.

mp

Usage

mp -a <action>

Summary

The mp command activates Media Patrol. Media Patrol searches the physical drives for media errors. When an error is found, Media Patrol attempts to repair the error. If it fails to correct the error, Media Patrol attempts to remap the sector. Note: Sector remapping is not currently supported.

You can start, stop, pause, or resume Media Patrol and monitor its progress and status.

Options

-a <action>　　　Specifies the action to perform.

　　　　　list　　(Default) Displays the status and progress of Media Patrol.

　　　　　start　Starts Media Patrol.

　　　　　stop　　Stops Media Patrol.

　　　　　pause　Pauses Media Patrol.

　　　　　resume　Resumes a paused Media Patrol.

Examples

mp

mp -a stop

mp -a resume

net

Usage

net [-a <action>] [-p <PortId>] [-v]

Summary

Net is used to display the TCP/IP specific information for the Ethernet ports.

Information such as IP addresses and subnetmask can be displayed.

Options

-a <action>   Which action to perform.

list   (Default) Displays a list of IP configurations for all or the specified ports.

-p <port ID>   To specify which Ethernet port to view or change settings.

1   Port 1

2   Port 2

3   Port 3

4   Port 4

-v   Verbose mode. Used with -a list.

Examples

net   *shows a list of ip info for all network ports*

Type " | more" at the end of each command, to display info page by page.

password

Usage

password -u <username>

Summary

The password command is used to modify a user password.

Options

-u <username>

Examples

password

old password:******

new password:******

new password:******

pdm

Usage

pdm [-a <action>] [-d <DaId>] [-s <SeqNo>]

pdm -a start -d <DaId> -s <SeqNo> -p <PdId>

pdm -a stop -d <DaId> -s <SeqNo>

pdm -a pause -d <DaId> -s <SeqNo>

pdm -a resume -d <DaId> -s <SeqNo>

Summary

The pdm command activates Predictive Data Migration (PDM). PDM replaces a suspect physical drive, such as a drive with a PFA condition, with a different drive. The replacement drive can be an unconfigured drive, a global spare, or a dedicated spare to this disk array.

During PDM, the data on the suspect drive is transferred to the replacement drive while the logical drive remains online.

After PDM, the replacement drive becomes part of the disk array. The suspect drive become unconfigured and any PFA condition remains on it.

This command starts, stops, pauses, and resumes a PDM and monitors the progress of a running PDM.

A PFA drive cannot be used until you clear the PFA condition. To clear the PFA conditon of a physical drive, please refer to **phydrv** command. Note that the destination drive must be the same media type, HDD or SSD, as the other physical drives in the disk array.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Displays the active and paused PDMs and their status.

        start   Starts a manual PDM.

        stop   Stops a PDM.

        pause   Pauses a PDM.

        resume   Resumes a paused PDM.

-d <DA ID>   Specifies which disk array on which to perform the PDM.

-s <sequence Num>   Specifies the sequence number of the suspect drive.

-p <PD ID>   Specifies physical drive ID of the replacement drive.

Examples

pdm

pdm -a start -d0 -s2 -p10

pdm -a stop -d0 -s2

phydrv

Usage

phydrv [-a <action>] [-p <PdId>] [-c <Pd count>] [-v]

phydrv -a mod -p <PdId> -s "<list of settings>"

phydrv -a locate -p <PdId>

phydrv -a online -p <PdId>

phydrv -a offline -p <PdId>

phydrv -a clear -t <condition type> -p <PdId>

Summary

The phydrv command displays physical drive information, changes physical drive settings, locates individual drives, and forces a drive to an online or offline state.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Displays all physical drives, their make, model number, and array

173

they belong to. Their status is also shown.

mod   Modifiies physical drive settings.

locate   Flashes the physical drive's LED so you can location it.

online   Forces a drive from an Offline to an Online state.

offline   Forces a drive from an Online to an Offline state.

clear   Clears a drive's condition.

-p <PD ID>   Specifies the physical drive ID.

-c <count> Specifies number of drives when their ID numbers are sequential.

-t <condition type> Specifies type of condition to clear. Requires the -a clear option.

pfa   Clears a PFA condition on the drive.

staleconfig   Clears a stale configuration on the drive.

-d <drive type>   Specifies type of settings to modify. Requires the -a mod option.
Defaults to be all if -d is not specified.

sata   SATA related setting(s): writecache, rlacache, and

cmdqueuing.   The SATA settings apply to all SATA physical drives.

all   All drives where is applicable.

-s "<option>=<value>" Specifies which settings to change.

alias=   User-specified name, only for configured physical drives. Up to 32 characters, containing alpha- numeric characters, blank spaces and underscores. Beginning and ending blank

Caution

Do this action only in extreme conditions. It causes data corruption in most cases.

spaces are discarded.

The following global settings are for physical drives that support these features:

writecache=   Enables or disables write cache on the physical drive(s).

      enable

      disable

rlacache=   Enables or disables read look ahead cache on the physical drive(s).

      enable

      disable

cmdqueuing=   Enables or disables command queuing on the physical drive(s).

      enable

      disable

temppollint=   (15-255) Drive temperature polling interval in seconds. If value is 0, polling is disabled. For high availability products only.

mediumerrorthreshold=   (0-4294967294) Medium error threshold. If the threshold is reached, the physical drive is marked as dead. The default value is 0, indicating that physical drive is not marked as dead for medium errors. For high availability products only.

-v   Verbose mode. Used with -a list.

Examples

phydrv

phydrv -v

phydrv -a locate -p 9

phydrv -a mod -s "writecache=enable,rlacache=enable"

phydrv -a offline -p 8

phydrv -a online -p 8

rc

Usage

rc [-a <action>] [-l <LdId>]

rc -a start -l <LdId> [-n] [-p]

rc -a stop -l <LdId>

rc -a pause -l <LdId>

rc -a resume -l <LdId>

Summary

The rc command starts, stops, pauses and resumes a Redundancy Check and monitors the progress of a running Redundancy Check.

Options

-a <action>   Specifies action to perform.

         list   (Default) Displays active and paused Redundancy Checks and their status.

         start   Starts a Redundancy Check.

         stop   Stops a Redundancy Check.

         pause   Pauses a Redundancy Check.

         resume   Resumes a paused Redundancy Check.

-l <Ld ID> Specifies the logical drive ID on which to run the Redundancy Check.

-n Do not fix inconsistent data. This option causes Redundancy Check to run without correcting inconsistent data. All inconsistency errors are reported.

-p Pause on error. This option causes Redundancy Check to pause when it encounters inconsistent data. The default is to continue on error.

Examples

rc

rc -a start -l3 -n -p

rc -a start -l3

rc -a stop -l2

rb

Usage

rb [-a <action>] [-d <DaId>] [-s <SeqNo>]

rb -a start -d <DaId> -s <SeqNo> -p <PdId>

rb -a stop -d <DaId> -s <SeqNo>

rb -a pause -d <DaId> -s <SeqNo>

rb -a resume -d <DaId> -s <SeqNo>

Summary

The rb command starts, stops, pauses, and resumes a Rebuild and monitors the progress of a running Rebuild.

Note that the replacement drive must be the same media type, HDD or SSD, as the other physical drives in the disk array.

Options

-a <action>	Specifies action to perform.	
	list	(Default) Displays the running and paused Rebuilds and their status.
	start	Starts a manual Rebuild.
	stop	Stops a Rebuild.
	pause	Pauses a Rebuild.
	resume	Resumes a paused Rebuild.
-d <DA ID>	Specifies which disk array on which to perform the Rebuild.	
-s <sequence Num>	Specifies the sequence number of the failed physical drive. The source drive of the Rebuild.	
-p <PD ID>	Specifies the ID of the replacement physical drive. The target drive of the Rebuild.	

Examples

rb

rb -a start -d0 -s2 -p10

rb -a stop -d0 -s2

sc

Usage

sc [-a <action>] [-i <SpareId>]

sc -a start [-i <SpareId>]

Summary

The sc command starts a Spare Check and monitors the status of a running Spare Check.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Displays Spare Check status.

        start   Starts the Spare Check.

-i <Spare ID>   Specifies the spare ID on which to run Spare Check. Valid value range is 0~255.

Examples

sc

sc -a start -i 3

spare

Usage

spare [-a <action>]

spare -a list [-i <SpareId>] [-d <DaId>] [-v]

spare -a add [-i <SpareId>] -p <PdId> [-t g|d] [-r y|n] [-d <DaId list>] [-s "<list of settings>"]

spare -a mod -i <SpareId> [-t g|d] [-r y|n] [-d <DaId list>] [-s "<list of settings>"]

spare -a del -i <SpareId>

Summary

The spare command displays a list of hot spare drives and creates, modifies, and deletes hot spare drives.

A global hot spare can replace a failed drive from any redundant disk array.

A dedicated hot spare is assigned to one or more redundant disk arrays, and can only replace a drive that belongs to one of the assigned arrays.

A revertible hot spare can be transitioned back to spare status after it replaces a failed drive in a disk array. See the transit command.

The hot spare drive must be of equal or greater size than the drive it replaces. The spare drive must be the same media type, HDD or SSD, as the other physical drives in the disk array.

Options

-a <action>   Specifies the action to perform.

      list   (Default) Displays a list of hot spare drives.

      add   Adds new hot spare drives.

      mod   Changes hot spare drive settings.

      del   Deletes a hot spare drive.

-i <Spare Id>   Specifies the ID of the spare drive.

-p <PD ID>   Specifies the ID of the physical drive. Requires the -a add option to configure a drive as a spare.

-d <DA ID or DA ID List>   Specifies the disk array ID. Requires the -a list option. Displays a list of global spares and spares dedicated to this disk array.

      When used with other actions, it specifies the disk array IDs to

179

which this spare is dedicated.

-t <type>   Specifies the type of hot spare drive.

          g   A global hot spare drive.

          d   A dedicated hot spare drive.

-r <revertible>   Specifies whether the spare drive is revertible.

          y   Yes.

          n   No.

-s "<option>=<value>" Specifies options for the spare drive.

mediapatrol=   Enables or disables Media Patrol.

          enable

          disable

Examples

spare

spare -a add -p 14 -t g -r y

spare -a mod -i 1 -t d -d 0,1 -s "mediapatrol=disable"

spare -a del -i 0

swmgt

Usage

swmgt [-a <action>]

swmgt -a mod -n <component name> [-t <startup type>] [-s "<list of settings>]

swmgt -a start -n <component name>

swmgt -a stop -n <component name>

swmgt -a restart -n <component name>

Summary

The swmgt command allows a user to view and modify setting of software components.

Options

-a <action> Which action to perform.

list (Default) Displays all software components.

start Start a software component.

stop Stop a software component.

restart Restart a software component.

mod Change a component's startup type when system boots.

-n <component name> Specifies the component name to view setting, modify, start or stop.

email Email notification.

webserver Web server.

snmp SNMP

-t <startup type> Specifies the startup type.

automatic Component is automatically started when system boots.

manual Component has to be manually started by issuing command.

-s "<option>=<value>" Used to specify settings for this component. This is used when modifying (mod).

These options are comma separated.

email settings

serverip=   SMTP server IP address.

serverport=   SMTP server port number.

authentication= SMTP server authentication.

  no

  yes

username=   Username if using SMTP authentication.

password=   Password if using SMTP authentication.

senderaddr=   Sender's email address.

subject=   Email subject.

webserver settings

httpport=   Port number for web server.

sessiontimeout= Session time out in minutes. Maximum 1440.

ssl=   Turn on or off SSL for web server.

  enable

  disable

httpsport=   Port number if using SSL.

snmp settings

port=   Port number.

sysname=   System name string.

syslocation=   System location string.

syscontact=   System contact information string.

readcommunity= Read community name.

-p "<option>=<value>" Used to specify trap sinks for snmp.

        Note: Modified trap sinks will over-write existing trap sinks.

trapsinkip=   Trap sink IP address. For snmp only.

trapfilter=   Trap filter level. It implies the level and above. For snmp only.

info

warning

minor

major

critical

fatal

Examples

swmgt

swmgt -n webserver

swmgt -a start -n webserver

swmgt -a stop -n webserver

swmgt -a mod -n webserver -t automatic

swmgt -a mod -n webserver -s "httpport=8090"

Type " | more" at the end of each command, to display info page by page.

stats

Usage

stats [-t <type>] [-i <devId>] [-c <Count>]

stats -a clear

Summary

The stats command displays statistics of subsytem, controller, enclosure, physical drives, and logical drives; and resets the statistics count to zero.

Options

-a <action>   Specifies the action to perform.

           list   (Default) Displays the statistics.

           clear   Resets the statistics count to zero.

-t <type>   Specifies the device type.

           ctrl   Controller.

           logdrv   Logical drive.

           phydrv Physical drive.

           all   All the above options.

-i <devId> Specifies the device ID. Default is the first available device ID.

-c <Count>Specifies the device count. Default is all devices.

Examples

stats -t logdrv -i 0 -c 5

stats -a list -t all

stats -a clear

subsys

Usage

subsys [-a <action>] [-v]

subsys -a mod -s "<list of settings>"

subsys -a lock [-r] [-t <number of minutes>]

subsys -a unlock [-f]

subsys -a chklock

Summary

The subsys command displays and changes subsystem settings and locks the subsystem so that only you can make modifications.

Options

-a <action>　　　　Specifies the action to perform.

　　　list　　(Default) Displays information for the specified subsystem.

　　　mod　　Modifies subsystem settings.

　　　lock　　Locks the subsystem so other users cannot apply changes.
　　Other users must wait for you to unlock the system or for your lock to expire.

　　　unlock　　　　Clears a subsystem lock.

　　　chklock　　　　Checks the status of the lock.

-s "<option>=<value>" Specifies which subsystem settings to change.

　　　alias=　　User-specified name for the subsystem. Up to 48 characters, alpha-numeric characters, blank spaces and underscores. Beginning and ending blank spaces are discarded.

-t <number of mins>　　　　Specifies the number minutes to lock the subsystem. Requires the -a lock option. Default is 30 minutes.

-r　Renews the lock timer. Requires the -a lock and -t <number of mins> options.

-f　Specifies a forced unlock. Requires super user privilege.

-v　Specifies verbose mode.

Examples

subsys subsys -v

subsys -a mod -s "alias=MySubsystem"

subsys -a lock -t 60

subsys -a lock -r -t 35

subsys -a unlock

subsys -a chklock

sync

Usage

sync [-a <action>] [-l <LdId>]

Summary

The sync command monitors the progress of background synchronization. Background synchronization makes logical drive consistent. It starts automatically when a redundant logical drive is created. But unlike initialization, background synchronization allows read and write operations on the logical drive.

If an initialization starts, the background synchronization pauses until the initialization has finished.

Since background synchronization is starts, pauses, and resumes automatically, there is no need for start, stop, pause, or resume functions.

Options

-a <action>   Specifies the action to perform.

         list   (Default) Displays the current background synchronization activities and their status.

-l   Specifies the logical drive ID on which background synchronization is running.

Examples

sync

sync -l3

sync -a list -l3

transit

Usage

transit [-a <action>] [-d <DaId>] [-s <SeqNo>]

transit -a start -d <DaId> -s <SeqNo> -p <PdId>

transit -a stop -d <DaId> -s <SeqNo>

transit -a pause -d <DaId> -s <SeqNo>

transit -a resume -d <DaId> -s <SeqNo>

Summary

The transit command starts, stops, pauses, and resumes a transition and monitors the progress of a running transition.

Transition is an operation to replace a revertible spare drive currently used in a disk array with an new physical drive, so the reveritible spare can be restored to spare drive status. The destination drive can be an unconfigured drive, a non- revertible global spare, or a non-revertible spare dedicated to the array.

During transition, the data on the revertible spare is transferred to the destination drive while the disk array remains online. After transition, the destination drive becomes the part of the array and the revertible spare is a spared drive once again.

Note that the destination drive must be the same media type, HDD or SSD, as the other physical drives in the disk array.

Options

-a <action>   Specifies the action to perform.

        list   (Default) Displays the running and paused transitions and their status.

        start   Starts a manual transition.

        stop   Stops a transition.

        pause   Pauses a transition.

        resume   Resumes a paused transition.

-d <DA ID>   Specifies the id of disk array which contains the revertible spare drive.

-s <sequence Num>   Specifies the sequence number of the revertible spare drive in the array.

-p <PD ID>   Specifies the physical drive ID of the destination drive.

Examples

transit

transit -a start -d 0 -s 2 -p 10

transit -a stop -d 0 -s 2

user

Usage

-a <action> -u <username> -p <privilege> -s "<option>=<value>"

Summary

The user command is used to list, modify, create and delete user accounts on the subsystem.

Options

-a <action>

      list   (Default) Displays the current users.

      add   Create a new user account.

      mod   Modify an user account.

      del   Delete a user account.

-u <username> Specify the user account to display, edit or delete.

-p <privilege>   Specify the privilege lavel of the user.

      super   Designates user has complete administrative control.

      power   Designate user cannot modify user accounts or delete configurations.

      maintenance   Designates the user can perform background tasks only.

      view   Designates the user can only view information, has no administrative or write capability.

-s "<option>=<value>"

      status= Enable or disable user account.

      enable

      disable

name= Specify user account name.

email= Specify user email address.

help

Usage

-a <action> -u <username> -p <privilege> -s "<option>=<value>"

Summary

The user command is used to list, modify, create and delete user accounts on the subsystem.

?

Usage

-a <action> -u <username> -p <privilege> -s "<option>=<value>"

Summary

The user command is used to list, modify, create and delete user accounts on the subsystem.

TROUBLESHOOTING

This section focuses on how to address issues that might appear during the lifetime of the Vess A Series enclosure. Common issues that customers might see include hard drive problems and how to know when there is a problem with a hard drive, and how to create and send a service report to technical support.

If a hard drive has errors, is about to fail or has already failed, it will need to be replaced. Follow the instructions in "Installing Disk Drives" on page 16 to swap out bad hard drives.

This chapter includes the following troubleshooting sections and related information:

- "How do I know when a drive is failing?"
- "How to Rebuild a Disk Array"
- "The Alarm Buzzer is Sounding, what does this mean?"
- "How to disable the alarm buzzer"
- "How to Save a Service Report"

Note

Hard drives on all Vess A-Series models can be hot swapped, that is, they can be replaced without first shutting down the system.

Note

Follow the instructions in "Installing Disk Drives" on page 16 to swap out bad hard drives.

How do I know when a drive is failing?

There are many options to determine the health of physical hard drives. In Web PAM PROe, you can either use the Event Frame or go to the Physical Drives information display. Or you can simply check the status LED of the drives on the device.

Check Drive Status LEDs

The quickest way to check drive status if you are near the device is to simply look at the hard drive status LED indicators, then use the other LED indicators to help diagnose any problems that might exist.

Vess A3340 front
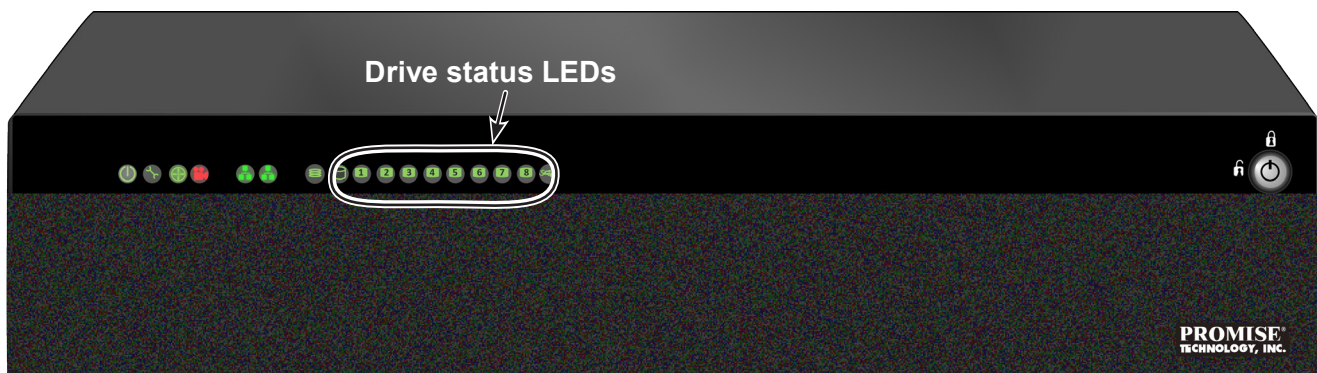
Vess A3340 Left front panel LED
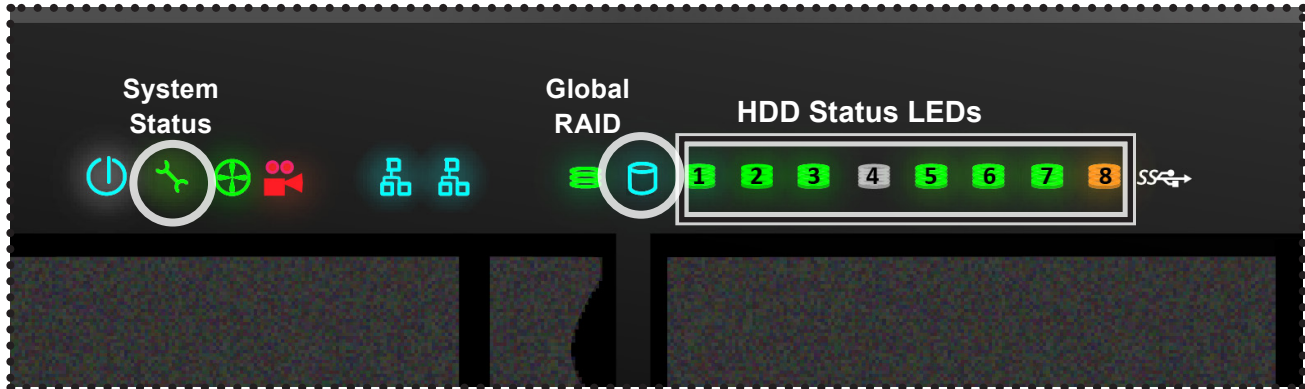
Status LEDs

Each drive slot on the Vess A3340 has a single corresponding HDD Status LED for, the LED display is located on the front panel. In addition to these, pay attention to the System Status and Global RAID LEDs to get an idea of what might be wrong with the affected hard drive.

Vess A3340 Status LED behavior
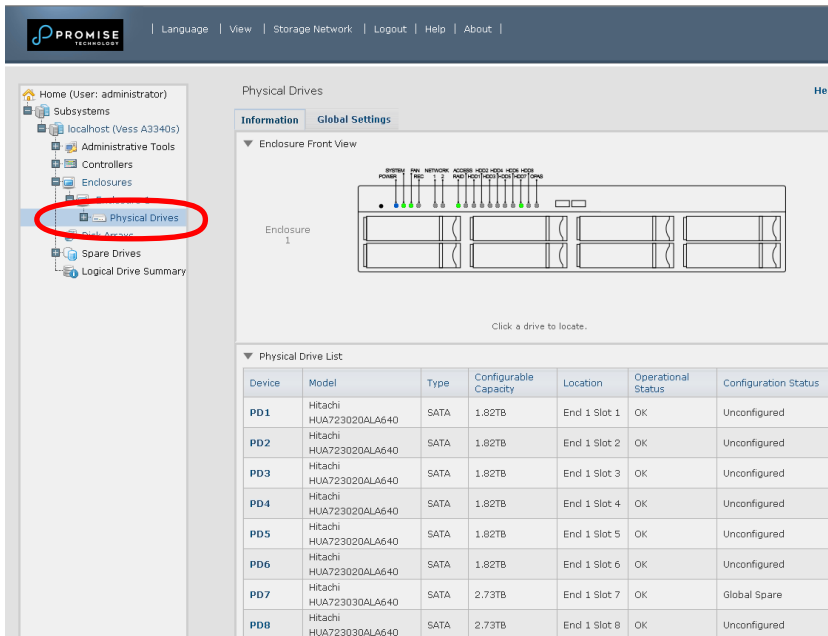
HDD Status	One LED for each HDD carrier. Each LED lights GREEN when healthy, RED if the RAID member is offline or there is a physical disk error, ORANGE indicates the drive is rebuilding, and a dark LED indicates either no drive is installed or the drive is not configured. A RED LED here means that drive should be replaced.
System Status	Lights GREEN when healthy, RED if there is a critical problem (LD offline, fan malfunction, PSU malfunction, voltage out of range, system temperature alert), remains dark when not ready.
Global RAID Status	Lights GREEN when healthy or RED if any RAID volume is offline, ORANGE for critical state of any logical drive. If a hard drive has failed, this will be ORANGE. In this case, it will be necessary to replace the affected drive and rebuild the affected RAID volume.

Check Drive Status in WebPAM PROe

To see the Event Frame, click **Show Event Frame** in the Web PAM PROe Header and check the list under **Device**, any physical drive problems will be indicated in the right most column, the top rows of the event table list the installed physical drives.

Also, in WebPAM PROee, you can go to the **Physical Drives List**. To see the Physical Drives List, expand the individual Enclosure icon in Tree View to see the Physical Drives icon for the enclosure. To display the information for any populated slot, you can expand the Physical Drives icon in Tree View to reveal links to each slot, or click on the slot in the Physical Drives List, or click on the populated slot in the virtual enclosure displayed in the menu.

View physical drive list

To see information about physical drives using the CLU menu:

1. Go to the **Main Menu** >> *Physical Drive Management*

2. Highlight the physical drive you want and press **Enter**. Basic information displays including the status of the physical drives.

View individual physical drive information

> **Note**
>
> In order that hard disk problems can be anticipated and dealt with smoothly, it is highly recommended to make sure that Media Patrol is enabled and running and Auto Rebuild is enabled if you are not using a spare drive. If using a spare drive, make sure it is healthy and available.

Anticipating Hard Drive Problems

It is recommended that you always keep a healthy spare drive installed, and run Media Patrol as a background activity so a failing hard drive can migrate data to the spare before the status turns critical.

In Web PAM PROe, Media Patrol is enabled or disabled using the Background Activities menu, you can also create a schedule to run Media Patrol.

Enable PDM and Media Patrol

- To enable Media Patrol, click on **Background Activities** in the Quick Links menu in the **Home** page, or, click on the **Subsystem** in Tree View then click on the Background Activities menu tab. Click to check the *Enable Media Patrol* option. Notice also that the *Auto Rebuild* option is here as well. If you want to automatically begin rebuilding a logical drive as soon as a faulty drive is replaced, make sure this option is enabled.

Start Media Patrol and Start PDM

- To begin running Media Patrol manually, click on the menu expander to the right of the Background Activities tab and scroll down and select *Start Media Patrol* to see the Start Media Patrol menu. Then click on the **Start** button.

- To schedule Media Patrol, click on the menu expander to the right of the Scheduler tab and scroll down and select *Add Media Patrol Schedule* to open the schedule menu. Use this menu to add a Media Patrol schedule.

To run Media Patrol using the CLU menu, go to **Main Menu** >> **Subsystem Management** >> **Media Patrol** and choose **Start, Stop, Pause,** or **Resume**. If you choose **Stop**, press **Y** to confirm.

Rebuilding a Disk Array
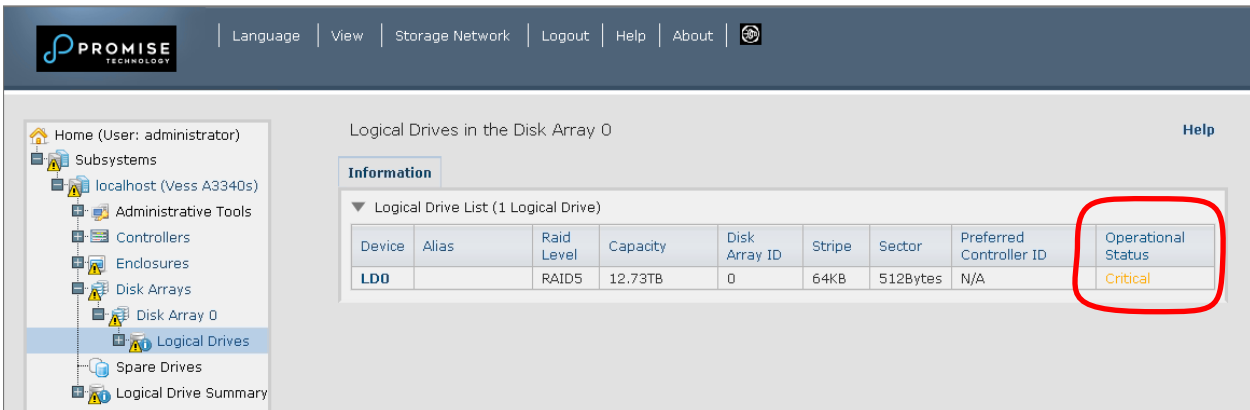
When you rebuild a disk array, you are actually rebuilding the data on one physical drive.

- When a physical drive in a disk array fails and a spare drive of adequate capacity is available, the disk array begins to rebuild automatically using the spare drive.

- If there is no spare drive of adequate capacity, but the Auto Rebuild function is ENABLED, the disk array begins to rebuild automatically as soon as you remove the failed physical drive and install an unconfigured physical drive in the same slot. See "Making Rebuild Settings"

- If there is no spare drive of adequate capacity and the Auto Rebuild function is DISABLED, you must replace the failed drive with an unconfigured physical drive, then perform a Manual Rebuild.

How to Rebuild a Disk Array

When a physical drive is indicated to be degraded or in critical state, the array that contains that drive needs to be rebuilt. If you are not using Auto Rebuild (requires a Spare Drive), then you must rebuild the array manually after the affected drive has been replaced. Follow the instructions here to rebuild an array.
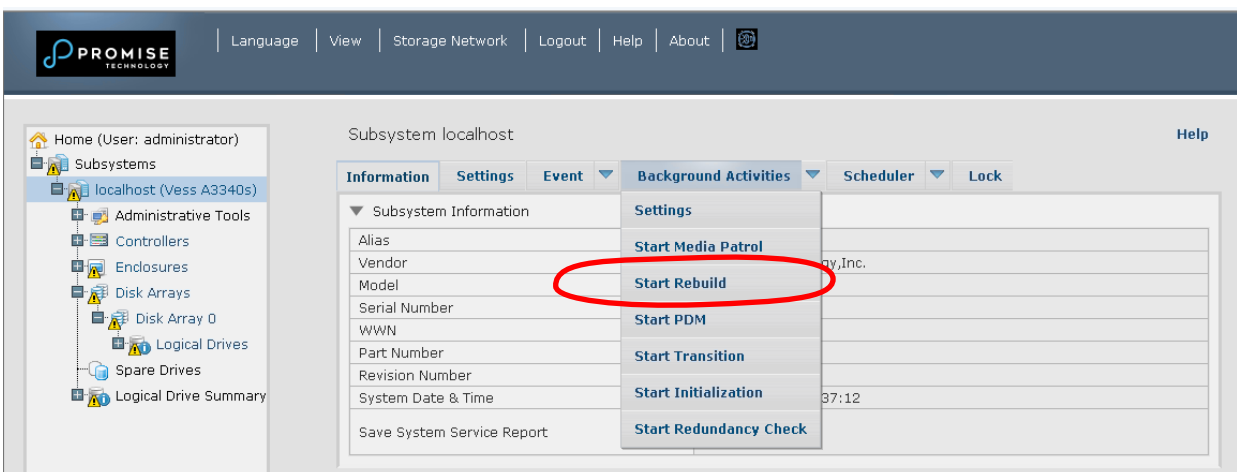
You will know that a logical drive is critical by looking at the **Operational Status** in the **Logical Drive Information** display.

To begin rebuilding the drive, go to the **Local Host** menu, the **Background Activities** and move the cursor to select **Start Rebuild**. A new menu appears.

Now determine the source and target for the rebuild. In the new menu, choose the **Source Physical Drive** and **Target Physical Drive** from the menus, and click on the **Submit** button.
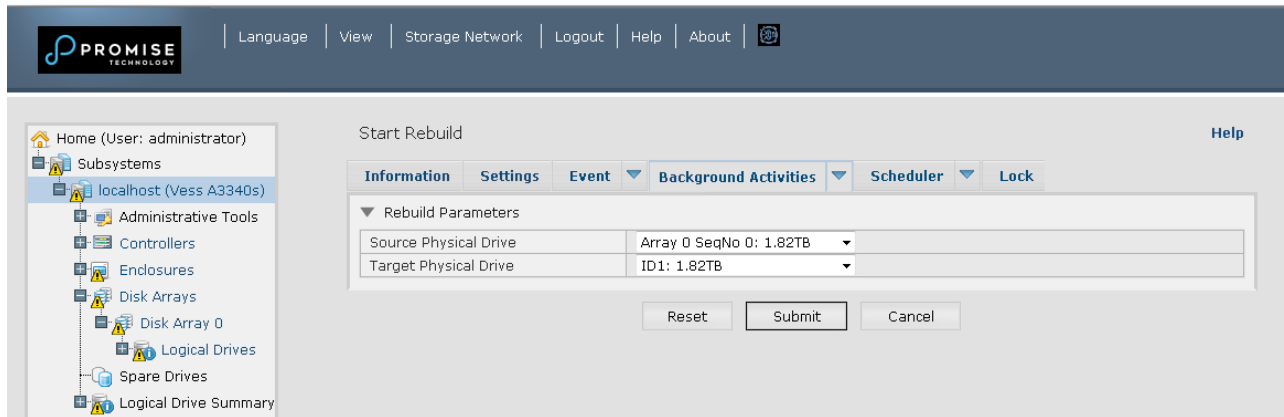
The progress of the rebuild is displayed in the Background Activities information display.

How to Save a Service Report

A Service Report is a detailed report covering the configuration and status of all components in your RAID system. A support technician or field engineer might request a service report for the purpose of diagnosis and troubleshooting.

To save a system configuration file:

1. Click on the Subsystem icon (IP address and device name) in Tree View to open the Subsystem Information display.

2. Click the **Save** button in the Save System Service Report row of the information display.

   Information for the report is gathered and compiled. This action takes up to a few minutes, depending on the size of your RAID system.

3. Determine where you want to store the file on the Host PC, then click the **Save** button in the pop-up menu.

   The report saves to your Host PC as a compressed HTML file.

4. Double-click the downloaded file to decompress it.

5. Double-click the report to open it in your default browser.

Once you have the service report file, you can email it to a Promise Technical Support representative.

The Service Report includes the following topics:

- About – Report utility
- BBM Info – Bad Block Manager
- BGA Summary – Status and settings
- Buzzer Info
- Controller Info
- Disk Array Info
- Disk Array Dump info
- Disk Array Verbose Info
- Enclosure Info
- Error Table Info
- Event Info - NVRAM
- Event Info - Runtime
- LogDrive Info – Basic logical drive information
- LogDrive Dump Info – Diagnostic information
- Logical Drive Verbose Info – Full logical drive information

- Network Info – Virtual port
- Phydriv Info – Basic physical drive information
- Phydriv Verbose Info – Full physical drive
- SWMGT Info – Software management
- Service Setting – Email
- Service Setting – Webserver
- Spare Info – Basic spare drive information
- Spare Dump Info – Diagnostic information
- Spare Verbose Info – Full spare Drive information
- Statistic Info
- Subsystem info
- User Info

The Alarm Buzzer is Sounding, what does this mean?

When you first power-up the Vess system beeps twice to show normal operation.

The audible alarm sounds at other times to inform you that the system needs attention. But the buzzer alarm is not specific. Check the device LEDs and Events displays or logs for more information.

When the alarm sounds:

- Check the front and back of the enclosure for red or orange LEDs.

- If email notification is enabled, check for new messages.

- Check the event log.

When a continuous tone sounds, there are multiple alarm patterns sounding at the same time (see example number 1 illustrated below).

Alarm buzzer patterns

1   .25s .75s .25s   **1x**

2   .25s .75s .25s .75s .25s   2.5s   ↻

3   .25s .5s .25s   6s   ↻

4   .25s .25s .25s .5s .25s .75s .25s 1s .25s 1.25s .25s   3s   **2x**

5   ∞ s
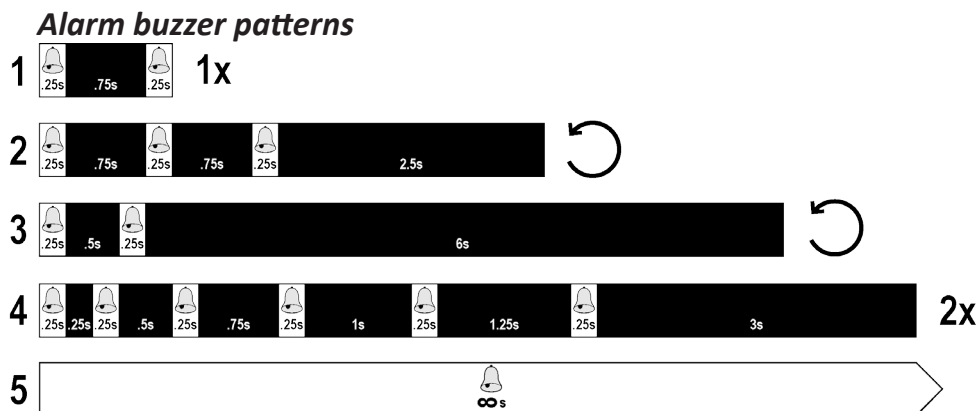
Other alarm patterns include three short buzzes followed by a longer silence, then repeated (example number 2 above). This can indicate a serious problem that requires immediate action such as high enclosure temperature or the system fan is not installed. If you hear this, check the System Status and Fan LEDs. If these are normal, it might indicate a physical drive problem, or a power supply problem. Check the event log for more information.

Pattern number 3 above might indicate an LD offline. Pattern number 4 might be an LD critical or bad sector on a physical disk.

How to disable the alarm buzzer

To disable the buzzer with Web PAM PROe, open WebPAM PROe, click on the enclosure in Tree View, then click on the Buzzer menu expander, scroll to *Settings* and click the **Enable Buzzer** option box to remove the check mark. Click the **Submit** button.
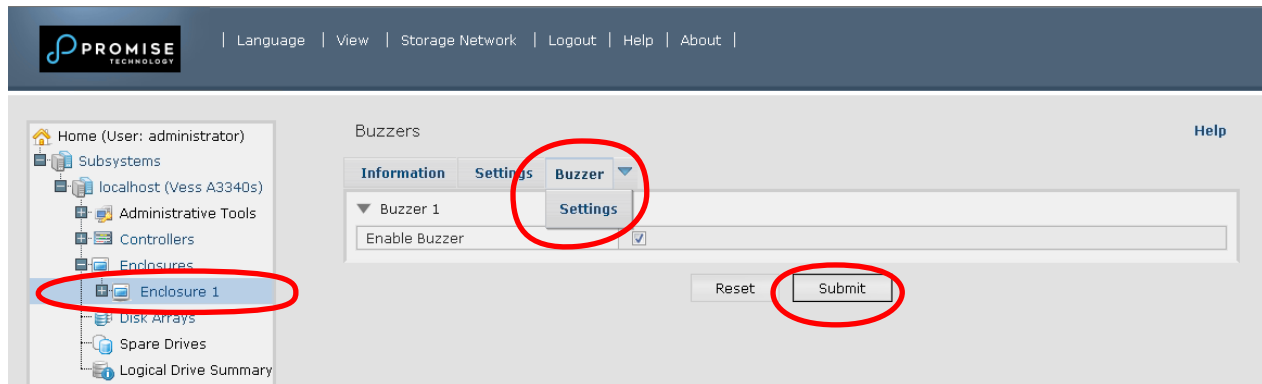
To disable the buzzer in the CLU,

1. From the **Main Menu** use the arrow keys to go to ***Buzzer***, a list of Controllers appears with the current buzzer setting and status.

2. Highlight ***Enabled*** and press the spacebar to toggle ***No***.

3. Press **Control-A** to save your settings.

Reinstalling the Operating System

In the unlikely event that your Vess A-Series system will not boot normally, you might need to reinstall the operating system. This can be done by first creating a boot image on a USB flash memory device, then loading the Windows from that image. Note that the BIOS of the Vess A-Series is configured to first look for the boot image in a USB drive. The install image is available at the PROMISE website online.

To download the install image, go to www.promise.com, and follow these steps:

1. From the **Promise** home page, find the Vess A-Series menu page.
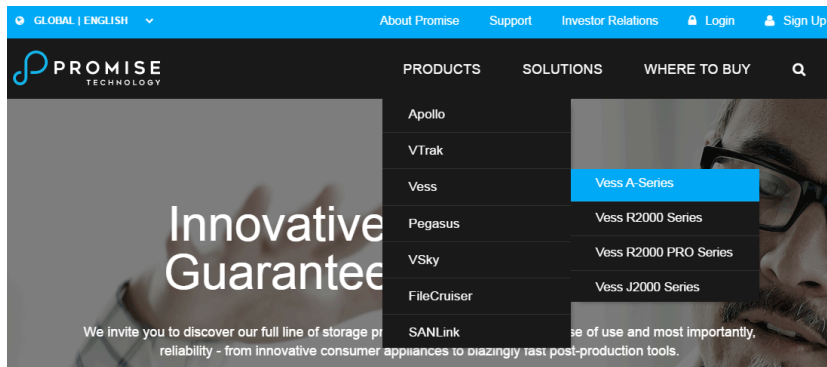
2. Scroll down the page and expand the **Resources** *menu*.
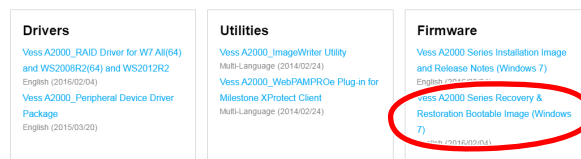
3. Under **Drivers/Utilities/Firmware**, click on the link for the *bootable restoration image* to download.

> ### Note
> You can also download an image writer utility for Vess A-Series here.

Reintsall Windows

Follow the instructions below to reinstall the Windows OS. You will need another computer running Windows to perform this procedure.

1. Download **ImageWriter** (see instructions on previous page).

2. Download latest *Vess A-Series Windows* image.

3. Insert the USB flash drive into your computer.

4. Use the **Select USB drive** menu to choose the drive letter of the USB flash memory device, then use the **Select Image** button to locate the image file you downloaded. When you have the USB drive letter and image file location selected, click **Write!** to begin. The process takes a few minutes. A boot image is written to the USB device.
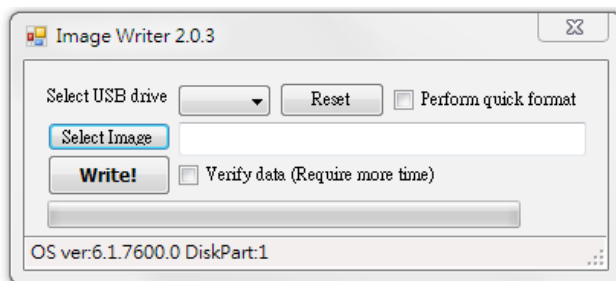
5. Insert the USB drive into the Windows Vess A-Series and boot up.

6. During the boot, a dialog menu asks if you want to reinstall Windows. Choose the option "i" to reinstall the Windows OS, you're existing RAID arrays will not be affected.

7. After the install is finished, remove the USB flash drive, boot the Vess A-Series, then complete Windows setup.

LED Troubleshooting Quick Guide

See illustration on next page.

System	Fan	Global RAID	HDD		PSU	Diagnosis	Check System Event	Corrective Action
Green	Green	Amber	Red		Off	LD critical	Logical drive status set to critical	Replace failed HDD and rebuild LD
Green	Green	Amber	Failed HDD: Red	Spare: Amber	Off	Rebuild	Rebuild is started	Wait until rebuild is finished. Both indicators will light green when rebuild is completed.
Red	Green	Red	Red		Off	LD offline	Logical drive status set to offline. Possible data loss.	Contact Technical Support
Red	Green	Off	Off		Off	Controller temperature above critical threshold	Enclosure temperature is above critical threshold	Check enclosure airflow, remove any obstruction.
Red	Green	Off	Off		Red	PSU failure	PSU is NOT installed PSU is malfunctioning and turned off	Check PSU power cord, plug and power connection.
							PSU is NOT installed PSU has been removed	Check PSU connection. Try unplugging power and plugging back in. Replace power cord if needed.
Red	Amber	Off	Off		Off	CPU fan malfunction	PSU is NOT installed	Contact Technical Support
Red	Amber	Off	Off		Off	System fan failure	Fan NOT installed	Replace system fan module
						Motherboard voltage out of range	Voltage power is out of threshold range	Contact Technical Support
blinking red	Green	Off	Off		Off	HDD temperature warning	Firmware detects physical drive temperature exceeded threshold	Check enclosure airflow, remove any obstruction.
						HDD temperature out of critical threshold	Firmware detects physical drive temperature exceeded critical threshold	Check enclosure airflow, remove any obstruction.
Off	Off	Off	Off		Off	Controller temperature warning	Enclosure temperature exceeded warning threshold	Check enclosure airflow, remove any obstruction.

209

LED indicators on front of Vess A3340
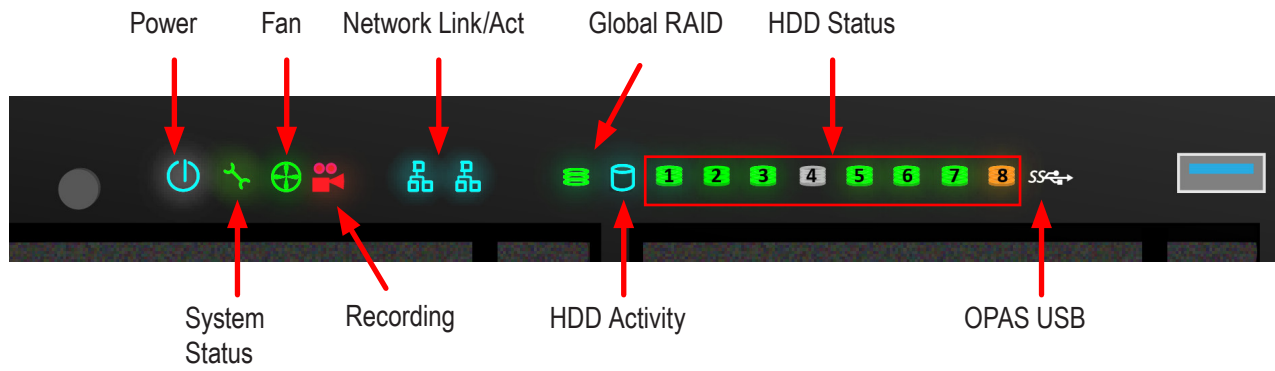
FAQ

Q: What is the Vess A3340 **Storage Appliance for Video Surveillances?**

A: The Vess A3340 storage platform is PROMISE's Storage Appliance for Video Surveillance solutions that are engineered specifically to be the best solution for midsize to large IP video surveillance deployments.

Q: How does it work for surveillance video recording?

A: In addition to the installed Windows operating system, the Vess A3340 package can be customized to include a leading Video Management Software suite and Disk Drives, thus minimizing the integration and installation process. Users no longer need an extra PC/server, add-on cards, or a separate connected storage for a complete video surveillance system; the Vess Storage Appliance for Video Surveillance does it all!

Q: What should I do if the device OS fails?

A: Unlike regular COTS servers that come with standard Windows OS, the Vess A3340 provides an embedded version that requires a certain process to rebuild the OS image. Users need to consult PROMISE tech support and follow installation guide to complete the setup.

Q: When I rebuild the Window embedded OS image, a product key# is required?

A: No, users do not have to enter any product key during re-installation. You need to get all the required software package like OS image(license built-in), RAID and device drivers from PROMISE Surveillance Storage web page for installation.

Q: Can I use more than one VMS with the Vess A3340**?**

A: Yes, you can choose any other video management software with the Vess A3340 as long as it functions compatible under WIN7 OS(64-bit).

Q: What's the standard warranty of Vess A3340**?**

A: We provide the same standard three (3) years hardware warranty from the time of the delivery of the product to the original end user.

Q: Can I purchase extended warranty package to Vess A3340**?**

A: Yes, we provide 2-year extended warranty program that uses the same order and support practice as Vess product series.

CONTACTING TECHNICAL SUPPORT

PROMISE Technical Support provides several support options for PROMISE users to access information and updates. We encourage you to use one of our electronic services, which provide product information updates for the most efficient service and support.

PROMISE E-Support: https://support.promise.com

PROMISE web site: http://www.promise.com//

When you contact us, please have the following information available:

- Product model and serial number
- BIOS, firmware, and driver version numbers
- A description of the problem / situation
- System configuration information, including: motherboard and CPU type, hard drive models, SAS/SATA/ATA/ATAPI drives & devices, and other controllers.

United States

580 Cottonwood Drive

Milpitas, Ca 95035, USA

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Australia

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

EMEA

Netherlands

Science Park Eindhoven 5228

5692 EG Son, The Netherlands

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Austria

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

France

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Germany

Europaplatz 9

44269 Dortmund, Germany

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Sweden

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Switzerland ITF

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Norway ITF

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Belgium

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Luxembourg

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

United Kingdom

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Taiwan

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

China

Room 1108, West Wing, Shi Chuang Plaza, 22 Information Road

Shangdi IT Park, Haidian District, Beijing 100085

Fax: 86-10-8857-8015

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Korea

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Hong Kong

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Singapore

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Japan

3F, Mura Matsu Bldg, 3-8-5, Hongo Bunkyo-ku

Tokyo 113-0033, Japan

Technical Support (E-Support): https://support.promise.com

Web site: http://www.promise.com//

Limited Warranty

PROMISE Technology, Inc. ("PROMISE") warrants that this product, from the time of the delivery of the product to the original end user:

    a)   all components for a period of three (3) years;

    b)   the cache backup battery, for a period of one (1) year;

    c)   will conform to PROMISE's specifications;

    d)   will be free from defects in material and workmanship under normal use and service.

This warranty:

    a)   applies only to products which are new and in cartons on the date of purchase;

    b)   is not transferable;

    c)   is valid only when accompanied by a copy of the original purchase invoice.

    d)   Is not valid on spare parts.

This warranty shall not apply to defects resulting from:

    a)   improper or inadequate maintenance, or unauthorized modification(s), performed by the end user;

    b)   operation outside the environmental specifications for the product;

    c)   accident, misuse, negligence, misapplication, abuse, natural or personal disaster, or maintenance by anyone other than a PROMISE or a PROMISE-authorized service center.

Disclaimer of other warranties

This warranty covers only parts and labor, and excludes coverage on software items as expressly set above.

Except as expressly set forth above, PROMISE disclaims any warranties, expressed or implied, by statute or otherwise, regarding the product, including, without limitation, any warranties for fitness for any purpose, quality, merchantability, non-infringement, or otherwise. PROMISE makes no warranty or representation concerning the suitability of any product for use with any other item. You assume full responsibility for selecting products and for ensuring that the products selected are compatible and appropriate for use with other goods with which they will be used.

PROMISE does not warrant that any product is free from errors or that it will interface without problems with your computer system. It is your responsibility to back up or otherwise save important data before installing any product and continue to back up your important data regularly.

No other document, statement or representation may be relied on to vary the terms of this limited warranty.

PROMISE's sole responsibility with respect to any product is to do one of the following:

   a)   replace the product with a conforming unit of the same or superior product;

   b)   repair the product.

PROMISE shall not be liable for the cost of procuring substitute goods, services, lost profits, unrealized savings, equipment damage, costs of recovering, reprogramming, or reproducing of programs or data stored in or used with the products, or for any other general, special, consequential, indirect, incidental, or punitive damages, whether in contract, tort, or otherwise, notwithstanding the failure of the essential purpose of the foregoing remedy and regardless of whether PROMISE has been advised of the possibility of such damages. PROMISE is not an insurer. If you desire insurance against such damage, you must obtain insurance from another party.

Some states do not allow the exclusion or limitation of incidental or consequential damages for consumer products, so the above limitation may not apply to you.

This warranty gives specific legal rights, and you may also have other rights that vary from state to state. This limited warranty is governed by the State of California.

Your Responsibilities

You are responsible for determining whether the product is appropriate for your use and will interface with your equipment without malfunction or damage. You are also responsible for backing up your data before installing any product and for regularly backing up your data after installing the product. PROMISE is not liable for any damage to equipment or data loss resulting from the use of any product.

Returning the Product For Repair

If you suspect a product is not working properly, or if you have any questions about your product, contact our Technical Support staff, and be ready to provide the following information:

- Product model and serial number (required)
- Return shipping address
- Daytime phone number
- Description of the problem
- Copy of the original purchase invoice

The technician helps you determine whether the product requires repair. If the product needs repair, the technician issues an RMA (Return Merchandise Authorization) number.

	Important
	Obtain an RMA number from Technical Support **before** you return the product and write the RMA number on the label. The RMA number is essential for tracking your product and providing the proper service.

Return ONLY the specific product covered by the warranty. Do not ship cables, manuals, CDs, etc.

USA and Canada:	PROMISE Technology, Inc. Customer Service Dept. Attn.: RMA # _____ 47654 Kato Road Fremont, CA 94538
Other Countries:	Return the product to your dealer or retailer. Contact them for instructions before shipping the product.

You must follow the packaging guidelines for returning products:

- Use the original shipping carton and packaging
- Include a summary of the product's problem(s)
- Write an attention line on the box with the RMA number
- Include a copy of your proof of purchase

You are responsible for the cost of insurance and shipment of the product to PROMISE. Note that damage incurred due to improper transport or packaging is not covered under the Limited Warranty.

When repairing returned product(s), PROMISE may replace defective parts with new or reconditioned parts, or replace the entire unit with a new or reconditioned unit. In the event of a replacement, the replacement unit is under warranty for the remainder of the original warranty term from purchase date, or 30 days, whichever is longer.

PROMISE pays for standard return shipping charges only. You must pay for any additional shipping options, such as express shipping.

APPENDIX: DRIVER INSTALLATION AND UPDATE

This appendix provides instructions for installing or updating the driver for the PROMISE RAID engine, as well as WebPAMPROe, the management GUI for the PROMISE Vess A-Series.

Follow these step-by-step instructions to install the latest hardware driver for the RAID and the latest WebPAMPROe version. These are available for download from the PROMISE website www.promise.com in a single compressed file package.

Instructions for uninstalling the driver and how to check the driver version are included after the update instructions.

Note, if you are using this procedure to update the driver and software, I/O operations will cease during the update procedure, so make sure any clients that are using the Live DB or video archive are alerted and prepared prior to starting the update.

Update/Installation Requirements

USB Flash Drive

A USB flash drive containing the update package is needed. Follow the instructions below to download the compressed file package and place a copy of the uncompressed file on the USB flash drive.

Operation Systems

The instructions in this document apply to Vess A3340 units running the Windows operating system.

Download Driver Package

1. Go to the PROMISE website and click on **Products** near the top of the page, select the **Vess** option, then choose **Vess A-Series**. Scroll down and expand the **Resources** menu, scroll down more for the **Drivers / Utilities / Firmware** links menu. Find the driver or driver package listed under **Drivers**, and click the link to download.

2. Uncompress the file and place it on the USB flash drive used for the update.

Update/Install the Driver

Follow these steps to complete the installation or update of the driver. If you have not yet downloaded the compressed files needed for updating the driver, see the previous page for download instructions.

For simplicity, variations of the terms "update" and "install" are used interchangeably in the following description to mean driver update or driver installation. The procedure for both updating or installing the driver are identical.

1. Launch the **Driver Update Package** install application.

    To launch, double-click on this icon:

2. The first dialog menu to appear is a standard warning. Press the **Run** button to proceed.
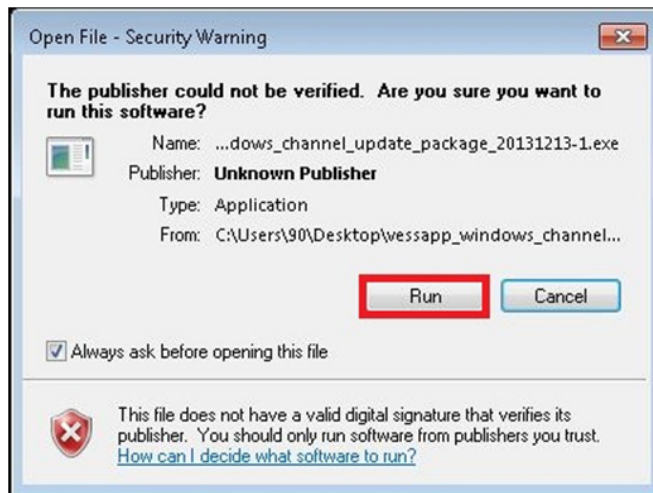
3. A new dialog asks if you want to install the package. Click on **Yes**.
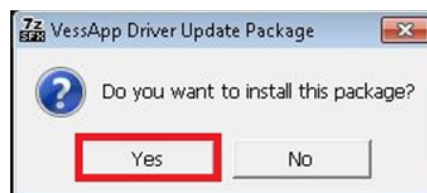
4. It is necessary to reboot the Vess A-Series during the update process.

   Click **Yes** to proceed with the update.
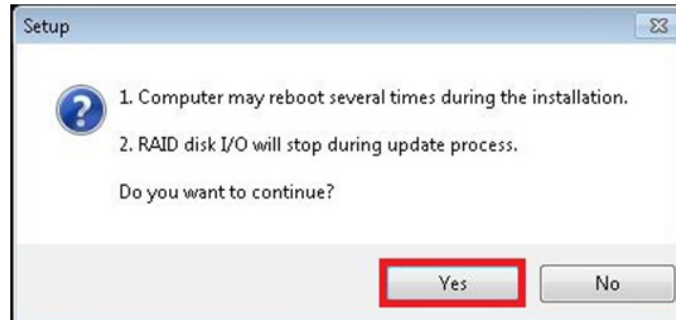
5. In the Setup Wizard menu, click on the **Next** button to proceed.
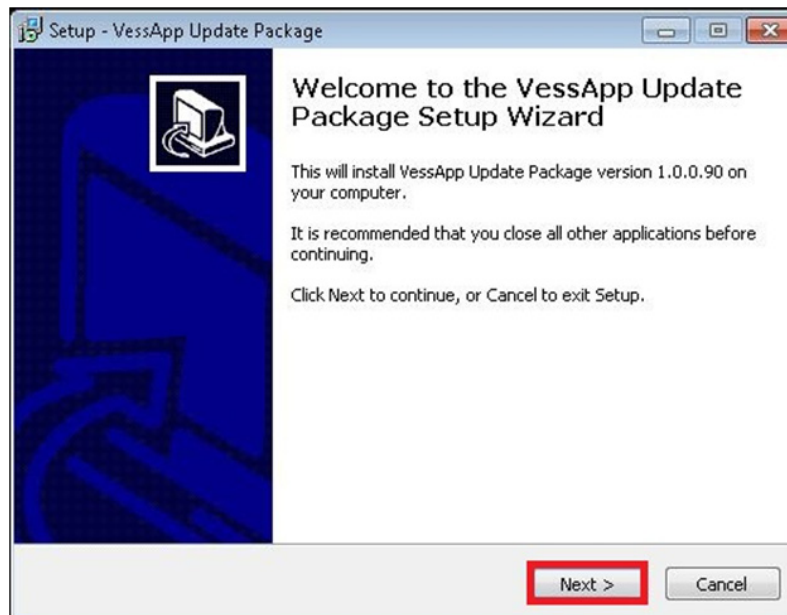
6. The driver update resumes, press the **Install** button to proceed.
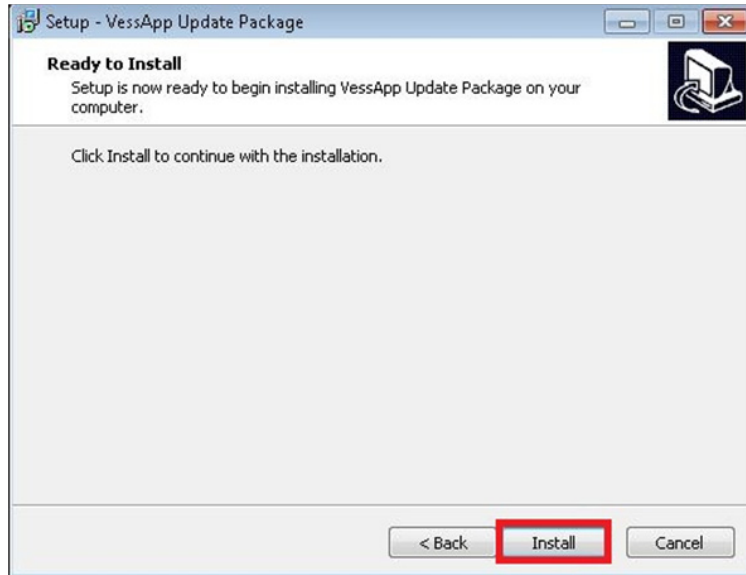
7. In the **Driver Installation Wizard** menu, press the **Next** button

8. The Driver Installation Wizard menu informs you that the driver is now installed. Press the

    Finish button to continue.

9. The final Setup menu appears. Click on **Finish**.
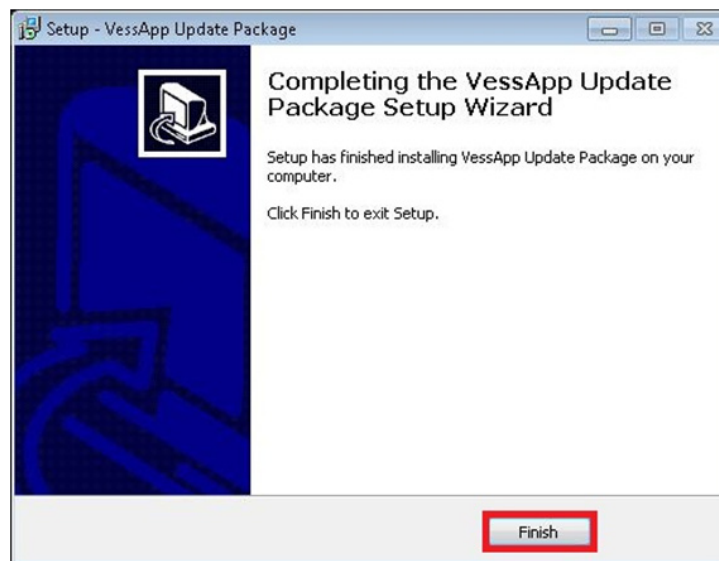
10. A restart is required for the new driver to begin operating. Press the **OK** button to restart the

    system.
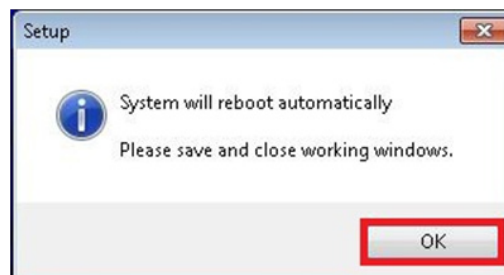
Uninstall Driver

If you need to uninstall the driver for the RAID engine or undo installation of the Update Package, follow these steps.

1. Open **Programs and Features** to uninstall the driver.

Go to **Control Panel>All Control Panel Items>Programs and Features**, choose the **Unistall** option. Get the most recent version of the **VessApp Update Package** listed in the menu.
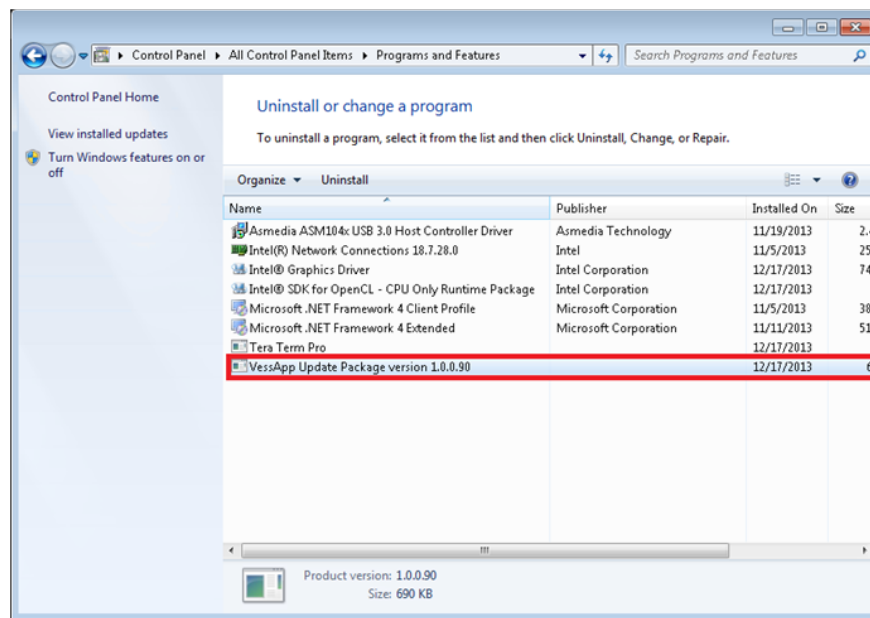
2. A system restart is necessary are uninstalling the driver. Click **Yes** to continue.
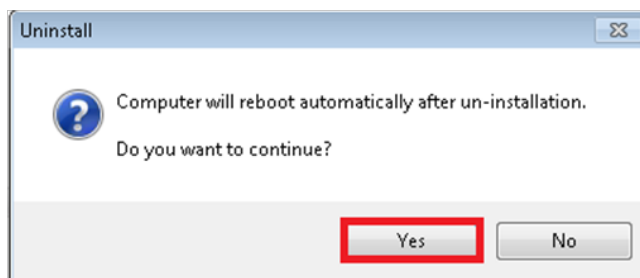
3. Confirm that you want to uninstall the driver by clicking on the **Yes** button.
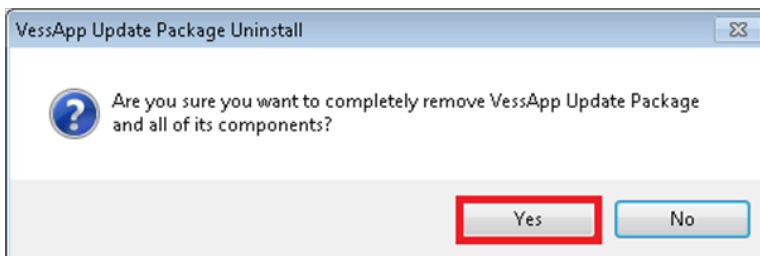
4. Click the **OK** button to continue.
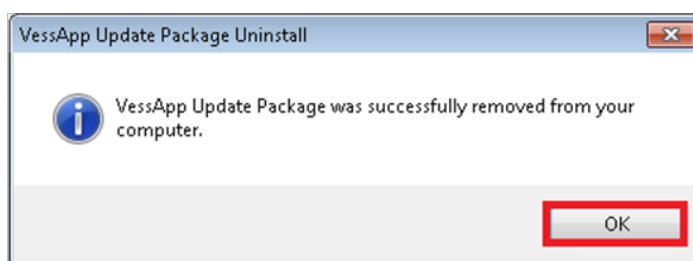
5. Click the **OK** button to restart Windows. Upon restarting the driver and software have been

   removed.
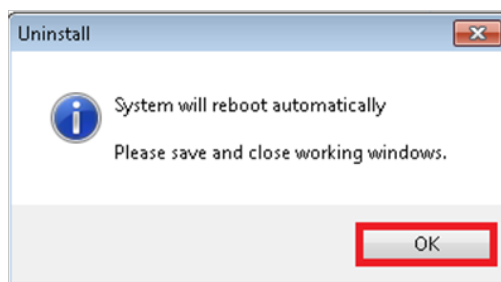
How to check driver version

To check if the Vess A-Series driver that is currently installed is up to date, you can check the RAID driver version or WebPAMPROebuild version with the CLI or WebPAMProE interfaces, or with the Windows device manager.
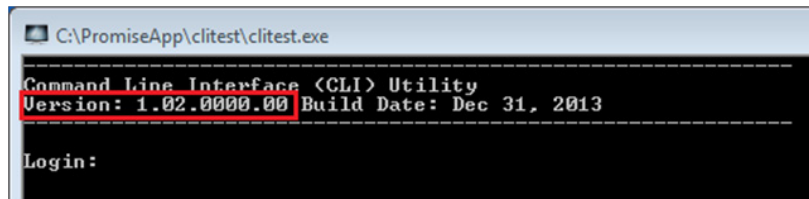
Check versions with CLI

Tocheck the BIOS version, Firmware version, software version and Install package version with the CLI user interface:

1. To open the CLI menu, click on the Windows **Start** button, type **clitest** in the text entry menu and press **Enter**. This displays the icon for the shortcut to the CLI interface. Double-click on the icon.
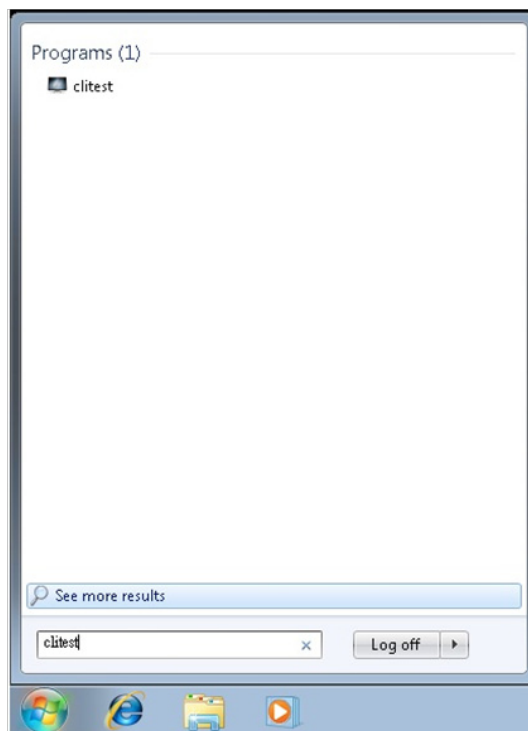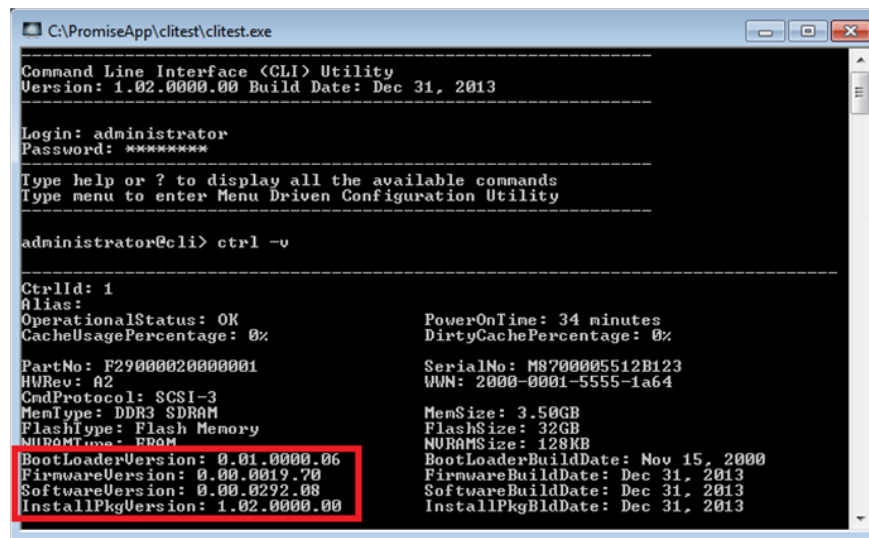
2. The RAID driver **Version** is listed at the top of the **Login** menu.

3. To view additional version information, login and type **ctrl –v**.

Note that the default User Name is **administrator** and the Password is **password**.

The version information is listed below the administrator prompt. See example above.

Check versions with WebPAM PROe

To check the Install package version with the WebPAMPROe user interface:

1. To open WebPAMPROe, click the shortcut of CLI of WebPAMProE on the desktop.

2. Login. The default User Name is **administrator** and the Password is **password**.

3. To view the Driver Version, go to **Controller >Controller1>Install PKg Version**, the package

    version is listed in the menu display (see below).

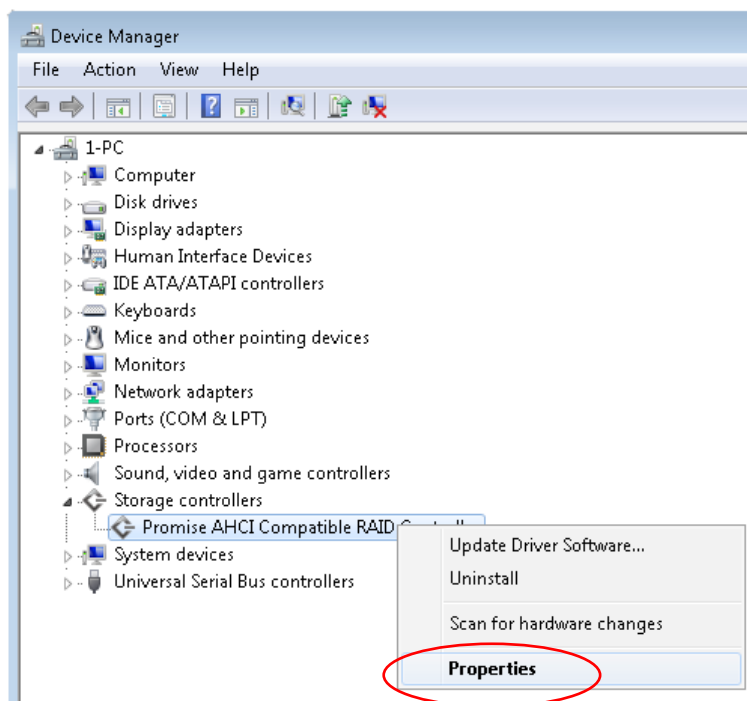# Check versions in windows device manager

To get the RAID driver version using the Windows Device Manager:

1. Open the **Windows Device Manager**. Go to **Start > Control Panel > Device Manager**.

Double-click the Device Manager icon
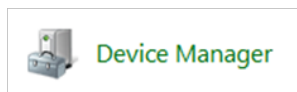
2. Look for **Storage controllers** and right-click on the **Properties** option in the pop-up menu.

3. Click the **Driver** tab to see the driver version.