

**Installation
and Reference
Guide**

HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition

Product Version: 3.0F

Eighth Edition (April 2005)

Part Number: AA-RR4VH-TE

This guide describes HP StorageWorks Secure Path for Active-Passive disk arrays, Secure Path for Active-Active disk arrays, and Secure Path Workgroup Edition for VA software.



© Copyright 2000–2005 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup
Edition Installation and Reference Guide
Eighth Edition April 2005
Part Number: AA-RR4VH-TE

Contents

About this Guide	9
Overview	10
Intended audience	11
Related documentation	11
Conventions	12
Document conventions	12
Text symbols	12
Equipment symbols	13
Getting help	15
HP technical support	15
HP storage web site	15
HP authorized reseller	15
1 Secure Path Active-Passive Disk Arrays	17
Overview	18
Features	21
Software components	22
Drivers	22
Agent	23
Management tools	24
Controller ownership	24
Path definition	25
Secure Path operation	26
Failback options	26
Load balancing	27
Path verification	28
Path management behavior summary	28
Secure Path for Active Passive disk arrays hardware setup	29
Hardware setup overview	29
Installing a new Secure Path configuration	30

Configuring switches	31
Configuring the HSG80-based <i>StorageWorks</i> array	32
Configuring optional HSG80-based array features	35
Setting up additional SCSI-2 LUNs	35
Setting a preferred unit to a controller	38
Using SCSI-3	39
Managing the command console LUN in SCSI-2 mode	39
Configuring the HSV110-based <i>StorageWorks</i> array	40
System configuration	41
Configuring SCSI-3 for HSG80-based systems	44
What to do if ioscan does not see all paths to the array	45
Installing Secure Path for Active-Passive disk arrays	49
Installing Secure Path	49
Installing Secure Path on a SAN boot device	53
Features	53
Prerequisites	53
Installation steps	53
Limitations	54
Managing Secure Path for Active-Passive arrays	55
Secure Path for Active-Passive devices	55
Spmgr commands	55
Spmgr common terms	58
Displaying configuration information	59
Controller states	59
Path states	59
Device states	60
Understanding LUN/path instance numbering	61
Display header information	63
Display differences between HSG and HSV controllers	63
The display command	64
# spmgr display	65
# spmgr display -a[v] HBA	66
# spmgr display -c[v] controller_serial_number	68
# spmgr display -d[v] device_instance	70
# spmgr display -p path_instance	72
# spmgr display -r[v] WWNN	73
# spmgr display -s	75
# spmgr display -u	76

The alias and unalias commands	77
# spmgr alias alias_name old_name	77
# spmgr unalias	77
# spmgr alias	78
Setting storage system parameters.	78
The set command.	79
# spmgr set -a on off WWNN.	79
# spmgr set -b on off rr lb li ls WWNN	80
# spmgr set -p on off WWNN	80
# spmgr set -f (1...65535 seconds)	80
The log command	80
# spmgr log -l 0, 1..3	81
# spmgr log -c 0,1..3	81
# spmgr log -n 0, 3.	81
# spmgr log	81
The notify command	82
Severity levels	82
# spmgr notify add.	82
# spmgr notify delete	83
# spmgr notify	83
Path management.	83
The select command	84
# spmgr select -c controller_serial_number.	84
# spmgr select -c controller_serial_number -d device	84
# spmgr select -p path_instance.	85
Preferred controller	85
The prefer and unprefer commands.	86
# spmgr prefer path_instance.	87
# spmgr unprefer path_instance.	88
Impact of load balancing and active paths.	88
The restore command	88
# spmgr restore all	89
# spmgr restore -d device.	89
# spmgr restore -r WWNN	90
The quiesce command	90
# spmgr quiesce -a HBA	90
# spmgr quiesce -c controller_serial_number	91
# spmgr quiesce -p path_instance	91

The restart command	91
# spmgr restart all	92
# spmgr restart -a HBA	92
# spmgr restart -c controller.	92
# spmgr restart -p path_instance	92
The add and delete commands.	93
Adding LUNs	93
Deleting LUNs.	94
# spmgr add WWLUNID	94
# spmgr add -r WWNN all.	95
# spmgr clean all	96
# spmgr clean -d WWLUNID	96
# spmgr clean -r WWNN.	96
# spmgr delete WWLUNID device	97
# spmgr delete -r WWNN all	97
# spmgr passwd	98
Secure Path for Active-Passive remote management.	98
Installing remote management.	99
Removing a client from a server	99
Remote spmgr execution	99
Removing/upgrading Secure Path for Active-Passive disk arrays	101
Removing Secure Path.	101
Upgrading Secure Path software	101
Upgrade requirements	102
Upgrade preparation	102
Upgrading from the Web.	104
Troubleshooting Secure Path for Active-Passive disk arrays.	106
2 Secure Path for Active-Active Disk Arrays.	117
Features.	118
ULM services	119
Dynamic load balancing	120
VA disk arrays	120
Automatic failover	121
Automatic path recovery.	122
Online device discovery	123
System requirements.	124
Installation	125
Installing Secure Path software	125

Secure Path SAN boot setup for Active-Active devices	126
Upgrading from the Web	127
Uninstalling Secure Path.	128
Command line interface	129
The autopath delete command	129
The autopath add command	130
The autopath set command.	131
The autopath display command	131
List of All Arrays Connected to a Host	132
Details of All LUNs Connected from an Array.	132
List of Array Controllers Connected to the Host.	133
List all LUNs in the Unattached List.	134
Display the LUN info of the Lun using a Device Path	135
Display the LUN info of the Lun using a LUN WWID	136
Display all LUNs Connected to the Host	137
The autopath help command	139
The autopath recover command.	140
The autopath discover command	140
The autopath retrieve command.	141
The autopath set_lbpolicy command	141
The autopath set_prefpath command.	141
Troubleshooting Secure Path	143
Recovering after a failure.	143
Secure Path messages.	143
3 Secure Path Workgroup Edition for VA	145
Features.	146
ULM services	147
Dynamic load balancing.	148
VA disk arrays	148
Automatic failover	149
Automatic path recovery.	150
Online device discovery	151
System requirements.	152
Installation	153
Installing Secure Path Workgroup Edition for VA	153
Secure Path SAN boot setup for VA devices.	153
Upgrading from the Web	155
Uninstalling Secure Path.	156

- Command line interface 157
 - The autopath delete command 157
 - The autopath add command 158
 - The autopath set command. 159
 - The autopath display command 159
 - List of All Arrays Connected to a Host. 160
 - Details of All LUNs Connected from an Array. 160
 - List of Array Controllers Connected to the Host. 161
 - List all LUNs in the Unattached List. 162
 - Display the LUN info of the Lun using a Device Path 163
 - Display the LUN info of the Lun using a LUN WWID 164
 - Display all LUNs Connected to the Host 165
 - The autopath help command 167
 - The autopath recover command. 168
 - The autopath discover command 168
 - The autopath retrieve command. 169
 - The autopath set_lbpolicy command 169
 - The autopath set_prefpath command 170
- Troubleshooting Secure Path 171
 - Recovering after failure 171
 - Secure Path messages. 171

- Glossary.173**

- Index175**

About This Guide

This installation and reference guide provides information to help you:

- Understand Secure Path technology.
- Determine hardware and software prerequisites.
- Install Secure Path software.
- Manage Secure Path.

“About this Guide” topics include:

- [Overview](#), page 10
- [Conventions](#), page 12
- [Getting help](#), page 15

Overview

This document covers the following topics:

Chapter 1 addresses Secure Path V3.0F for Active-Passive disk arrays, which includes:

- HP StorageWorks MA6000, HSG60
- HP StorageWorks RA/MA8000, HSG80
- HP StorageWorks ESA12000/EMA12000, HSG80/HSG60
- HP StorageWorks EMA16000, HSG80/HSG60
- HP StorageWorks EVA5000, HSV110
- HP StorageWorks EVA3000, HSV100

Chapter 2 addresses Secure Path V3.0F for Active-Active disk arrays, which includes:

- HP StorageWorks Disk Array XP48
- HP StorageWorks Disk Array XP128
- HP StorageWorks Disk Array XP256
- HP StorageWorks Disk Array XP512
- HP StorageWorks Disk Array XP1024
- HP StorageWorks Disk Array XP12000
- HP StorageWorks Disk Array VA7100
- HP StorageWorks Disk Array VA7400
- HP StorageWorks Disk Array VA7110
- HP StorageWorks Disk Array VA7410
- HP StorageWorks EVA8000, HSV210
- HP StorageWorks EVA4000/EVA6000, HSV200

Chapter 3 addresses Secure Path V3.0F Workgroup Edition for VA, which includes:

- HP StorageWorks Disk Array VA7100
- HP StorageWorks Disk Array VA7400
- HP StorageWorks Disk Array VA7110
- HP StorageWorks Disk Array VA7410

Intended audience

This book is intended for use by system administrators who are experienced with the following:

- Data processing and direct-access storage device subsystems and their basic functions
- Operating systems, including commands and utilities
- Any of the storage system disk arrays described in “[Overview](#)” on page 10.

Related documentation

In addition to this guide, HP provides the *HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition Release Notes*.

Conventions

Conventions consist of the following:

- Document conventions
- Text symbols
- Equipment symbols

Document conventions

This document follows the conventions in [Table 1](#).

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
<i>Italics</i>	Text emphasis and document titles in body text
Monospace font	User input, commands, code, file and directory names, and system responses (output and messages)
<i>Monospace, italic font</i>	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:



Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.



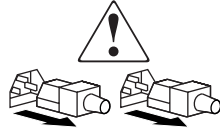
Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: <http://www.hp.com>.

HP technical support

Telephone numbers for worldwide technical support are listed on the following HP Web site: <http://www.hp.com/support/>. From this Web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage web site

The HP Web site has the latest information on this product, as well as the latest drivers. Access the storage Web site at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this Web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP Web site for locations and telephone numbers: <http://www.hp.com>.

This page has been intentionally left blank.

Secure Path Active-Passive Disk Arrays



HP StorageWorks Secure Path is a server-based software product that enhances HP StorageWorks RAID array storage systems by providing automatic path recovery from server-to-storage-system connection failures. Secure Path supports multiple I/O paths between host and storage, which improves overall data availability. If any component in a path between host and storage fails, Secure Path redirects I/O requests to an alternate path.

This chapter provides the following Secure Path information:

- [Overview, page 18](#)
- [Features, page 21](#)
- [Software components, page 22](#)
- [Secure Path for Active Passive disk arrays hardware setup, page 29](#)
- [Installing Secure Path for Active-Passive disk arrays, page 49](#)
- [Installing Secure Path on a SAN boot device, page 53](#)
- [Managing Secure Path for Active-Passive arrays, page 55](#)
- [Removing/upgrading Secure Path for Active-Passive disk arrays, page 101](#)
- [Troubleshooting Secure Path for Active-Passive disk arrays, page 106](#)

Overview

Secure Path is a high-availability software product that manages and maintains continuous data access to the following StorageWorks storage systems:

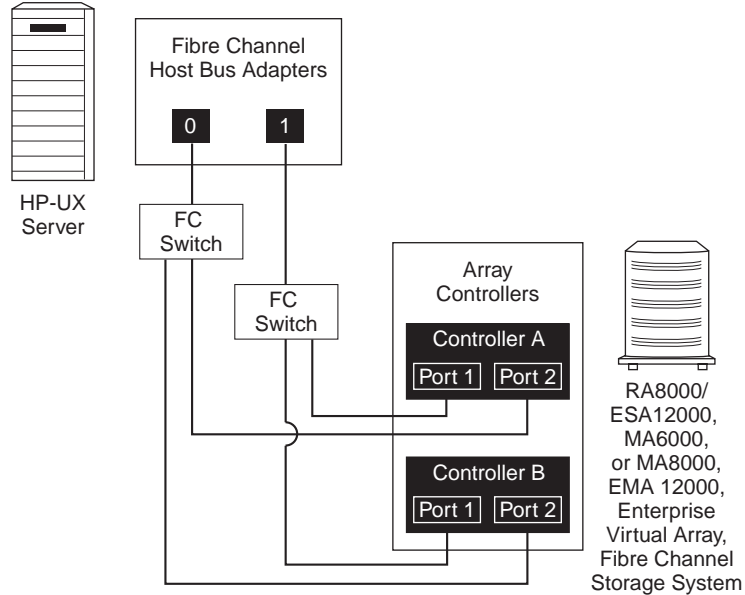
- RA8000
- ESA12000
- EMA16000
- MA6000
- MA8000
- EMA12000
- EVA5000
- EVA3000

Secure Path eliminates the RAID controller, host bus adapter (HBA), and interconnect hardware (cables, switches, and connectivity devices) as single points of failure in the storage system.

By using redundant hardware and advanced RAID technology, Secure Path enhances fault tolerance and storage system availability by providing automated failover capability.

Redundant physical connections define separate *paths* in a Secure Path hardware configuration. Each path originates at a unique HBA port on a server and ends at a unique RAID controller port in the storage system.

[Figure 1](#) on page 19 illustrates basic Secure Path hardware configurations. The physical connections define two separate paths. Each path originates at a unique storage area network (SAN) HBA on a server and ends at a port on a separate RAID controller on the storage system.



SHR-2456C

Figure 1: Basic Secure Path Fibre Channel configuration

Secure Path disk array enables dual StorageWorks RAID controllers to operate in an active/passive implementation, referred to as dual-redundant multiple-bus mode. Multiple-bus mode allows each controller to process I/O independently of the other controller under normal operation. A path consists of a unique connection from adapter to device. I/O is active on one path at a time, and access to storage units (LUNs) may be moved between paths using the Secure Path Management utility `spmgr`.

Secure Path takes advantage of preferred path unit attribute. Available storage units are preferred to one or the other of the two controllers by setting a preferred path unit attribute. This attribute determines which controller is used for access at storage system boot time. During runtime, storage units may be moved between paths at any time through the use of the Secure Path Management utility. On Active-Passive RAID storage systems, storage units may also be accessed on each controller through either of two available ports.

The Secure Path software detects the failure of I/O operations on a failed path and automatically re-routes traffic to other available paths. Secure Path software gathers alternate paths through available SAN switches, controllers, controller ports, and HBAs. Path failover is completed seamlessly, without process disruption or data loss.

Following replacement of a failed adapter, cable, controller, or attached components, storage units can be restored or failed back to their original path using the Secure Path Management utility.

To protect against drive failure in a Secure Path environment, storage units can be configured using RAID levels 0+1, 1, or 5.

Features

Secure Path for Active-Passive disk arrays provides the following features:

- Allows StorageWorks dual-controller RAID systems and host servers equipped with multiple HBAs, redundant physical connectivity along Fibre Channel SAN-switched fabric paths
- Monitors each path and automatically re-routes I/O to a functioning alternate path if an HBA, cable, switch, or controller failure occurs
- Determines the status of available storage units and physical paths through path verification diagnostics
- Monitors and identifies failed paths
- Facilitates static load balancing, which allows manual movement of devices between paths
- Automatically restores failed over storage units to repaired paths with auto failback capability enabled
- Implements anti-thrash filters to prevent failover/failback effects caused by marginal or intermittent conditions
- Exploits the potential for improved data throughput and increased bandwidth using dual RAID controllers configured in multiple-bus mode operation with load balancing capability enabled
- Detects failures reliably without inducing false or unnecessary failovers
- Implements failover/failback actions transparently without disrupting applications
- Facilitates remote management through the `spmgr` utility
- Supports fresh installation of Secure Path on the server's local disk without requiring a system reboot
- Supports configuring an EVA LUN as a system boot/swap/dump device on HP-UX 11i V1.0 and HP-UX 11i V2.0.

Software components

This section describes the software components of the Secure Path Software Kit for HP-UX.

Drivers

The following Secure Path drivers manage paths to a storage device while providing a single device target to applications.

- `swsp` driver—A failover driver that is presented as a pseudo-HBA driver to system SCSI disk drivers. This driver presents multiple paths as a single device to the host SCSI disk driver. It also initiates path failover when necessary and manages all kernel threads related to failover.
- `hsx` driver—An array-specific driver that provides paths from an HBA driver for specific arrays up to the `swsp` driver. This driver manages the separate paths to a LUN and encapsulates array-specific knowledge, such as specific commands to migrate a LUN from one controller to the other. The `hsx` driver supports HP StorageWorks HSG and HSV controllers.

[Figure 2](#) on page 23 illustrates the driver model structure.

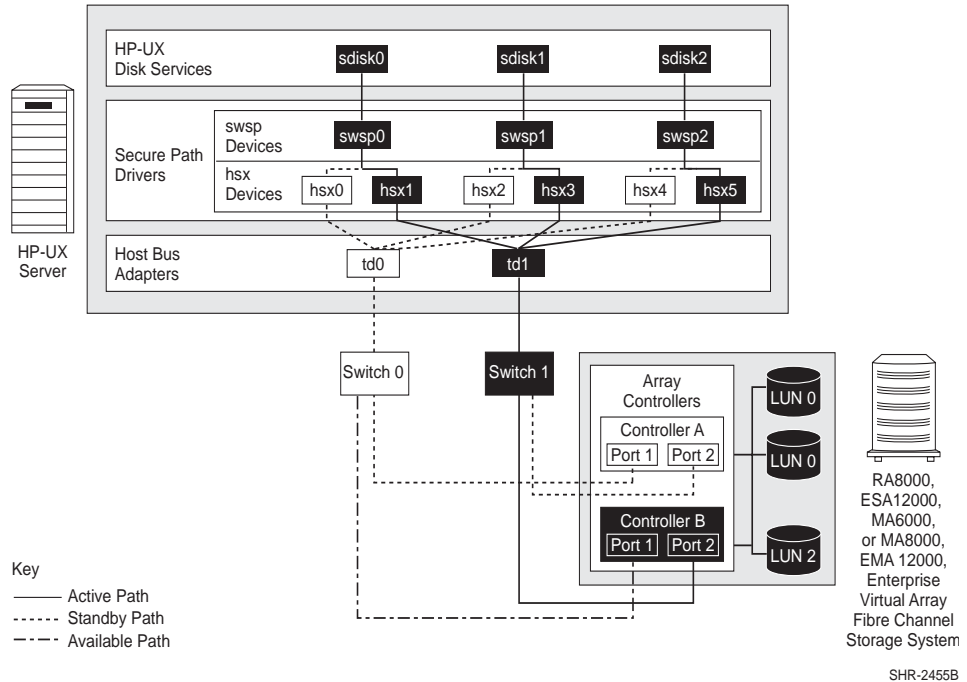


Figure 2: Driver model structure

Agent

The Secure Path agent (`spagent`) is a daemon process that provides an interface for Secure Path applications and utilities to communicate to the multipath drivers. The `spagent` daemon also provides notification of path-change events through e-mail. The `spagent` daemon is not required to be running for Secure Path drivers to provide full failover functionality. However, it must be running if e-mail event notification is desired. The only supported method to start and stop the Secure Path agent is the `spinit` script.

Management tools

The Secure Path Manager (`spmgr`) utility is a command-line application that allows you to monitor and manage Secure Path devices and to change the configuration settings of the drivers. See “[Managing Secure Path for Active-Passive arrays](#)” on page 55 for a complete description of `spmgr` commands.

The `spin` script starts and stops the Secure Path agent `/sbin/spagent`.

Controller ownership

Storage systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of the following basic operational models:

- **Active/passive**—In the active/passive model, all storage sets are assigned ownership to one controller of the pair for I/O processing. The other controller is inactive, but available as a substitute in case of a failure on the active controller.
- **Active/active**—In the active/active model, I/O processing may be routed through both controllers simultaneously, providing better performance in addition to high availability. The RAID arrays supported by Secure Path implement a modified version of the active/active model. Although I/O can be processed simultaneously by both controllers, any given storage set is *owned* or online to a host through only one controller.

Ownership of a storage set may be transferred to the other controller at any time through a host-initiated command sequence. However, because the ownership transfer results in controller cache flushing and I/O wind down, the storage set may become inaccessible for a period of several seconds. Arbitrary ownership transfers are never automatically initiated by Secure Path and should be avoided.

Note: Secure Path automatically retries I/O requests that terminate in error due to ownership transfers. Secure Path Active-Passive arrays also queues new I/O requests until the ownership transfer has completed to ensure data integrity.

Path definition

Within Secure Path, a path is defined as the collection (configuration) of physical interconnect components including HBAs, switches, cables, RAID controllers, and the ports on the controllers. Because the Secure Path driver component is positioned between the HBA driver and the system SCSI disk driver, the Secure Path driver distinguishes the physical paths when elements of the SCSI equivalent address are different.

Some configurations include multiple switches within a fabric, with the switches connected by one or more inter-switch links. Secure Path cannot detect these paths and cannot manage them. While these inter-switch paths provide an additional level of redundancy within the fabric, their management is handled directly within the switch. Refer to the documentation received with your switch hardware for more information about inter-switch link routing and failover policies.

Secure Path automatically sets the path state and reflects the status of the current active path. Because of path failures, the currently active path may be different from what you expect. See [Table 7](#) on page 59 for a list and description of path states.

Secure Path operation

Path failover occurs automatically when a selected set of error conditions is detected. Secure Path normally performs path failover only when user I/O is active or if path verification is enabled. However, it is possible for `spmgr` to show some units with a common failed path in the failover state, while other units remain accessible through that path. Units remain in the failed path if there is no I/O or until they are polled.

Failover follows a hierarchy, conditioned by the state of load balancing, as described below. Secure Path does not change the mode of preferred paths in failover situations, so you can restore original path assignments after making repairs.

- Load balancing disabled:

When a failure occurs, Secure Path marks the path failed and switches to the next available path connected to the same controller, if there is one.

If there is no available path on the same controller, Secure Path attempts to move the device to a standby path on the other controller.

- Load balancing enabled:

When a failure occurs, Secure Path marks the affected path as failed. This removes it from the list of usable paths for the storageset. If no active paths remain on the same controller, Secure Path attempts to move the device to a standby path on the other controller.

Failback options

Secure Path lets you set the path failback option to manual mode or automatic mode.

- In manual mode, you must enter a management utility command to restore devices to their preferred path. The operation is performed even if system I/O is in process to the selected device.
- In automatic mode, Secure Path tests a failed path at fixed intervals if I/O is in process for the affected device. If the path appears to be viable, the path state is set to active and I/O will again be routed through this path.

Load balancing

When enabled without selecting a policy, load balancing allows multiple paths between a host and a specific storage set to be used in a round-robin fashion. Using multiple paths spreads the load across all components in the RAID storage system and maximizes performance.

Load balancing may not be used in environments that have device reservations as a lock mechanism because the RAID array controllers enforce reservations on a per-port basis.

Load balancing requires a Fibre Channel configuration that results in at least four unique paths from the host node to the storage system. While this can be accomplished with several different physical configurations, maximum performance potential is achieved when all four ports of the RAID storage system are used.

When load balancing is enabled, the Secure Path driver causes all paths to the owning controller to be marked active by default. This is true when the following conditions occur:

- A host boots up.
- Secure Path fails over a storage set from one controller to the other.
- You manually move a selected storage set between controllers using the Secure Path management utility, `spmgr`.

Secure Path supports four types of load-balancing policies:

- Round Robin—The I/O is routed through the paths in a round-robin fashion.
- Least I/O—I/O is routed through the path which has the least amount of I/O requests.
- Least Service Time—I/O is routed through the path which has the least completion time for an I/O request.
- Least Bandwidth—I/O is routed through the path which has the least amount of bytes queued.

Path verification

When enabled with `spmgr`, path verification causes Secure Path to periodically test the availability of all paths to all storage sets for paths marked available, failed, active, or standby. Path verification does not test paths that are in a quiesced state.

Path verification is useful for detecting failures that affect overall path redundancy before they affect failover capability. If an active path fails path verification, failover occurs. If an available path fails path verification, its state will change from available to failed.

If a path marked failed passes path verification, the path state is set to available, and if auto-failback is enabled, the path becomes active. If the path is on the active controller, it is marked preferred.

Path management behavior summary

[Table 2](#) provides a summary of the path management behavior of Secure Path.

Table 2: Path management behavior summary

Feature	Behavior/Action
Startup	Chooses the preferred path to the controller to which the LUN is online. Marks the preferred path active. If no path is marked preferred, selects one and makes it the active path.
Active Path Failure	Marks the active path as failed. Redirects I/O through available path. If there are no available path, failover occurs to a standby path on the other controller.
Available or Standby Path Failure	Performs path verification. Marks failed path as failed.
Path Repaired	Marks the path available or standby, depending on which controller has the online device. If auto-failback is enabled and the path was the active path prior to the path failure, it makes the path the active path.

The `spmgr` utility may be used to customize the management of your configuration. See [“Managing Secure Path for Active-Passive arrays”](#) on page 55 for more information on `spmgr` customization.

Secure Path for Active Passive disk arrays hardware setup

This section provides the following Secure Path hardware setup information:

- [Hardware setup overview, page 29](#)
- [Installing a new Secure Path configuration, page 30](#)
- [Configuring switches, page 31](#)
- [Configuring the HSG80-based StorageWorks array, page 32](#)
- [Configuring optional HSG80-based array features, page 35](#)
- [Configuring the HSV110-based StorageWorks array, page 40](#)
- [System configuration, page 41](#)
- [Configuring SCSI-3 for HSG80-based systems, page 44](#)
- [What to do if ioscan does not see all paths to the array, page 45](#)

Hardware setup overview

The following procedure outlines the hardware setup:

1. Prior to setting up your hardware, verify the following:
 - All users have logged off the server.
 - All array file systems have been backed up and unmounted.
 - All volume groups have been exported.
2. Perform one of the following procedures:

Note: If your StorageWorks array has not been configured with your HP server, perform the procedure [“Installing a new Secure Path configuration”](#) on page 30.

- Configure SAN switches, as described on [page 31](#).
- Configure the StorageWorks RAID array, as described on [page 32](#).
- Perform system configuration, as described on [page 41](#).

Installing a new Secure Path configuration

Before connecting the StorageWorks array to your host system, perform the following steps:

1. Verify that HP-UX 11i V1.0 or 11i V2.0 is running.
2. Refer to the *HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition Release Notes* to verify that your configuration is supported.
3. Use an FC utility to determine the World Wide Name (WWN) of the Fibre Channel adapters within the server.

Note: The appropriate FC utilities are `fcmsutil` and `fcutil`.

An example of the `fcmsutil` command follows this paragraph. Use the output of this command to record the WWN of the HBAs that are connected to the array. This information is required to set up the host connection to the HSV-based array and for verification of your configuration.

```
# fcmsutil /dev/td0
```

The instance number for the HBA is `td0`. The system displays the following:

```
Vendor ID is = 0x00103c
Device ID is = 0x001028
TL Chip Revision No is = 2.3
PCI Sub-system Vendor ID is = 0x00103c
I Sub-system ID is = 0x000006
Topology = PTTOPT_FABRIC
Local N_Port_id is = 0x011500
N_Port Node World Wide Name = 0x50060b000009ce61
N_Port Port World Wide Name = 0x50060b000009ce60
Driver state = ONLINE
Hardware Path is = 0/2/0/0
Number of Assisted IOs = 59812
Number of Active Login Sessions = 2
```

In this example, record the N_Port Port World Wide Name, `50060b000009ce60`. Do this for each HBA that will be connected in the Secure Path configuration.

Perform the following steps to connect the StorageWorks array to your host system.

Note: This configuration is recommended to optimize storage component availability.

1. Connect FC cables between the FC HBAs and the ports on the HP SAN switch.
2. Connect FC cables from each HSG/HSV array controller port to the HP SAN switch.
3. Follow the procedure “[Configuring switches, page 31](#)”

Configuring switches

To configure switches:

1. Turn on the power to the SAN switches.

2. Log on to the switch.

Note: For more information, refer to the Fibre Channel SAN switch management guide that was shipped with your switch.

3. At the `switch:admin` prompt, verify that the switch is in `Fabric` mode and not in `QuickLoop` mode by entering the following command:

```
switch:admin> qlShow
```

- If the switch responds `Switch is not in QuickLoop mode`, go to [step 4](#).
- If the switch is in `QuickLoop` mode, disable `QuickLoop` mode by entering the following command:

```
switch:admin> qlDisable
```

The switch should respond by displaying the following information:

```
Setting switch to Fabric mode.  
Committing configuration...done.  
Re-enable FL_ports
```

4. Power up the StorageWorks array and follow the procedure “[Configuring the HSG80-based StorageWorks array](#)” on page 32 or “[Configuring the HSV110-based StorageWorks array](#)” on page 40.

Configuring the HSG80-based StorageWorks array

To configure the HSG80-based array:

1. Establish a terminal connection to the top controller's Command Line Interpreter (CLI) port. Refer to the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* for help in making that connection.
2. Enter the following CLI commands to see your existing array configuration:

```
HSG80> show this_controller  
HSG80> show other_controller
```

3. Determine whether your array is configured for loop or fabric connectivity. The following is a sample output of a fabric connectivity setting:

```
PORT_1_TOPOLOGY = FABRIC
```

If the port is configured for `fabric` mode, proceed to [step 5](#).

4. Configure the RA8000, MA8000, ESA12000, or EMA12000 array for fabric connectivity. Enter the following commands to set the array for SAN-switched fabric:

```
HSG80> set this_controller port_1_topology=offline
HSG80> set this_controller port_1_topology=fabric
HSG80> set other_controller port_1_topology=offline
HSG80> set other_controller port_1_topology=fabric
HSG80> set this_controller port_2_topology=offline
HSG80> set this_controller port_2_topology=fabric
HSG80> set other_controller port_2_topology=offline
HSG80> set other_controller port_2_topology=fabric
```

5. Determine whether your array is configured for transparent failover or multiple-bus mode. The following is a sample output of an array configured for transparent failover:

```
Configured for dual-redundancy with ZG80200290
In dual-redundant configuration
```

If the controllers are configured in MULTIBUS_FAILOVER mode, go to [step 8](#) on page 33.

6. Configure the RA8000, MA8000, ESA12000, or EMA12000 array for multiple-bus operation by accessing the CLI. For more information about the CLI and configuring the array, refer to the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* and the *HSG80 Array Controller CLI Reference Guide*. These documents came with your HSG80 ACS Solution Software for HP-UX Solution Software Platform Kit. Enter the following commands in order as shown:

```
HSG80> set nofailover
```

IMPORTANT: The *other* controller will shut down and must be manually restarted by momentarily pressing **reset** on the controller's front panel. Wait for two minutes for the controller to boot before proceeding. Ignore the controller `misconfigured` messages.

```
HSG80> set multibus_failover copy=this_controller
```

7. Wait two minutes for the controllers to reboot before proceeding. The controllers will restart in multiple-bus mode.
8. Verify that the array is in SCSI-2 mode by entering the following commands:

```
HSG80> show this_controller
HSG80> show other_controller
```

The following is a sample output of an array in SCSI-2 mode:

```
SCSI_VERSION      = SCSI-2
```

Note: If you are planning to use SCSI-3 mode, see [“Configuring SCSI-3 for HSG80-based systems”](#) on page 44. *The array should be in SCSI-2 mode at this point.*

9. If the array is in SCSI-2 mode and you want to ultimately use SCSI-3 mode, verify that unit D0 is unassigned. If it is assigned, delete D0 and reassign. Enter the following command:

```
HSG80> delete D0
```

Go to [step 13](#).

10. If the array is not in SCSI-2 mode, set the array to SCSI-2 mode. Enter the following command:

```
HSG80> set this_controller scsi_version=scsi-2
```

11. Restart the controllers to have SCSI-2 take effect.

```
HSG80> restart other_controller
```

```
HSG80> restart this_controller
```

Wait two minutes for the controllers to reboot before proceeding.

12. Verify that the controllers are now in SCSI-2 mode.

```
HSG80> show this_controller
```

13. Perform the following steps if this is a new factory-configured array or one that is being reconfigured. The array's internal connection table may contain connections that are out of date.

- a. Review the array's internal connection table by entering the following command:

```
HSG80> show connections
```

- b. Delete all connections to this host that are shown in the array's internal connection table. The first time the server scans the Fibre Channel bus during boot, the new connections will be registered.

- c. Delete each connection by entering the following command:

```
HSG80> delete connection_name
```

`connection_name` is one of the names listed in the array's internal connection table that was displayed when you issued the `show connections` command in [step a](#) on page 34.

14. Complete readying the array by creating storagesets and assigning LUN unit numbers, noting the following information:
 - Refer to the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* that came with your StorageWorks Solution Software Kit for details.
 - If you are reconfiguring an array set up for SCSI-2 that already had storagesets configured, you may use these units without reconfiguring as long as you are using units D0 through D7. If you are using offset LUNs, D8 through D199, you must reconfigure these units.
 - In a SCSI-3 array, you can use units D1 through D127. Units D128 through D199 must be reconfigured.
15. Select and follow procedures for “[Configuring optional HSG80-based array features](#)” on page 35 as needed. When you have completed any optional array feature, perform the procedure for “[System configuration](#)” on page 41 to configure the system for Secure Path.

Configuring optional HSG80-based array features

This section provides the following optional HSG80-based array feature setup information and procedures. The optional features include:

- [Setting up additional SCSI-2 LUNs, page 35](#)
- [Setting a preferred unit to a controller, page 38](#)
- [Using SCSI-3, page 39](#)
- [Managing the command console LUN in SCSI-2 mode, page 39](#)

Setting up additional SCSI-2 LUNs

The HP-UX `sdisk` driver allows only 8 LUNs per target. The RA8000, MA8000, ESA12000, or EMA12000 arrays normally present the LUNs as a single target. The array can be set up to present a second target of another 8 LUNs for a maximum of 16 LUNs for the array.

When deciding which configuration to use, refer to [Table 3](#).

Table 3: Target/LUNS per array comparison chart with dual fabric

Highest availability	Lower availability	Highest availability
8 LUNs/array 2 HBAs/server	16 LUNs/array 2 HBAs/server	16 LUNs/array 4 HBAs/server
4 paths/LUN	2 paths/LUN	4 paths/LUN
Load balancing (across 2 HBAs and 2 controller ports)	No load balancing	Load balancing (across 2 HBAs)

With the architecture of the RA8000, MA8000, ESA12000, or EMA12000 array, Load balancing can only be accomplished across ports of the selected controller in a redundant controller pair.

1. Complete all configuration steps described in “[Hardware setup overview](#)” on page 29.

During the boot sequence, the `ioscan` creates a connection table entry in the array. Modifications to the array's connection table enable the second target of LUNs.

2. Enter the following command for each A5158A, A6795A, or A6685A adapter:

```
# fcmsutil /dev/td#
```

3. Record the adapter's N_Port Port World Wide Name (the last 4 hex digits should suffice) on a configuration schematic.
4. Establish a CLI connection to the array and enter the following command:

```
HSG80> show connections
```

A connection table similar to the following is displayed:

```

Connection
Name      Operating system  Controller Port Address  Status Offset  Unit
!NEWCON13  HP                THIS 1      011000  OL this 0
HOST_ID=5006-0B00-0009-DB13 ADAPTER_ID=5006-0B00-0009-DB12
!NEWCON14  HP                OTHER 1      021000  OL other 0
HOST_ID=5006-0B00-0009-DB13 ADAPTER_ID=5006-0B00-0009-DB12
!NEWCON15  HP                OTHER 2      021000  OL other 0
HOST_ID=5006-0B00-0009-DD71 ADAPTER_ID=5006-0B00-0009-DD70
!NEWCON16  HP                THIS 2      011000  OL this 0
HOST_ID=5006-0B00-0009-DD71 ADAPTER_ID=5006-0B00-0009-DD70

```

In this example, you can see that the adapter -DB12 is connected to port 1 of *this* controller with a connection name of !NEWCON13 and to port 1 of *other* controller with a connection name of !NEWCON14.

The connection names are assigned by the array and can be changed for your convenience or for setting up Selective Storage Presentation for using the array as part of a SAN. For more information, refer to “Restricting Host Access” in the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide*.

5. Select two paths that you will assign to the second target on the configuration map.

Note: This assignment MUST allow each adapter to reach opposite controllers (*this* and *other*) through opposite switches.

For example, in the previous table, select either !NEWCON13 and !NEWCON15, or !NEWCON14 and !NEWCON16 .

6. Enter the following commands for the selected pair:

```
HSG80> set !newcon13 unit_offset=10
```

```
HSG80> set !newcon15 unit_offset=10
```

7. Initialize the storagesets that you want to define for the second target, using procedures found in the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide*.

8. To view all the storagesets, enter:

```
HSG80> show devices
```

Up to 8 devices should be shown as used by units D0 through D7, and your new devices should be shown as having no used by assignment.

9. Add the new devices as units D10 through (or up to) D17. For example:

```
HSG80> add unit D10 M9
```

```
HSG80> add unit D11 DISK40300
```

Keep adding devices up to a maximum of D17.

The array will now identify units D10 to D17 with a unit offset of 10, as a second target of LUNs 0 to 7.

10. Enter the following command at the server console:

```
# ioscan -fn (to see the new units)
```

```
# insf -e (to install special files for each new unit)
```

An `ioscan -fnk` now shows all new LUNs. These LUNs will be seen on only half of the original paths, and the old LUNs will be seen on the other half of the original paths.

11. If you do not see all or part of the new LUNs following the `ioscan`, follow the procedure described in [What to do if ioscan does not see all paths to the array](#), on page 45.

Note: This irregularity results from HP-UX tables that are used by the OS for maintaining accurate I/O system persistence across reboots and is not a cause for concern.

Setting a preferred unit to a controller

In multiple-bus failover mode, you can specify units to be normally selected by a specific controller of a controller pair. This process is called *preferring* and is useful in static load balancing.

Units can be preferred to one controller or the other by the `preferred_path` switch of the `ADD UNIT` or `SET UNIT` command. You must use this option of preferring a unit to a controller if you intend to use the preferred path feature in Secure Path.

For example, enter the following command to prefer unit D5 to this controller and then later set a preferred path to that unit, using the Secure Path `spmgr` utility `prefer` command:

```
HSG80> set D5 preferred_path=this_controller
```

Using SCSI-3

If you are installing Secure Path on a system that shares a StorageWorks array through a SAN that requires SCSI-3, the array must be in SCSI-3 mode. This section describes the following requirements for SCSI-3.

- Secure Path V3.0F requires the HSG80 controllers to be at ACS firmware V8.7 or later for SCSI-3 operation with extended LUN support. To enable extended LUN support, the HSG80 operating system mode parameter must be set to `HP_VSA`.
- The Command Console LUN (CCL) is required for SCSI-3, and the CCL is the first array unit (D0). This reduces the number of available LUNs by one on the HP-UX system.

Note: To facilitate a clean and understandable `ioscan` output during installation, do not enable SCSI-3 until instructed in [“System configuration”](#) on page 41.

See [“Configuring optional HSG80-based array features”](#) on page 35 if you want to configure an optional feature, or continue with [“System configuration”](#) on page 41 to configure the system for Secure Path.

Managing the command console LUN in SCSI-2 mode

The StorageWorks array is factory-configured with a virtual LUN, located on Controller A, LUN 0. This device, called the Command Console LUN (CCL), enables the array to be recognized by some host systems as soon as it is attached to the Fibre Channel switch and configured into the operating system. The CCL also serves as a communications device for the StorageWorks Command Console (SWCC) Agent. The CCL identifies itself to the host via a unique identification string. This string, `HSG80CCL`, is returned in response to the SCSI Inquiry command.

The following list describes the CLI commands that affect CLL:

- The CCL is enabled upon delivery. Determine its address by entering the following CLI command:

```
HSG80> show this_controller
```

- Disable the CCL by entering the following CLI command:

```
HSG80> set this_controller nocommand_console_lun
```

- Enable the CCL by entering the following CLI command:

```
HSG80> set this_controller command_console_lun
```

In dual-redundant controller configurations, these commands alter the setting of the CCL on both controllers.

When the CCL is enabled, its ID is the lowest-numbered available LUN. When creating storage sets and logical units on the RAID array using the CLI, the address of the CCL should be reserved to D0, and that address (D0) should not be used for a data LUN. However, if the CCL's LUN is assigned to a storage set, the CCL will float to the next-lowest LUN that is available.

Note: On HP servers running Secure Path, the floating nature of the CCL could result in unreliable unit assignments when adding or deleting units. HP strongly recommends that D0 *be left unassigned* if the CCL is required or that *the CCL is disabled* if it is not going to be used.

Configuring the HSV110-based StorageWorks array

Before beginning the configuration, collect and record the following host information:

- Host LAN name
- Host IP address
- Fibre Channel adapter World Wide Names that will be configured for Secure Path

Use a supported Web browser to access the Command View EVA management appliance.

Note: Refer to the online Command View EVA help system or the *Storage Management Appliance Element Manager for Enterprise Only Users Guide* for information on these procedures. All of these procedures need to be completed for your host to use the virtual disks.

Before your host servers can use the virtual disks, ensure that you have the following completed:

1. **Initialize the storage system and create disk groups.** When you first view the EVA from the Command View EVA software, the storage pool is presented as *un-initialized* storage. Follow documented procedures for initializing the storage system and creating disk groups.
2. **Add the host to the storage system.** Before the host can use the storage system's virtual disks, the host WWN of one HBA must be known to the storage system. Adding the host creates a path from the storage system to one host adapter.
3. **Add ports to all host adapters.** From the host properties page, use **Add Port** to add connections to the remaining HBA host adapters.
4. **Create and present virtual disks to the host.** Follow the steps for creating a virtual disk family to create the virtual disk family, create virtual disks, and present the disks to the host.

Several options are available for selecting a path preference and mode for a virtual disk. To optimize load balancing, the load should be evenly distributed between controller A and controller B. The boot default selected controller may be chosen by setting the controller `Preferred path/mode`. It is recommended that either **Path A - Failover only** or **Path B - Failover only** be used. This mode allows Secure Path to control failback to the original controller following a controller failure and replacement.

Note: **Path A - failover/failback** and **Path B - failover/failback** are not supported on Secure Path for HP-UX. That feature is designed for operating systems that cannot run Secure Path.

System configuration

To configure the system for Secure Path:

1. Power on the server and boot HP-UX.

During the boot process, device special files are created for each logical unit configured on the Active-Passive controller and are assigned to each storageset or virtual disk configured on the Active-Passive controller. Because Secure Path is not yet installed, you should see an instance of a LUN for every path to the array. For example, if you have 2 adapters, 2 switches, and 2 connections from each switch to the array, you have 4 distinct device instances (paths) to each LUN that is configured on the array.

2. Before installing Secure Path, verify that you can see all your Active-Passive storage by entering the following command:

```
# ioscan -fnk
```

If you do not see all or part of the new LUNs following the `ioscan` command, perform the procedure “[What to do if ioscan does not see all paths to the array](#)” on page 45. This anomaly results from HP-UX tables that are used by the OS to maintain accurate I/O system persistence across reboots and is not a cause for concern.

Note: The `ioscan` utility establishes the connection table on the array, and the array operating system mode parameter defaults to WINNT.

The following example shows a normal array with a single LUN:

Class	I	H/W Path	Driver	S/W State	H/W Type	Description
Ba	1	0/2	lba	CLAIMED	BUS_NEXUS	Local PCI Bus Adapter (782)
Fc	0	0/2/0/0	td	CLAIMED	INTERFACE	HP Tachyon TL/TS Fibre
Channel Mass Storage Adapter						
/dev/td0						
fc	0	0/2/0/0.1	fc	CLAIMED	INTERFACE	FCP Domain
ext_bus	7	0/2/0/0.1.18.255.0	fcpdev	CLAIMED	INTERFACE	FCP Device Interface
target	7	0/2/0/0.1.18.255.0.0	tgt	CLAIMED	DEVICE	
disk	239	0/2/0/0.1.18.255.0.0	sdisk	CLAIMED	DEVICE	DEC HSG80
/dev/dsk/c7t0d0 /dev/rdisk/c7t0d0						
ext_bus	9	0/2/0/0.1.19.255.0	fcpdev	CLAIMED	INTERFACE	FCP Device Interface
target	8	0/2/0/0.1.19.255.0.0	tgt	CLAIMED	DEVICE	
disk	241	0/2/0/0.1.19.255.0.0	sdisk	CLAIMED	DEVICE	DEC HSG80
/dev/dsk/c9t0d0 /dev/rdisk/c9t0d0						
ba	2	0/4	lba	CLAIMED	BUS_NEXUS	Local PCI Bus Adapter (782)
fc	1	0/4/0/0	td	CLAIMED	INTERFACE	HP Tachyon TL/TS Fibre
Channel Mass Storage Adapter						
/dev/td1						
fc	1	0/4/0/0.1	fc	CLAIMED	INTERFACE	FCP Domain
ext_bus	13	0/4/0/0.1.18.255.0	fcpdev	CLAIMED	INTERFACE	FCP Device Interface
target	9	0/4/0/0.1.18.255.0.0	tgt	CLAIMED	DEVICE	
disk	346	0/4/0/0.1.18.255.0.0	sdisk	CLAIMED	DEVICE	DEC HSG80
/dev/dsk/c13t0d0 /dev/rdisk/c13t0d0						
ext_bus	15	0/4/0/0.1.19.255.0	fcpdev	CLAIMED	INTERFACE	FCP Device Interface
target	10	0/4/0/0.1.19.255.0.0	tgt	CLAIMED	DEVICE	
disk	348	0/4/0/0.1.19.255.0.0	sdisk	CLAIMED	DEVICE	DEC HSG80
/dev/dsk/c15t0d0 /dev/rdisk/c15t0d0						

3. Choose one of the following options:
 - If you are using SCSI-3, proceed to “[Configuring SCSI-3 for HSG80-based systems](#)” on page 44 to continue the installation.
 - If you are using SCSI-2, proceed to “[Installing Secure Path for Active-Passive disk arrays](#)” on page 49 to continue the installation.

Configuring SCSI-3 for HSG80-based systems

1. Establish a terminal connection to the top controller’s CLI port to set the Operating System mode for each Connection Name path as shown in the following example:

```
HSG80> show connections
```

Connection Name	Operating System	Controller	Port	Address	Status	Unit	Offset
!NEWCON1	WINNT	OTHER	1	011500	OL	other	0
HOST_ID=5006-0B00-0009-CE61ADAPTER_ID=5006-0B00-0009-CE60							
!NEWCON2	WINNT	THIS	1	021500	OL	this	0
HOST_ID=5006-0B00-0009-CE61ADAPTER_ID=5006-0B00-0009-CE60							
!NEWCON3	WINNT	THIS	2	021500	OL	this	0
HOST_ID=5006-0B00-0009-D8C7ADAPTER_ID=5006-0B00-0009-D8C6							
!NEWCON4	WINNT	OTHER	2	011500	OL	other	0
HOST_ID=5006-0B00-0009-D8C7 ADAPTER_ID=5006-0B00-0009-D8C6							

2. Change the operating system mode for each path shown to HP for SCSI-2 or HP_VSA for SCSI-3. For example, enter the following set of commands:

```
HSG80> set !NEWCON1 operating_system=HP (or HP_VSA)
HSG80> set !NEWCON2 operating_system=HP (or HP_VSA)
HSG80> set !NEWCON3 operating_system=HP (or HP_VSA)
HSG80> set !NEWCON4 operating_system=HP (or HP_VSA)
```

Note: The array must be at firmware revision ACS 8.7 or later to use the SCSI-3 protocol and the HP_VSA mode.

3. Verify that all connections are now in HP mode by entering the following command:

```
HSG80> show connections
```

4. Verify that the array is in SCSI-2 mode.

```
HSG80> show this_controller
```

If you want the array in SCSI-2 mode, stop here. If you want the array in SCSI-3 mode, complete steps 5 through 7.

5. Set the array to SCSI-3 mode.

```
HSG80> set this_controller scsi_version=scsi-3
```

6. Restart the controllers to have SCSI-3 take effect.

```
HSG80> restart other_controller
```

```
HSG80> restart this_controller
```

7. Wait two minutes for the controllers to reboot before proceeding.

8. Verify that the controllers are now in SCSI-3 mode.

```
HSG80> show this_controller
```

9. Proceed to [“Installing Secure Path for Active-Passive disk arrays”](#) on page 49, to continue the installation.

What to do if `ioscan` does not see all paths to the array

If your server has been factory integrated, or if you are adding units with SCSI-2 CCL enabled, changing array unit offsets, or adding array unit offsets, `ioscan` may not see part or all of the added or changed paths. This problem is caused by

HP-UX tables that are used by the OS for maintaining accurate I/O system persistence across reboots. Enter the following series of commands to update system tables for accurate subsequent `ioscans`:

```
# fcmsutil /dev/td0 get remote all      (to obtain all Target N_Port_ids in the
                                         form 0x011200 for attached arrays)

# fcmsutil /dev/td0 replace_dsk Target N_Port_id#1
# fcmsutil /dev/td0 replace_dsk Target N_Port_id#2
...
...
# fcmsutil /dev/td0 replace_dsk Target N_Port_id#n
# fcmsutil /dev/td1 get remote all      (to obtain all Target N_Port_ids in the
                                         form 0x011200 for attached arrays)

# fcmsutil /dev/td1 replace_dsk Target N_Port_id#1
# fcmsutil /dev/td1 replace_dsk Target N_Port_id#2
...
...
# fcmsutil /dev/td1 replace_dsk Target N_Port_id#n
# fcmsutil /dev/tdn get remote all      (to obtain all Target N_Port_ids in the
                                         form 0x011200 for attached arrays)

...
...
...
# ioscan -fn
```


Installing Secure Path for Active-Passive disk arrays

The installation process installs Secure Path drivers, management utilities, and manual pages. This section provides the following procedures and information:

- [Installing Secure Path, page 49](#)
- [Installing Secure Path on a SAN boot device, page 53](#)

Installing Secure Path

The Secure Path for HP-UX Kit CD-ROM contains scripts that require administrator access to install the Secure Path depot (package). The following procedure describes how to install Secure Path software.

1. Ensure that all users have logged off the server and that all I/O from the server has ceased.
2. Back up the entire system according to normal procedures.
3. Insert the Secure Path for HP-UX CD-ROM into the CD-ROM drive.
4. Verify that the `pfs_mountd` and `pfsd` daemons are running by entering the following command:

```
# ps -ef | grep pfs
```

If these daemons are not listed, start them by entering the following commands:

```
# pfs_mountd &
```

```
# pfsd &
```

5. Mount the CD-ROM by entering a command similar to the following:

```
# pfs_mount /dev/dsk/cdrom_device_file /mnt_directory
```

Example:

```
# pfs_mount /dev/dsk/c2t1d0 /cdrom
```

In the previous example, `cdrom_device_file` is `c2t1d0` and the `mnt_directory` is `/cdrom`.

6. Change to the CD-ROM Secure Path installation directory by entering the following command:

```
# cd /cdrom
```

7. Install the Secure Path software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```

8. Select **Secure Path 3.0F for HP-UX for Active-Passive Disk Array**.

The system reboots after successful installation of Secure Path 3.0F for HP-UX for Active-Passive Disk Array.

Note: In HP-UX 11i V2.0, the following message is displayed at the end of the installation process:

```
WARNING: The currently running configuration has changes  
that are being held for next boot.
```

```
==> Do you wish to continue? y
```

```
Choose Y for this option.
```

Note: You must always use the `install.sh` script to install Secure Path. Do not use the `swinstall` command to install the Secure Path depot package.

The script checks the server for required drivers and patches before installing Secure Path. When the installation is complete, Secure Path claims the devices configured on the Active-Passive disk arrays.

In addition, the `install.sh` script does the following:

- If the installation is on the server's local disk, then the install script builds the kernel. The server is ready for use without a reboot after the installation is complete.
- If the installation is on an EVA disk, then the install script builds the kernel and reboots the server after installation. See [“Installing Secure Path on a SAN boot device”](#) on page 53 for detailed information about installation on an EVA Boot disk.

Note: At least 100 MB of free disk space is required in the `/tmp` file system.

When the installation is complete, the following occurs:

- An `ioscan` discloses new disk instances for each HSG80/HSV110 LUN configured on the server.
- Secure Path claims all units that have been presented to the host from the array and numbers them sequentially starting with target 0, LUN 0.
- Secure Path is enabled with the following default values:
 - Auto-Restore—off
 - Load Balancing—off
 - Path Verification—on
 - Verification Period—30 seconds
 - Paths preferred—none
 - Console event logging of critical messages
 - Syslog event logging of critical and warning messages
 - Mail event logging of critical, warning, and informational messages enabled to send to the root account

Use `spmgr` to customize your configuration. Refer to “[Spmgr commands](#)” on page 55 for more information on the `spmgr` utility.

Secure Path installs the following utilities:

- The Secure Path agent (`/sbin/spagent`) provides an interface for Secure Path applications to communicate with the Secure Path drivers. The `spagent` script starts after Secure Path installation and at system boot (for subsequent reboots) and must be running for `spmgr` to operate. The `spinit` script (`/sbin/init.d/spinit`) starts and stops the `spagent`.
- The Secure Path management utility (`sbin/spmgr`) displays device information, actively manages paths to each device, and sets driver options such as load balancing, path verification, and auto-restore. See “[Spmgr commands](#)” on page 55 for more information.
- The Man pages for `spmgr`, `spagent`, `spinit`, `hsx`, and `swsp`.

If you are using StorageWorks Command Console (SWCC) to manage an HSG80 environment, all devices that existed prior to the install are now hidden behind the `hsx` and `swsp` drivers, and new names are presented to the `sdisk` SCSI class driver.

Perform the following procedures to update the new device names:

1. Execute the `ioscan` command to determine the new device names.

2. Refer to the *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* and perform the following procedures:
 - a. Modify the access device with the new name.
 - b. Enable the option to start the agent during system boot.
 - c. Restart the agent.

Installing Secure Path on a SAN boot device

Features

The following are SAN Boot device features:

- Secure Path V3.0F supports SAN boot from an EVA LUN 11i V1.0 and 11i V2.0. This includes providing high availability to the SAN boot LUN. Support for the SAN boot is provided only if the root volume group is configured using Logical Volume Manager (LVM).
- Supports the Dump and Swap devices configured on an EVA LUN on 11i V1.0 and 11i V2.0.

Prerequisites

- Ensure that there are at least two paths to the active controller of the EVA disk array.
- Ensure that the connectivity to the standby controller for the EVA Boot LUN is disabled.
- Install Hardware Enablement Bundle Mar 2003 (or a later version) before installing Secure Path for 11i V1.0.

Installation steps

Use the following steps for the new installation of Secure Path on a SAN boot device:

1. Install HP-UX 11i V1.0 or 11i V2.0 on an EVA LUN.
2. Refer to the *HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition Release Notes* (part number T3549-96205) to verify that all required patches are installed.

The system reboots automatically after the patch installation.

3. Install Secure Path V3.0F.

The system reboots after the installation completes.

4. After the system comes up, determine the hardware path of the standby path for the EVA boot LUN by using the `spmgr display` and `ioscan` commands. Set the alternate boot path with this hardware path using `setboot -a hardware_path`.

Note: To install Secure Path, follow the instructions outlined in [“Installing Secure Path for Active-Passive disk arrays”](#) on page 49 or [“Removing/upgrading Secure Path for Active-Passive disk arrays”](#) on page 101. Do not use the `swinstall` command to install the Secure Path depot package.

Limitations

The following are limitations to Secure Path for HP-UX on a SAN boot device:

- `Root/Swap/Dump` are not supported with HSG LUNs.
- `Root/Swap/Dump` should be under LVM while installing HP-UX.
- `Root/Swap/Dump` should not be under VxVm configuration while installing HP-UX.
- Do not configure multiple `Swap/Dump` devices as a whole disk before installing Secure Path V3.0F.
- After the system comes up on a SAN LUN, do not run any applications before installing Secure Path.
- Uninstalling Secure Path for HP-UX is not supported on a SAN boot device.

Managing Secure Path for Active-Passive arrays

This section describes the user interface for the Secure Path for Active-Passive V3.0F Management utility `spmgr`. It includes the following topics:

- [Secure Path for Active-Passive devices, page 55](#)
- [Spmgr commands, page 55](#)
- [Spmgr common terms, page 58](#)
- [Displaying configuration information, page 59](#)
- [Path states, page 59](#)
- [The alias and unalias commands, page 77](#)
- [Setting storage system parameters, page 78](#)
- [Path management, page 83](#)
- [The add and delete commands, page 93](#)
- [Secure Path for Active-Passive remote management, page 98](#)

Note: Examples are based on the HSG80 controller, but all actions are identical for the HSV controllers.

Secure Path for Active-Passive devices

The `spmgr` utility lets you monitor and manage devices, storage systems, and paths to units that are in the Secure Path for Active-Passive configuration. It also lets you modify the configuration to repair, replace, or reconfigure devices. The `spmgr` utility relies on `spagent` to handle calls to the driver (`swsp`).

Spmgr commands

[Table 4](#) lists the `spmgr` command options. Their format and syntax are presented and described in the sections following the table.

Table 4: Spmgr commands

Command	Options / Arguments	Description
spmgr add	<i>WWLUNID</i> target LUN -r <i>WWNN</i> all	Add a new device to the Secure Path for Active-Passive configuration
spmgr alias	<i>alias_name old_name</i> no argument	Assign an alias to an object
spmgr clean	-d [<i>WWLUNID</i>] -r [<i>WWNN</i>] all	Clean device data from the Secure Path's stale device list
spmgr delete	<i>WWLUNID</i> <i>device</i> -r <i>WWNN</i> all	Removes a device from the Secure Path for Active-Passive configuration
spmgr display	-a[v] <i>adapter</i> -c[v] <i>controller_ser_num</i> -d[v] <i>device</i> -p <i>path-Instance</i> -r[v] <i>WWNN</i> -s -u no argument	Displays information about configured Secure Path for Active-Passive devices
spmgr log	-c 0, 1...3 -l 0, 1...3 -n 0, 3 no argument	Sets logging to the console, system log file, and e-mail notification
spmgr notify	add <i>severity_level</i> <i>e-mail_address</i> delete <i>e-mail_address</i> no argument	Manage e-mail address and event logging severity to each e-mail recipient
spmgr passwd		Provides security on the server side to restrict client access.
spmgr prefer	<i>path_instance</i>	Assign a preferred attribute to a path

Table 4: Spmgr commands (Continued)

Command	Options / Arguments	Description
spmgr quiesce	-a <i>adapter</i> -c <i>controller_ser_num</i> -p <i>path_instance</i>	Move I/O to an alternative object and temporarily remove selected object from use
spmgr restart	-a <i>adapter</i> -c <i>controller_ser_num</i> -p <i>path_instance</i> all	Return a previously quiesced object to an active or available state
spmgr restore	-d <i>device</i> -r <i>WWNN</i> all	Restore one or more devices to their preferred I/O path
spmgr select	-c <i>controller_ser_num</i> [-d <i>device</i>] -p <i>path_instance</i>	Select a path for I/O
spmgr set	-a on off <i>WWNN</i> -b on off rr lb li ls <i>WWNN</i> -f <i>interval</i> -p on off <i>WWNN</i>	Enable or disable special driver functionality
spmgr unalias	<i>alias_name</i> <i>old_name</i>	Delete an alias
spmgr unprefer	<i>path_instance</i>	Remove a preferred path attribute

Note: Commands entered without an argument respond with `usage` if the command is a configuration altering command. The commands `alias`, `display`, `log`, and `notify` respond with current command or configuration information.

The changes to the configuration settings performed by the following commands are persistent across system reboots and Secure Path upgrades:

- `spmgr add`

- `spmgr clean`
- `spmgr delete`
- `spmgr log`
- `spmgr prefer`
- `spmgr set`
- `spmgr unprefer`

The changes to the configuration settings performed by the following commands are persistent across system reboots but not persistent across Secure Path upgrades:

- `spmgr alias`
- `spmgr unalias`
- `spmgr notify`

Spmgr common terms

The following table describes the common `spmgr` terms. For a more complete list of Secure Path for Active-Passive terms, refer to the Glossary provided at the end of this guide.

Table 5: Spmgr common terms

Term	Definition
Device	The standard representation for a device or device link on a server. For example: <code>cXtYdZ</code> .
Logical Unit	A device that is managed by Secure Path for Active-Passive and identified by its 32-digit World Wide LUN Identifier (WWLUNID).
Adapter	The operating system ID of the HBA.
Storage System Array WWNN	A storage system is identified by its 16-digit World Wide Node Name (WWNN).
Controller serial number	The controller is identified by a unique serial number. The serial number of the HSG80 is a 10-character alphanumeric string.

Displaying configuration information

Controller states

The following table lists and describes the possible controller states.

Table 6: Controller states

Controller state	Description
Critical	A controller pair bound in multi-bus failover mode when only one of the controllers is available. The Critical state may mean a failed or offline condition because the server cannot communicate with the controller at this time.
Operational	The controller is available with a good status.
Failed	The server cannot communicate with this controller.

Path states

The following table lists and describes the path states reported by the Secure Path for Active-Passive device.

Table 7: Path states

Path state	Description
Active	The path is currently used for the I/O stream.
Available	The path is available on the active controller for the I/O stream.
Failed	The path is currently unusable for the I/O stream.
Quiesced	The path is valid, but has been made unavailable for I/O.
Standby	The path is valid on the standby controller.

Device states

The following table lists and describes device states.

Table 8: Device states

Device state	Description
Critical	Only one path remains available to the storage unit.
Degraded	One or more paths to the storage unit are failed.
Operational	All paths are available to the storage unit.
Unknown	Unable to communicate with the unit. This may indicate no available path or a failed device.
Failed	Paths are available but an inquiry to the device returns a not-ready state even after retries.

Understanding LUN/path instance numbering

When Secure Path for Active-Passive is installed or when an array is added to a configuration, Secure Path for Active-Passive numbers LUNs sequentially starting with target 0 LUN 0. This sequential numbering may not match the numbering of units on the array. For example, unit D12 on an HSG80 may have a device instance number of `c12t0d6` as seen in the `spmgr display` output. The `c12` is the next available instance number when the array was added and the `t0d6` is simply the next LUN added following `c12t0d5`.

It is possible in most cases, however, to map the device instance number back to the array unit number by using the path instance number. In most cases, the path instance target/LUN doublet is the octal equivalent of the array unit number as seen by Secure Path for Active-Passive arrays.

For example, here is a partial output of an `spmgr display` command:

```
TGT/LUN   Device      WWLUN_ID          H/W_Path          #_Paths
0/  3      c12t0d3     6000-1FE1-0016-6C30-0009-2030-2549-000A  4
                255/0.0.3

Controller Path_Instance  HBA      Preferred? Path_Status
ZG20302549
                c4t0d4          td1      no         Active
                c10t0d4         td3      no         Available

Controller Path_Instance  HBA      Preferred? Path_Status
ZG20400420
                c6t0d4          td1      no         Standby
                c8t0d4          td3      no         Standby

TGT/LUN   Device      WWLUN_ID          H/W_Path          #_Paths
0/  4      c12t0d4     6000-1FE1-0016-6C30-0009-2030-2549-000E  4
                255/0.0.4

Controller Path_Instance  HBA      Preferred? Path_Status
ZG20302549
                c4t6d3          td1      no         Active
                c10t6d3         td3      no         Available

Controller Path_Instance  HBA      Preferred? Path_Status
ZG20400420
                c6t6d3          td1      no         Standby
                c8t6d3          td3      no         Standby
```

Convert the path instance target and LUN octal value to decimal. The decimal value is the array unit or virtual disk number.

In this example, to determine the array's unit number for device `c12t0d3`, convert the path instance `c4t0d4` target/LUN octal doublet 04 to a decimal number 04. The HSG80 array's D4 has been mapped to Secure Path for Active-Passive device `c12t0d3`.

For the example's second device `c12t0d4`, the path instance `c4t6d3` yields an octal doublet 63 that converts to a decimal 51. The server, therefore, sees a unit number 51 (D51 for an HSG80) from the array.

If you are configuring an HSG80-based array, this conversion must account for unit offsets if they are used. If the unit number on the array is D25 and the unit offset is 20, the server sees a unit number of 5 (25 minus 20), and the path instance for that unit would be of the form `c#t0d5`.

If you are using an HSV110 or HSG80-based array, virtual disk numbers or unit numbers *greater* than 128/127, respectively, do not follow the above convention. For a virtual disk or unit number greater than 128, Secure Path for Active-Passive assigns a new `c` instance number, drops the most significant bit (subtracts 128), and assigns the path instance number. For example, if an HSV110 presented a virtual disk number 138 to the server, Secure Path for Active-Passive would assign a device number `cyt1d2`, where `y` is a new `c` number and `t1d2` is derived from $138 - 128 = 10$ converted to an octal 12.

Display header information

Due to the possible complexity of the Secure Path for Active-Passive configuration and the possibility of shared storage or clustered software across multiple servers, the display information always has two standard lines of information at the start of the display:

Line 1: Server: Server Name Report Created: Date and Time

Line 2: Command: Command string

Display differences between HSG and HSV controllers

All general examples in this document use the HSG80 serialization format and actual HSG80 examples. The HSG80 and HSV110 Array Controllers present objects to Secure Path for Active-Passive arrays in identical ways. Therefore, there are no differences in the way you manage settings, paths, and devices using the `spmgr` utility.

There are, however, two differences in serialization of array objects that allow you to quickly determine which type of array is being displayed. The following examples list the differences:

```
HSG80
Controller Serial Number ZG10506981
Array World Wide Node Name (WWNN) 5000-1FE1-0010-5B00
World Wide LUN ID (WWLUNID)
6000-1FE1-0010-5B00-0009-1050-6981-1234
```

```
HSV110
Controller Serial Number P4889B29LC01J
Array World Wide Node Name (WWNN) 5000-1FE1-0015-0AEO
World Wide LUN ID (WWLUNID)
6005-08B4-0001-40BF-0000-A000-1234-0000
```

Note: The location of the sequence “1234” in the WWLUNID examples is unique for each LUN and is in a different position for the array types.

The display command

This section describes the `spmgr display` commands and associated switch parameters. Each switch results in a different type of display.

Note: The verbose flag may be used with only some, but not all, cases of the command.

Syntax:

```
# spmgr display -a[v] HBA
-c[v] controller_serial_number
-d[v] device
-p path_instance
-r[v] WWNN
-s
-u
(no argument)
```


For each of these command switches, this section presents:

- Description
- Syntax
- All forms of the command
- Examples of all forms of the command
- Example displays of all forms of the command

spmgr display

When you enter the `spmgr display` command, all information for the entire configuration is displayed. The amount of information displayed depends on the number of HBAs, storage systems, and paths to a unit on each storage system.

The full display derives from the component portions described in this section. You can limit the amount of data displayed by combining the `spmgr display` command with one of the described switches.

Example:

```
# spmgr display
Server: hp.mydomain.com Report Created: Thu, Sep 13 16:11:50
2004
Command: spmgr display
=====
Storage: 5000-1FE1-0010-5B00
Load Balance: Off Auto-restore: Off

Path Verify: On      Verify Interval: 30
HBAs: td0 td1

Controller: ZG10505167, Operational
            ZG10506981, Operational

Devices: c16t0d0 c16t0d1

TGT/LUN Device WWLUN_ID H/W_Path                #_Paths
0/  0   c16t0d0 6000-1FE1-0010-5B00-0009-1050-6981-0013 4
                                0/0/255.0.0.0
```

```

Controller Path_Instance HBA Preferred? Path_Status
ZG10505167
      c4t0d0      td0      no      Standby
      c10t0d0     td0      no      Standby
Controller Path_Instance HBA Preferred? Path_Status
ZG10506981
      c5t0d0      td0      no      Active
      c11t0d0     td1      no      Available
TGT/LUN Device WWLUN_ID H/W_Path #_Paths
0/ 1 c16t0d1 6000-1FE1-0010-5B00-0009-1050-6981-0014 4
      0/0/255.0.0.1
Controller Path_Instance HBA Preferred? Path_Status
ZG10505167
      c4t0d1      td0      no      Standby
      c10t0d1     td1      no      Standby
Controller Path_Instance HBA Preferred? Path_Status
ZG10506981
      c5t0d1      td0      no      Active
      c11t0d1     td1      no      Available

```

spmgr display -a[v] *HBA*

The `-a` switch lists HBA (adapter) related information. If a parameter is supplied, it must be the adapter instance number.

Syntax:

```

# spmgr display-a
      -av
      -a HBA
      -av HBA

```

When the `-a` switch is used without a parameter, the display contains a complete list of all HBAs in the Secure Path for Active-Passive configuration from the server where the command is entered.

Example:

```
# spmgr display -a
Server: hp.mydomain.com Report Created: Thu, Sep 13 16:11:50
2004
Command: spmgr display -a
Adapters in the Secure Path
Configuration
=====
td0, td1
```

When the -a switch is paired with the v switch, the display contains a list of all adapters in the Secure Path for Active-Passive configuration. In this case, the v acts like a wildcard for the device switch, -a .

Example:

```
# spmgr display -av
Server: hp.mydomain.com Report Created: Wed, Aug 15 14:51:23
2004
Command: spmgr display -av
Adapter   Hardware Path Driver Version
=====
td0      0/2/0/0 N/A
td1      0/4/0/0 N/A
```

When invoked with the -a switch, v switch, and HBA, the display shows all paths attached to the HBA, as shown in the following example:

Example:

```
# spmgr display -av td0
Server: hp.mydomain.com Report Created: Wed, Aug 15 14:56:25
2004
Command: spmgr display -av td0
=====
Adapter: td0
Hardware Path: 0/2/0/0
Storage: 5000-1FE1-0010-5B00
0  c19t0d0 ZG10505167 td0  0/0/255.0.0.0 c14t0d0
   WWNN: 5000-1FE1-0010-5B00      Path State: Standby
1  c19t0d0 ZG10506981 td0  0/0/255.0.0.0 c15t0d0
   WWNN: 5000-1FE1-0010-5B00      Path State: Active
2  c19t0d1 ZG10505167td0  0/0/255.0.0.1 c14t0d1
   WWNN: 5000-1FE1-0010-5B00      Path State: Standby
3  c19t0d1 ZG10506981 td0  0/0/255.0.0.1   c15t0d1
   WWNN: 5000-1FE1-0010-5B00 Path State: Active
```

spmgr display -c[v] *controller_serial_number*

The `-c` switch displays controller-related information. If a parameter is supplied, it must be a controller serial number. The command has four possible forms:

Syntax:

```
# spmgr display -c
                -cv
                -c controller_serial_number
                -cv controller_serial_number
```

Example:

```
# spmgr display -c
Server: hp.mydomain.com Report Created: Thu, Sep 13 16:30:23
2004
Command: spmgr display -c
Current Controller List
=====
ZG10505167, ZG10506981
```

Example:

```
# spmgr display -cv
Server: hp.mydomain.com Report Created:Thu, Sep 13 16:30:23
2004
Command: spmgr display -cv
Controller: ZG10505167 Status: Operational
Vendor: HP
WWNN: 5000-1FE1-0010-5B00
HBAs: td0, td1
Controller: ZG10506981 Status: Operational
Vendor: HP
WWNN: 5000-1FE1-0010-5B00
HBAs: td0, td1
```

Example:

```
# spmgr display -c ZG10505167
Server:hp.mydomain.com Report Created: Thu, Sep 13 16:39:49 2004
Command: spmgr display -c ZG10505167
Controller: ZG10505167 Status: Operational
Vendor: HP
WWNN: 5000-1FE1-0010-5B00
HBAs: td0, td1
```

Example:

```
# spmgr display -cv ZG10505167
Server:hp.mydomain.com Report Created: Thu, Sep 13:16:41:17 2004
Command: spmgr display -cv ZG10505167
Controller: ZG10505167 Status: Operational
Vendor: HP
```

```
WWNN: 5000-1FE1-0010-5B00
HBAs: td0, td1
```

Item	Device	Controller	HBA	Parent	Instance
0	c16t0d0	ZG10505167	td0	0/0/255.0.0.0	c4t0d0
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
1	c16t0d0	ZG10505167	td1	0/0/255.0.0.0	c10t0d0
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
2	c16t0d1	ZG10505167	td0	0/0/255.0.0.1	c4t0d1
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
3	c16t0d1	ZG10505167	td1	0/0/255.0.0.1	c10t0d1
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
4	c16t0d2	ZG10505167	td0	0/0/255.0.0.2	c4t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
5	c16t0d2	ZG10505167	td1	0/0/255.0.0.2	c10t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	

spmgr display -d[v] *device_instance*

The -d switch displays device-related information. If a parameter is supplied, it must be a device instance.

Syntax:

```
# spmgr display    -d
                  -dv
                  -d device_instance
                  -dv device_instance
```

Example:

```
# spmgr display -d
Server:hp.mydomain.com Report Created: Thu, Sep 13 16:44:25 2004
Command: spmgr display -d
Devices by Storage System
=====
Devices: c16t0d0 c16t0d1
```

Example:

```
# spmgr display -dv
Server:hp.mydomain.com Report Created: Thu, Sep 13 16:50:04 2004
Command: spmgr display -dv
Device:          c16t0d0 Status: Operational [4 paths (2/0/2)]
Storage:         5000-1FE1-0010-5B00
LUN ID:          6000-1FE1-0010-5B00-0009-1050-6981-0013
Preferred Controller: None
HBAs: td0 td1
Device:          c16t0d1 Status: Operational [4 paths (2/0/2)]
Storage:         5000-1FE1-0010-5B00
LUN ID:          6000-1FE1-0010-5B00-0009-1050-6981-0014
Preferred Controller: None
HBAs: td0 td1
etc.
```

Note: Secure Path for Active-Passive arrays display path states using the following convention:

[total number of paths (active/failed/offline)]

“Offline” refers to the total count of standby paths and failed paths.

Actual numerical equivalents replace the text.

For example, the following attributes are displayed as [10 paths (8/0/2)]:

Total paths = 10, Active = 8, Failed = 0, Offline = 2

Example:

```
# spmgr display -d c16t0d2
Server:hp.mydomain.com Report Created: Thu, Sep 13 16:51:43 2004
Command: spmgr display -d c16t0d2
Device:      c16t0d2  Status: Operational [4 paths (2/0/2)]
Storage:     5000-1FE1-0010-5B00
LUN ID:      6000-1FE1-0010-5B00-0009-1050-6981-0015
Preferred Controller: None
HBAs: td0 td1
```

Example:

```
# spmgr display -dv c16t0d2
Server:hp.mydomain.com Report Created: Thu, Sep 13 16:51:43 2004
Command: spmgr display -d c16t0d2
Device:      c16t0d2 Status: Operational [4 paths (2/0/2)]
Storage:     5000-1FE1-0010-5B00
LUN ID:      6000-1FE1-0010-5B00-0009-1050-6981-0015
Preferred Controller: ZG10506981
HBAs: td0 td1
```

Item	Device	Controller	HBA	Parent	Instance
0	c16t0d2	ZG10505167	td0	0/0/255.0.0.2	c4t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
1	c16t0d2	ZG10506981	td0	0/0/255.0.0.2	c5t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Active [P]	
2	c16t0d2	ZG10505167	td1	0/0/255.0.0.2	c10t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Standby	
3	c16t0d2	ZG10506981	td1	0/0/255.0.0.2	c11t0d2
	WWNN: 5000-1FE1-0010-5B00			Path State: Available	

spmgr display -p *path_instance*

The `-p` switch displays storage path information. A parameter is required and it must be a path instance.

Syntax:

```
# spmgr display -p path_instance
```


Example:

```
# spmgr display -p c6t0d0
Server:hp.mydomain.com Report Created: Thu, Sep 13 12:16:14 2004
Command: spmgr display -p c6t0d0
Path:      c6t0d0                      Adapter: td0
Controller: ZG10506770 Status: Operational
Device:    c17t0d0 Status: Operational
```

spmgr display -r[v] WWNN

The `-r` switch displays storage system information. If a parameter is supplied, it must be a WWNN. The command has four possible forms:

Syntax:

```
# spmgr display -r
                    -rv
                    -r WWNN
                    -rv WWNN
```

Example:

```
spmgr display -r
Server:  hp.mydomain.com Report Created: Wed, Aug 15 15:19:38
2004
Command: spmgr display -r
Storage Systems List
=====
Storage:  5000-1FE1-0010-5B00
Storage:  5000-1FE1-0010-59F0
```

Example:

```
# spmgr display -rv
Server:  hp.mydomain.com Report Created: Wed, Aug 15 15:21:02
2004
Command: spmgr display -rv
Storage Systems List -Full
=====
Storage:  5000-1FE1-0010-5B00
Load Balance: Off  Auto-restore: Off
Path Verify: On   Verify Interval: 30
HBAs:  td0  tdl
Controller:  ZG10505167, Operational
             ZG10506981, Operational

Devices:  c19t0d0 c19t0d1 c19t0d2 c19t0d3
Storage:  5000-1FE1-0010-59F0
```

```

Load Balance: Off   Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: td0  td1

Controller: ZG10504878, Operational
            ZG10505136, Operational

Devices:  c21t0d0 c21t0d1 c21t0d2 c21t0d3 c21t0d4
          c21t0d5

etc.

```

Example:

```

# spmgr display -r 5000-1FE1-0010-59F0
Server: hp.mydomain.com Report Created: Wed, Aug 15 15:24:14
2004
Command: spmgr display -r 5000-1FE1-0010-59F0
Storage Systems List -Full
=====
Storage: 5000-1FE1-0010-59F0
Load Balance: Off   Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: td0  td1

Controller: ZG10504878, Operational
            ZG10505136, Operational

Devices:  c21t0d0 c21t0d1 c21t0d2 c21t0d3 c21t0d4 c21t0d5

```

Example:

```

# spmgr display -rv 5000-1FE1-0010-59F0
Server:hp.mydomain.com Report Created: Wed, Aug 15 15:26:49 2004
Command: spmgr display -rv 5000-1FE1-0010-59F0
Storage Systems List -Full
=====
Storage: 5000-1FE1-0010-59F0
Load Balance: Off   Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: td0  td1

Controller: ZG10504878, Operational
            ZG10505136, Operational

Devices:  c21t0d0 c21t0d1 c21t0d2 c21t0d3 c21t0d4 c21t0d5
Path Information: [P] = Preferred

Item  Device  Controller  HBAHardware Path  Instance
=====
      0  c21t0d0    ZG10504878  td0      0/0/255.1.0.0  c11t0d0

```

```

      WWNN: 5000-1FE1-0010-59F0      Path State: Standby
1  c21t0d0      ZG10505136  td0      0/0/255.1.0.0 c12t0d0
      WWNN: 5000-1FE1-0010-59F0      Path State: Active
2  c21t0d0      ZG10504878  td1      0/0/255.1.0.0 c13t0d0
      WWNN: 5000-1FE1-0010-59F0      Path State: Standby
3  c21t0d1      ZG10505136  td1      0/0/255.1.0.1 c18t0d1
      WWNN: 5000-1FE1-0010-59F0      Path State: Available
4  c21t0d1      ZG10504878  td0      0/0/255.1.0.1 c11t0d1
      WWNN: 5000-1FE1-0010-59F0      Path State: Standby
5  c21t0d1      ZG10505136  td0      0/0/255.1.0.1 c12t0d1
      WWNN: 5000-1FE1-0010-59F0      Path State: Active
6  c21t0d1      ZG10504878  td1      0/0/255.1.0.1 c13t0d1
      WWNN: 5000-1FE1-0010-59F0      Path State: Standby
7  c21t0d1      ZG10505136  td1      0/0/255.1.0.1 c18t0d1
      WWNN: 5000-1FE1-0010-59F0      Path State: Available
8  c21t0d2      ZG10504878  td0      0/0/255.1.0.2 c11t0d2
      WWNN: 5000-1FE1-0010-59F0      Path State: Standby

```

spmgr display -s

This command requires no parameter and returns a display of all undiscovered units for each storage system. This switch provides the list of units by storage system and reports the WWLUN ID for each. The information gathered by this display may be used to clean stale data from the Secure Path for Active-Passive configuration.

Example:

```
#spmgr display -s
Server:hp.mydomain.com Report Created: Wed, Aug 15 15:42:37 2004
Command: spmgr display -s
Undiscovered Units Listing
= = = = =
Storage: (fire) 5000-1FE1-0000-1290
LUN ID: 6000-1FE1-0000-1290-5000-1FE1-0000-4321
        6000-1FE1-0000-1290-5000-1FE1-0000-4334

Storage: (jazzy) 5000-1FE1-0003-4420
LUN ID: 6000-1FE1-0000-9320-5000-1FE1-9321-5733
```

spmgr display -u

This command requires no parameter and displays all unattached units for each storage system. This switch provides the list of units by storage system and reports the WWLUN ID for each. The information gathered by this display can then be used to add a unit to the Secure Path for Active-Passive configuration.

Example:

```
#spmgr display -u
Server:hp.mydomain.com Report Created: Wed, Aug 15 15:42:37
2004
Command: spmgr display -u
Unattached Units Listing
= = = = =
Storage: (fire) 5000-1FE1-0000-1290
LUN ID: 6000-1FE1-0000-1290-5000-1FE1-0000-4321
        6000-1FE1-0000-1290-5000-1FE1-0000-4334

Storage: (jazzy) 5000-1FE1-0003-4420
LUN ID: 6000-1FE1-0000-9320-5000-1FE1-9321-5733
```

The alias and unalias commands

Secure Path for Active-Passive supports the use of aliases. Aliases replace longer strings for shorter strings.

Example:

The WWNN of a storage system is 5000-1FE1-0005-3480. You can assign the alias `Bird` to replace the longer, less easy-to-remember WWNN 5000-1FE1-0005-3480.

When an alias is displayed by an `spmgr` command, the alias name is shown in parentheses before the term for which it substitutes.

Example:

```
Storage: (fire) 5000-1FE1-0001-3420
The alias is fire.
```

Alias commands:

- Define an alias and store it for future use.
- Remove an alias from the alias table.
- Display the alias table.

`spmgr alias alias_name old_name`

To add an alias to the alias table, use the following `alias` command.

Syntax:

```
# spmgr alias alias_name old_name
```

The following example creates the alias `Birdtop` for the controller serial number ZG66654211.

```
# spmgr alias Birdtop ZG66654211
```

`spmgr unalias`

To remove an alias from the alias table, invoke the `spmgr unalias` command and enter either the alias name or the old name.

Syntax:

```
# spmgr unalias old_name
                alias_name
```

In the following example, the alias, `Birdtop`, is removed from the alias table.

```
# spmgr unalias Birdtop
```

spmgr alias

Use the `spmgr alias` command to display the alias table.

Syntax:

```
# spmgr alias
```

Example:

```
# spmgr alias
Server:  hp.mydomain.com Report Created: Wed, Aug 15 15:42:37
2004

Alias:old_string

= = = = =
bob:5000-1fe1-0000-1231
jim:5000-1fe1-0000-1233
fredt:ZG111298235442
fredb:ZG238817633215
= = = = =
```

Note:

- When the `spmgr display` command is invoked, the screen output uses both the alias, if any, and the standard storage system WWNN or controller serial number. The alias will be enclosed in parentheses (*alias_name*).
 - For a command set that requires a parameter, it is assumed that the parameter or its alias may be input. Commands cannot be aliased.
-

Setting storage system parameters

The Secure Path for Active-Passive V3.0F driver has options you can enable or disable on a storage system or global basis. These options may be turned off and on dynamically. These changes occur within 45 seconds.

- The `spmgr set` command lets you enable storage system-specific settings for the Secure Path for Active-Passive device.
 - **Load balancing**—V3.0F of Secure Path for Active-Passive implements various types of load balancing algorithms to effectively use all of the available paths to a unit for I/O. The default for load balancing is disabled.
 - **Path verification**—The driver checks the state of all possible paths to all units at a selectable period or frequency. The default for path verification is enabled with a period of 30 seconds.

- **Auto-restore**—The `auto-restore` command enables the driver to automatically restore paths to their preferred path after a failure and subsequent reinstatement of that path. The default for auto-restore is disabled.
- The `spmgr log` command lets you enable logging from the Secure Path for Active-Passive device to the `syslog`, console, and e-mail notification.
- The `spmgr notify` command lets you manage the distribution of the three classes of event reports (critical, warning, and informational) via an e-mail address list.

The set command

Syntax:

```
# spmgr set -a (on | off) WWNN
             -p (on | off) WWNN
             -f verify_period
             -b (on | off) WWNN
             -b type           WWNN
```

The variable `type` is used to enable the type of load balancing. The following is the syntax for load balancing types:

```
rr - Round Robin
li - Least I/O
ls - Least Service Time
lb - Least Bandwidth
```

spmgr set -a on | off WWNN

This command enables or disables the auto-restore feature of the driver. When auto-restore is enabled, it directs the driver to monitor the state of the paths. If the preferred path should fail and then later return to service, the driver will automatically re-route all I/O to the restored path. When auto-restore is disabled, there is no auto-restore by the Secure Path driver. The I/O will continue along the current paths until another event changes the active path. The default setting is disabled (off).

Note: If you enable auto-restore using `spmgr set -a on` and select a new path using `spmgr select path`, the selected path will stay selected and will not be auto-restored. Auto-restore returns to the currently active path *only* if that path has failed and the failure has been repaired.

Note: On a server reboot, it does not matter if auto-restore is on or off, or if paths have been preferred or not. The active path comes up on the last path probed and *not necessarily on the preferred path*. An `spmgr restore all` command must be issued to restore all active paths to their preferred paths.

spmgr set -b on | off | rr | lb | li | ls *WWNN*

This command enables or disables the load balancing option of the driver. This command also allows you to set the type of load balancing algorithm to be used for path selection. The default load balancing algorithm is round robin. When load balancing is enabled, it allows I/O to be sent to the unit along all available paths per the selected algorithm. When load balancing is disabled, the I/O will be sent along the preferred path (if one is selected) or the I/O will use the first available path. The default setting is disabled (off).

spmgr set -p on | off *WWNN*

This command enables or disables the path verification of the driver. When enabled, this command verifies the state of all possible paths to all units. On large configurations with active I/O to many units, this command may reduce performance. The default setting is enabled (on).

spmgr set -f (*1...65535 seconds*)

This command sets the path verification interval. This interval can be set between 1 to 65535 seconds. The use of the `-f` switch does not change the current state of the path verification. It will only change the value for the interval. Therefore, if path verification is disabled, it remains disabled with the new interval. The default setting is 30 seconds.

The path verification interval is the same for all storagesets. The setting is retained even if all storagesets are deleted. Any new storageset added to the Secure Path configuration assumes the path verification interval that is currently set.

The log command

Syntax:

```
# spmgr log -l (level 0, 1..3)
             -c (level 0, 1..3)
             -n (level 0, 3)
```


The numerical level indicates the message severity. The levels of severity are:

1. Critical
2. Warning
3. Informational

When you select a numerical level, messages of that severity and higher are delivered to the appropriate output.

- If 3 is selected, then 3, 2, and 1 are logged.
- If 2 is selected, then 2 and 1 are logged.
- If 1 is selected, then 1 is logged.
- If 0 is selected, then logging is disabled for that item.

spmgr log -l 0, 1..3

This command sets the level of logging to the `syslog` of the server. When you select level 1..3, messages of that severity and higher are written to the `syslog` file. The default setting is 2.

spmgr log -c 0, 1..3

This command sets the level of logging to the console. When you select level 1..3, messages of that severity and higher are displayed on the console. The default setting is 1.

spmgr log -n 0, 3

This command enables or disables logging to the `notify` function. This option has two values, 0 and 3. The default setting is 3. Level 0 is provided for disabling all notification messages.

spmgr log

The `spmgr log` command displays the current logging settings.

Example:

```
# spmgr log
Server:  hp.mydomain.com  Report Created:  Wed, Aug 15 15:42:37
2004
CurrentLog Options
=====
Syslog,    enabled, level 2
```

```
Console,  disabled,level 0
Notify,   enabled,level 3
=====
```

The notify command

The `notify` command lets you manage the distribution of the three classes of event reports: critical, warning, and informational. In Secure Path for Active-Passive V3.0F, notification occurs through e-mail.

Syntax:

```
#spmgr notify add
                delete
                (no argument)
```

Severity levels

Messages from the Secure Path for Active-Passive devices are one of three severity levels:

- Critical messages are severity level 1.
- Warning messages are severity level 2.
- Informational messages are severity level 3.

`Notify` sends event notices to users from the highest to the lowest level of the severity marking as follows:

- A user with severity level 3 receives level 3, 2, and 1 severity messages.
- A user with severity level 2 receives level 2 and 1 severity messages.
- A user with severity level 1 receives severity level 1 messages only.

spmgr notify add

This command adds an e-mail address to the notification list.

Syntax:

```
# spmgr notify add severity_level e-mail_address
```

Example:

```
# spmgr notify add 3 john.doe@oscar.edu.it
```

Severity_level is 3 and the *e-mail_address* is john.doe@oscar.edu.it.

Note: A user is defined by a unique `e-mail_address`. A user with more than one `e-mail_address` may have multiple records, one for each unique address.

spmgr notify delete

This command deletes an e-mail address from the notification list.

Syntax:

```
# spmgr notify delete e-mail_address
```

Example:

```
# spmgr notify delete julie.smith@hollywood.edu
```

The `e-mail_address` is `julie.smith@hollywood`.

spmgr notify

This command displays the list of users to be notified.

Example:

```
# spmgr notify
Server: hp.mydomain.com Report Created: Wed, Aug 15 15:42:37
2004
Command: spmgr notify

Current Log Options

Severity Mode e-mail_address
=====
1 M elizabeth.bradshaw@dork.com
3 M evil.knevil@jump.net
2 M harry.houdini@magic.org
=====
```

Path management

Secure Path for Active-Passive V3.0F supports up to 32 paths to an HSG or HSV unit on a storage system. Given the very large number of paths that can be configured for a single system, the `spmgr` utility is available to manage and monitor those paths.

The path management tasks include:

- Selecting paths
- Quiescing and restarting objects and paths

The select command

A path is a combination of all the components from server to the unit on the storage system. When you describe the entire path you must identify the HBA and the controller port.

Selecting paths means to identify a path to be used for I/O. Path information, including *selected* paths, can be viewed with one or more options of the `spmgr display` command.

If the paths are selected for the duration of the server's current processing time, they are referred to as *selected paths* and are not preserved during a reboot or power cycle of the server.

Syntax:

```
spmgr select -c controller_serial_number -d device
                -p path_instance
```

`spmgr select -c controller_serial_number`

This command selects the path with the indicated controller serial number and makes that path active. For example, if there are three HBAs with paths through one controller, the Secure Path for Active-Passive device marks one path for each device from one HBA, not necessarily the same HBA. The result is to have identified selected paths for multiple units with this command.

Example:

```
# spmgr select -c ZG10505167
```

Result: The Secure Path for Active-Passive device marks each path through the controller, ZG10505167, to each unit as the selected path for I/O.

`spmgr select -c controller_serial_number -d device`

This command selects the path with the indicated controller and device and makes that path active. This command selects one controller. Therefore, the driver is able to mark one path for each device on that controller as selected. This command indicates which controller to begin selecting and which unit to end marking. Thus if there are three HBAs with paths through that controller, the Secure Path for Active-Passive device will mark one path for the device from one HBA. The overall result is to have identified selected paths for a single unit with this command.

Example:

```
# spmgr select -c ZG10505167 -d c21t0d2
```

Result: The Secure Path for Active-Passive device marks each path through the controller, ZG10505167, to unit c21t0d2 as the selected path for I/O.

`spmgr select -p path_instance`

This command selects the indicated path and makes that path active. This parameter, `path_instance`, satisfies the path equation because it contains the necessary components of HBA, controller port, and device. Therefore, no other switches or parameters are required to identify the path.

Example:

```
# spmgr select -p c18t0d1
```

Result: The Secure Path for Active-Passive device marks path c18t0d1 as the selected path for I/O.

Preferred controller

The term preferred path means that the paths are being referred to the preferred controller LUN attribute on the array.

The preferred controller LUN attribute on the array is set as follows:

- For the HSG80, use the `ADD` or `SET` command and the `preferred_path` attribute for preferring a unit to *this* or *other* controller. For example, a unit can be assigned to be preferred to *this* controller by entering the following command:

```
HSG80> SET D6 PREFERRED_PATH = THIS_CONTROLLER
```

- For the HSV110, log onto the HSV Element Manager to execute the following steps for preferring a virtual disk to controller A or controller B:
 - a. Select the virtual disk you want to modify in the Navigation pane.
 - b. Set the **Preferred Path/Mode** to **Path A-Failover Only** or **Path B-Failover Only** on the Virtual Disk Active Properties page.
 - c. Click **Save Changes** at the top of the Content pane to direct the system to process the change.

A status page is displayed indicating whether the modification was completed successfully.

- d. Click **OK**.

An updated Properties page is displayed.

The prefer and unprefer commands

On an array, each LUN may be assigned to a particular controller and be available for selection at startup. This feature is enabled by using the HSG80 or HSV110 management utilities.

Because Secure Path can have more than one path to each controller, you can further specify a preferred path. To differentiate between the controller unit attribute of preferred_path and the Secure Path preferred path, this document refers to the controller-based preferred-path attribute as the preferred controller.

The preferred path assignment lets you control setting static load balancing because the path chosen determines which adapter and controller port are designated as the default path at system startup. One preferred path can be assigned to each controller for each LUN.

For the preferred path feature to work, you must set either the preferred controller LUN attribute on the array or the preferred path attribute on Secure Path, or both the preferred controller and preferred path attributes. Examples of preferred path priority follow:

- Controller attribute priority

The preferred controller attribute has priority over the preferred path attribute. For example, if you have preferred controller A to a LUN and have also set the preferred path to that LUN as a path to controller B, a restore or reboot results in a path on controller A being selected as active.

- Controller attribute and path priority

If you have preferred controller A to a LUN and have also set the preferred path to that LUN as a path to controller A, a restore or reboot results in the preferred path on controller A being selected as active.

- Path priority

If you have no controller preferred to a LUN and have a preferred path set for that LUN, then a restore or reboot results in the preferred path being selected as active.

To set the preferred controller LUN attribute for the HSG80, use the HSG80 ADD or SET commands and the preferred-path attribute for preferring a unit to *this* or *other* controller. For example, a unit can be assigned to be preferred to *this* controller by entering the following command:

```
HSG80> SET D6 PREFERRED_PATH = THIS_CONTROLLER
```

To set the preferred controller LUN attribute for the HSV110, log on to the Command View EVA to execute the following steps for preferring a virtual disk to controller A or controller B:

1. Select the virtual disk you want to modify in the navigation pane.
2. Set the Preferred Path/Mode to **Path A-Failover Only** or **Path B-Failover Only** on the virtual disk active properties page.
3. Click **Save Changes** at the top of the Content pane to direct the system to process the change. A status page is displayed indicating whether the modification was completed successfully.
4. Click **OK**. An updated properties page is displayed.

At any time you can select a different path to be used for I/O. The selected path is not preserved for a server power cycle or operating system restart. To preserve an active path through power cycles and restarts, identify it as a preferred path. Preferred path identifications are marked by the Secure Path driver in the running system and the identifications are stored in the configuration files for that driver. Therefore, the path may be maintained permanently until removed or another preferred path is selected.

To support adding and removing preferred paths, `spmgr` provides two commands, `spmgr prefer` and `spmgr unprefer`. These two commands each require the path instance parameter.

Note: The results of these commands are stored in configuration files, and the files persist across reboots. Because these commands make dynamic changes to the driver in kernel space, `spmgr update` must be executed for the new configuration to persist across reboots. See “Secure Path persistence across reboots” on page 101.

`spmgr prefer path_instance`

This command instructs the Secure Path driver to mark a selected path as preferred. If load balance is disabled, this path becomes the active I/O path. Additionally, `spmgr` adds the specified `path_instance` to the Secure Path driver's configuration file and upon reboot of the server, the preferred paths will be restored.

Syntax:

```
# spmgr prefer path_instance
```

This command requires that the `path_instance` be supplied on the command line. The `path_instance` is provided in the `spmgr display` listings.

Example:

```
# spmgr prefer c21t0d5
```

spmgr unprefer path_instance

This command instructs the Secure Path driver to unmark the path as a preferred path. Additionally, the configuration file for the Secure Path driver is modified by removing the preferred path markings.

Syntax:

```
# spmgr unprefer path_instance
```

Example: path verification

```
# spmgr unprefer c21t0d5
```

Impact of load balancing and active paths

Preferred path and selected path are meaningless designations when you enable load balancing. Load balancing treats all paths equally and directs I/O to all available paths. In other words, load balancing is a higher priority than preferred or selected paths.

When load balancing is enabled, as a default, the Secure Path for Active-Passive device attempts to use all the available paths to a LUN in a round-robin fashion.

If load balancing is enabled and you set the path as preferred, the driver marks the path as preferred, but the path will not be used as preferred until the load balancing is turned off.

If load balancing is enabled and you select a path, the system performs the following actions:

- If the path is on the standby controller, I/O moves to the standby controller and the selected path is one of the active paths.
- If the path is on the active controller, the path continues to be used as one of the set of active paths.

This selection and marking is not preserved across reboots or power cycling.

The restore command

Once a path has failed or has been taken offline by one or more events, the `spmgr restore` command lets you restore one or more LUNS to their preferred I/O path. This command lets you manually restore all or part of a configuration when the auto-restore feature has been disabled.

A path to a device consists of an adapter (HBA) and a port on a controller (WWNN). A unit on a storage system may be seen through several paths, for example, more than one HBA and controller. The default for `spmgr restore` will transition all LUNs to their preferred controller and their adapter if they have been specified. By using one or more of the switches for this command, you have full control of restoring preferred paths to the Secure Path for Active-Passive configuration.

The use of this command assumes two important conditions:

- Paths were preferred previously. If paths to some LUNs have not been preferred, no action will be performed on those units.
- Load balancing is currently disabled. If load balancing is currently enabled, no action will be performed on any path.

Note: The `restore` command will return successfully if no restore action has been taken by the driver. For example, if the preferred path has failed and a `restore` is issued, the command will return successfully.

Syntax:

```
spmgr restore all
           -d device
           -r WWNN
```

`spmgr restore all`

Restores all LUNs to their preferred paths and/or preferred controller. If there is no preferred controller, the default will be the current controller. If there is no preferred path, the default will be the current path.

Syntax:

```
# spmgr restore all
```

Example:

```
# spmgr restore all
```

`spmgr restore -d device`

Restores a preferred path to the indicated device.

Syntax:

```
# spmgr restore -d device
```

Example:

```
# spmgr restore -d c21t0d2
```

spmgr restore -r *WWNN*

Restores a preferred path to the indicated storage system.

Syntax:

```
# spmgr restore -r WWNN
```

Example:

```
# spmgr restore -r 5000-1FE1-0010-5B00
```

The quiesce command

Quiescing an object means to:

- Move all active I/O from an object to an alternate path.
- Mark all paths to the object as quiesced to temporarily remove the object from use.

The objects that are supported for V3.0F of Secure Path for Active-Passive arrays are adapters and controllers. Also, quiescing individual paths is supported to allow other fabric infrastructures, such as switches, to be removed and replaced.

Syntax:

```
# spmgr quiesce -a HBA  
                  -c controller_serial_number  
                  -p path_instance
```

spmgr quiesce -a *HBA*

When this command is invoked, `spmgr` moves all active I/O using this HBA to paths available on other HBAs. The paths of the specified HBA are marked as quiesced and no further I/O is sent along those paths until the HBA returns to service with the corresponding `restart` command.

These actions may be verified by issuing the `# spmgr display -a HBA` command to view the current path state.

Use this feature to move I/O to another adapter as the first step to replacing an HBA.

Example:

```
# spmgr quiesce -a td0
```

`spmgr quiesce -c controller_serial_number`

When this command is invoked, `spmgr` moves all active I/O using this controller to paths on the other controller of the storage system. The paths of the specified controller are marked as quiesced and no further I/O is sent along that path until the controller returns to service with the `restart` command.

These actions may be verified by issuing the

`spmgr display -c controller_serial_number` command to view the current path states.

Use this feature to move I/O to the other controller as the first step to upgrading or replacing a controller.

Example:

```
# spmgr quiesce -c ZG11233409
```

`spmgr quiesce -p path_instance`

When this command is invoked, `spmgr` moves all active I/O using this path to another path on the same controller, if possible, or to a path on the other controller. The specified path is marked as quiesced and no further I/O is sent along that path until the `restart` command returns the path to service.

These actions may be verified by issuing the `spmgr display` command to view the current path states.

Example:

```
# spmgr quiesce -p c12t0d5
```

The restart command

Object restarting changes a quiesced adapter or controller to an available or standby state. When restarted, the HBA or controller is available as an I/O entity for a path.

Note: The `restart` command will return successfully if no restart action has been taken by the driver. For example, if a `restart` is issued to a path that is not quiesced, the command will return successfully.

Syntax:

```
# spmgr restart all
    -a HBA
    -c controller
    -p path_instance
```

spmgr restart all

When this command is invoked, `spmgr` verifies the existence of all components on quiesced paths and changes those paths to available or standby as appropriate. If the auto-restore feature is enabled and one or more of those paths are preferred paths, those paths will be made the active path.

spmgr restart -a *HBA*

When this command is invoked, `spmgr` verifies the existence of the HBA and then uses the HBA to change the state of the paths to available or standby. If the auto-restore feature is enabled and a path using that HBA is the preferred path, the path will be made the active path.

Example:

```
# spmgr restart -a td0
```

spmgr restart -c *controller*

When invoked, `spmgr` verifies the existence of the controller and then changes the state of the paths using the controller to standby. If the auto-restore feature is enabled and a path using that controller is the preferred path, then the path will be made the active path.

Example:

```
# spmgr restart -c fire-top
```

spmgr restart -p *path_instance*

When invoked, `spmgr` verifies the existence of the path and then changes the state of the path to available or standby. If the auto-restore feature is enabled and the path is the preferred path, the path will be made active.

Example:

```
# spmgr restart -p c12t0d5
```

The add and delete commands

Secure Path for Active-Passive arrays enables the dynamic addition and deletion of LUNs by using the `spmgr add` and `spmgr delete` commands.

Secure Path V3.0F for Active-Passive supports LUN addition and removal differently than V3.0. Secure Path V3.0F enables `ioscan` to claim all new storage in a manner more familiar to HP-UX system administrators. However, this change does add some steps to the `spmgr add` and `spmgr delete` commands.

The terms in [Table 9](#) have special meaning:

Table 9: Section terms

Term	Description
add	Refers to using <code>spmgr</code> to add a LUN or all LUNs of an array to the Secure Path for Active-Passive configuration.
delete	Refers to using <code>spmgr</code> to eliminate a LUN or all LUNs of an array from the Secure Path for Active-Passive configuration.
present	Refers to using the StorageWorks array utilities to add a unit or virtual disk so that the server or host can see it.
unpresent	Refers to using the StorageWorks array utilities to eliminate a unit or virtual disk so that the server or host cannot see it.

Adding LUNs

During installation, all HSG80 units and HSV110 virtual disks that are presented to the server are added and attached by Secure Path for Active-Passive arrays.

To add storage after installation:

1. Present the units or virtual disks to the storage system.
2. Run `ioscan` to add and attach the new storage.
3. Run `insf` to install and assign device files.

Note: The `spmgr add` command does not have to be used for adding new storage.

To add units or virtual disks that have been previously deleted using `spmgr delete` and are shown in the `spmgr display -u` list of unattached devices:

1. Use `spmgr add` to add the LUNs to Secure Path for Active-Passive array.
2. Run `ioscan` to claim the LUNs.
3. Run `insf` to install and assign device files.

Note: To configure a LUN under Secure Path during new LUN discovery or during the `spmgr add`, resources `c#t#d#` value and system memory must be available. If any of these resources are not available, the LUN will be in an unmapped state and will be shown as part of the unattached list. To map such LUNs and bring them under Secure Path active list, ensure that the above resources are available, and run `ioscan`.

Deleting LUNs

To unpresent a storage device or array from the Secure Path for Active-Passive configuration, use the following procedure:

1. Delete the device or array from Secure Path for Active-Passive arrays using `spmgr delete`.
2. Remove or unpresent the device from the array.

Note: If a device that has been deleted and unpresented is subsequently re-presented to the array, the device (or devices) is brought into Secure Path for Active-Passive arrays in the unattached (`spmgr display -u`) list. The Secure Path for Active-Passive device keeps track of the device deleted status as long as the server has not been rebooted.

Use the following steps to delete a LUN from the attached list of LUNs and have that device be seen as unattached using the `spmgr display -u` command:

1. Use `spmgr delete` to remove the LUN.
2. Run `ioscan` to unattach the device.

`spmgr add` *WWLUNID*

Syntax:

```
# spmgr add WWLUNID
```

WWLUNID is the World Wide LUN ID of the new unit to add on the storage system.

This command verifies the indicated unit and adds that unit to the system.

Example:

```
# spmgr add 6000-1FE1-0005-B480-0009-9341-4111-00FB
```

When invoked, the Secure Path for Active-Passive device will probe for the unit and, if it is available, add it to the data.

This command requires that you use administrative commands before and afterwards. Prior to using `spmgr add`, new array units must be found by the system and after the `spmgr add` command, units must be claimed by the system. This command sequence must be done at least once for adding single or multiple units.

Example:

```
# spmgr display -u (to identify unmapped WWLUNIDs)
# spmgr add WWLUNID1 [target LUN]
# spmgr add WWLUNID2 [target LUN]
# spmgr add WWLUNIDn [target LUN]
# ioscan -fnCdisk (for the Server to claim newly added units)
# insf -e (to install and assign device files)
```

Note: The driver settings can override the values you have supplied for the target and LUN.

#spmgr add -r *WWNN* all

This command identifies all unclaimed units for the specified array and adds them all to the Secure Path for Active-Passive configuration.

Syntax:

```
# spmgr add -r WWNN all
```

WWNN is the World Wide Node Name of the array that will have all of its units added to the Secure Path for Active-Passive configuration.

Example:

```
# spmgr add -r 5000-1FE1-000-1234 all
```

When invoked, the Secure Path for Active-Passive device will probe for all unclaimed units associated with the specified array and, if available, add them to the data. At the same time, the configuration files will be updated.

This command requires that you use administrative commands before and afterwards. Prior to using `spmgr add`, new array units must be found by the system and after the `spmgr add` command, units must be claimed by the system. This command sequence must be done at least once for adding single or multiple units.

Example:

```
# spmgr display -u (to identify the WWNN of the array with unmapped units)
# spmgr add -r WWNN all
# ioscan -fnCdisk (for the Server to claim newly added units)
# insf -e (to install and assign device files)
```

spmgr clean all

This command identifies all undiscovered units on the system and cleans the persistent data of those units from the Secure Path for Active-Passive configuration.

Syntax:

```
# spmgr clean all
```

Example:

```
# spmgr clean all
```

spmgr clean -d *WWLUNID*

This command verifies and cleans the indicated unit from the Secure Path for Active-Passive configuration.

Syntax:

```
# spmgr clean -d WWLUNID
```

Example:

```
# spmgr clean -d 6000-1FE1-0000-9320-5000-1FE1-9321-5733
```

spmgr clean -r *WWNN*

This command identifies all undiscovered units for the specified array and cleans the persistent data of those units from the Secure Path for Active-Passive configuration.

Syntax:

```
# spmgr clean -r WWNN
```

Example:

```
# spmgr clean -r 5000-1FE1-0003-4420
```

#spmgr delete *WWLUNID* | *device*

This command verifies the device and, if correct, deletes the device from the Secure Path for Active-Passive configuration. These actions occur only on the server where the command was issued. For shared storage, the unit must be deleted on each server that has access to it.

Syntax:

```
# spmgr delete WWLUNID | device
```

Example:

```
# spmgr delete fireD12
```

Alias `fireD12` is used for the `WWLUNID`.

After the delete, the following command sequence must be issued at least once to delete single or multiple units from the system.

Example:

```
# spmgr display (to identify WWLUNIDs)
# spmgr delete WWLUNID1
# spmgr delete WWLUNID2
# spmgr delete WWLUNIDn
```

Note: If the units are being unrepresented or deleted at the array, the following command does not need to be executed.

```
# ioscan -fnC disk (for the server to unclaim deleted units)
```

spmgr delete -r *WWNN* all

This command identifies all unclaimed units for the specified array and deletes them all from the Secure Path for Active-Passive configuration. This command can take up to 15 minutes to complete for the maximum number of units (256).

Syntax:

```
# spmgr delete -r WWNN all
```

WWNN is the World Wide Node Name of the array that will have all of its units deleted from the Secure Path for Active-Passive configuration.

Example:

```
# spmgr delete -r 5000-1FE1-000-1234 all
```

This command verifies the array and, if correct, will delete all of the array's devices from the configuration.

These actions occur only on the server where the command was issued. For shared storage, the unit must be deleted on each server that has access to it.

After the delete, the following command sequence must be issued at least once to delete the units from the system.

Example:

```
# spmgr display (to identify the WWNN of the array to be deleted)
# spmgr delete -r WWNN all
```

Note: If the units are being unrepresented or removed from the array, the following command does *not* need to be executed.

```
# ioscan -fnCdisk (for the server to unclaim newly deleted units)
```

#spmgr passwd

This command provides security on the server side to restrict client access.

Syntax:

```
spmgr passwd | password <newpassword>
```

Note: You cannot remotely execute the `spmgr passwd` command.

Secure Path for Active-Passive remote management

Remote management remotely executes `spmgr` commands on any other server in which Secure Path for Active-Passive disk array is installed.

Installing remote management

To install remote management, use the following steps:

1. Copy `spmgr` from the `/sbin/` directory in which Secure Path for Active-Passive resides, to the host you want to manage.
2. Add the client name using the following syntax:

```
spmgr client add client_name
```

The *client_name* is the name of the client host that will be managed by Secure Path for Active-Passive arrays. For example:

```
# spmgr client add xyz.hp.com
```

The `client add` command enables the remote client to communicate with the server in which Secure Path for Active-Passive array is installed and is to be managed.

Removing a client from a server

Remove a client as follows:

Delete the client name with the following syntax:

```
spmgr client delete client_name
```

The *client_name* is the name of the client host to be deleted from where Secure Path for Active-Passive is managed. For example:

```
# spmgr client delete xyz.hp.com
```

The `client delete` command disables the remote client communicating with the server in which Secure Path for Active-Passive array is installed and managed.

The previous commands need to be executed at the server in which Secure Path for Active-Passive array is installed and is to be managed.

Remote spmgr execution

To execute remote management, use the following syntax:

```
spmgr remote_host:command_name
```

Example:

```
# spmgr xyz.hp.com:display
```

The `spmgr remote_host:command_name` command executes the desired command on the system where Secure Path for Active-Passive array is installed and displays information on the remotely managed host.

The following commands can be executed remotely:

- add
- clean
- delete
- display
- log
- prefer
- quiesce
- restart
- restore
- select
- set
- unprefer

The following commands cannot be executed remotely:

- alias
- unalias
- notify
- passwd
- client

Removing/upgrading Secure Path for Active-Passive disk arrays

This section describes how to remove and/or upgrade Secure Path software and includes the following sections:

- [Removing Secure Path, page 101](#)
- [Upgrading Secure Path software, page 101](#)
 - [Upgrade requirements, page 102](#)
 - [Upgrade preparation, page 102](#)
 - [Upgrading from the Web, page 104](#)

Removing Secure Path

Removing the Secure Path software restores the server to a single-path, RAID storage environment. Under a single-path configuration, the HSG80 controllers must be set into transparent failover mode. Consult your *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* for details.

Secure Path can be removed using HP's SD utility or the System Administration Manager (SAM). When you remove Secure Path, all files, including configuration files, are removed. You can use SAM or enter:

```
# swremove -x autoreboot=true CPQswsp,r=*
```

Note: After Secure Path is removed, you must reconfigure the array for transparent failover mode. Refer to your *HSG80 ACS Solution Software for HP-UX Installation and Configuration Guide* for details. If Secure Path is installed on a SAN boot device (EVA LUN), refer to Secure Path Boot Device (EVA LUN) for further details.

Upgrading Secure Path software

This section describes the requirements and procedures to upgrade Secure Path software.

Upgrade requirements

The following requirements must be met to ensure a successful installation:

- At least 100 MB of free disk space is required in the `/tmp` file system for installation.
- The upgrade requires an additional 10 MB of space in `/usr` and 10 MB in `/opt`.

Upgrade preparation

Secure Path V3.0F does not support HSG80 array controllers using ACS V8.6 in SCSI-3 mode. It does continue to support ACS V8.6 or later in SCSI-2 mode. Since V3.0F with ACS V8.7 or later enables the support of up to 127 LUNs per array, HP recommends that you configure the array for SCSI-3 operation.

If you are upgrading an existing Secure Path V3.0 configuration and are adding Enterprise Virtual Array systems to the configuration, perform the upgrade on the existing HSG80-based storage first. Then add the HSV110-based storage using the hardware setup described in “[Secure Path for Active Passive disk arrays hardware setup](#)” on page 29 once the Secure Path V3.0F upgrade is complete and verified.

This procedure will not change your existing StorageWorks device file assignment or modify any existing logical volumes. It will add and attach all new or unattached LUNs that can be seen by your server, and depending on the existing target/LUN numbering, can add these devices in non-sequential order.

Use the following steps to add and attach all new or unattached LUNs:

1. Verify that your server and storage configuration meets the software, patch, firmware, and hardware revision levels defined in the *Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition* release notes (part number T3549-96205).
2. Ensure all users have logged off the server and that all I/O from the server has ceased.
3. Perform a complete system backup according to your normal procedures, and document your server file systems, mount points, and device files.

4. Choose a SCSI option:
 - If you want to continue to use SCSI-2 and ACS V8.6 or later, proceed to [“Upgrading from the Web”](#) on page 104.
 - If you are using SCSI-2 and want to use SCSI-3, you must first change the array in SCSI-3 mode. Use the procedure in the section titled [“Using SCSI-3”](#) on page 39 to change to SCSI-3.

Keep the following in mind:

 - Secure Path V3.0F requires ACS V8.7 or later for use with SCSI-3 mode. Upgrade the HSG80 controllers to ACS V8.7 or later using the instructions supplied in the Platform Kit’s Maintenance and Service Guide.
 - The rolling upgrade method that upgrades ACS 8.7-3 to ACS 8.8 (described in the *Maintenance and Service Guide for Solution Software V8.8 for HP-UX*) fails if the server is running application I/O to the array being upgraded. You must quiesce all I/O to the array before starting the rolling upgrade procedure.
5. Change the HSG80 operating system mode from HP to HP_VSA using the array’s CLI interface (ACS 8.7 or later):

```
HSG80> show connections
```

A connection table similar to the following is displayed:

Connection	Unit					
Name	Operating system	Controller	Port	Address	Status	Offset
!NEWCON13	HP OTHER	1	offline	0		
	HOST_ID=5006-0B00-0009-CE61	ADAPTER_ID=5006-0B00-0009-CE60				
!NEWCON14	HP OTHER	2	offline	0		
	HOST_ID=5006-0B00-0009-D8C7	ADAPTER_ID=5006-0B00-0009-D8C6				
!NEWCON15	HP THIS	1	offline	0		
	HOST_ID=5006-0B00-0009-CE61	ADAPTER_ID=5006-0B00-0009-CE60				
!NEWCON16	HP THIS	2	offline	0		
	HOST_ID=5006-0B00-0009-D8C7	ADAPTER_ID=5006-0B00-0009-D8C6				

- Using the connection names for the server to be upgraded, change the operating system mode with the following commands:

```
HSG80> set !NEWCON13 operating_system=hp_vsa
HSG80> set !NEWCON14 operating_system=hp_vsa
HSG80> set !NEWCON15 operating_system=hp_vsa
HSG80> set !NEWCON16 operating_system=hp_vsa
```

- Verify the change by issuing another `show connections` command. The resulting output should look similar to the following:

```
HSG80> show connections
Connection      Unit
  Name          Operating system Controller Port Address Status Offset
!NEWCON13      HP_VSAOTHER      1 offline 0
                HOST_ID=5006-0B00-0009-CE61 ADAPTER_ID=5006-0B00-0009-CE60
!NEWCON14      HP_VSAOTHER      2 offline 0
                HOST_ID=5006-0B00-0009-D8C7 ADAPTER_ID=5006-0B00-0009-D8C6
!NEWCON15      HP_VSA THIS      1offline 0
                HOST_ID=5006-0B00-0009-CE61 ADAPTER_ID=5006-0B00-0009-CE60
!NEWCON16      HP_VSA THIS      2offline 0
                HOST_ID=5006-0B00-0009-D8C7 ADAPTER_ID=5006-0B00-0009-D8C6
```

Upgrading from the Web

Access the upgrade package at

<http://www.hp.com/country/us/eng/prodserv/storage.html>

This package is intended as an upgrade only. The patch depot upgrades only Secure Path V3.0A, V3.0 SP1, V3.0B, V3.0B SP1, V3.0C, or V3.0D to V3.0F. Therefore, one of these revisions must have been installed for the upgrade to succeed.

- Copy the upgrade tar package to a temporary directory (for example, `/tmp/CPQswsp`).
- Unbundle the upgrade files by entering the following commands:

```
# cd /tmp/Securepath
# tar xvf sp_v30F_hp_web.tar
```

Verify that the directory contains the installation script `install.sh` and the following patch depots:

- `HPswsp_v30F`

- CPQswsp_v30F
3. Install Secure Path software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```
 4. Select **Secure Path Ver 3.0F for HP-UX for Active-Passive class of Disk Arrays** when prompted. Follow the on-screen instructions.

When the installation is complete and the server reboots, a subsequent `swlist` displays the following Secure Path output:

```
#  
# Product(s) not contained in a Bundle  
  
CPQswsp A.3.0F.00F.00F HP StorageWorks Secure Path Device  
Driver, utilities, and upgrade patch for Active-Passive class of  
Disk Arrays.
```

Note: If you are using SCSI-2 protocol, the LUNs you see after the upgrade are the same ones you configured before the upgrade. If you are using SCSI-3 or are changing from SCSI-2 to SCSI-3, the LUNs you see after the upgrade are the ones you configured before the upgrade, followed by all LUNs (up to 127 LUNs) that the server can see and claim for the array.

Troubleshooting Secure Path for Active-Passive disk arrays

Troubleshooting can be performed by you or an HP service representative in accordance with your HP service contract. If you are unable to resolve an error condition, ask your HP service representative for assistance.

[Table 10](#) on page 107 lists Secure Path events, sample user notification messages, and sample `syslog` messages.

Table 10: Secure Path event messages

Event description	User notification messages	Syslog messages
Occurs when array settings (such as load balancing, path verification, path verification period, auto-restore) are changed and there is a failure to update the persistent data of array settings in the kernel.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to update the persistent data for the Array 50001FE150003440. This may result in the loss of Secure Path configuration settings for this Array across system reboots
Occurs when there is a failure in retrieving the persistent data of an array (like load balancing, path verification, path verification period, auto-restore) during boot.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to update the persistent data for the Array 50001FE150003440. This may result in the change of c#t#d# values of the LUNs configured on this Array across system reboots

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Occurs when you add LUNs using <code>spmgr add</code> or when you present new LUNs at the array after you run <code>ioscan</code> , and if there is a failure in updating the persistent data of the Secure Path Virtual LUN in the kernel.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to update the persistent data for the LUN 600508B40001492000016000005B0000. This may result in the change of c#t#d# value of this LUN across system reboots
Occurs when the log settings are changed (such as <code>syslog</code> , <code>console</code> , and <code>notify</code>) and there is a failure to update the persistent data of these settings in the kernel.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to update the persistent data for the <code>syslog</code> setting. This may result in the loss of Secure Path log level settings across system reboots

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Occurs when there is a failure to retrieve the persistent data of an array (like load balancing, path verification, path verification period, auto-restore) or a failure while retrieving the persistent data of the swsp interface nodes of the array.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve the persistent data for the Array 50001FE150003440. This may result in loss of Secure Path configuration settings for this Array. Also this may result in the change of c#t#d# values of the LUNs configured on this Array
Occurs when there is a failure in retrieving the persistent data of an array (like load balance, path verification, path verification period, auto-restore) during boot.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve the persistent data for the Array 50001FE150003440. This may result in loss of Secure Path configuration settings for this Array

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Occurs when there is a failure to retrieve the persistent data of the swsp interface nodes of the array during boot.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve the persistent data for the Array 50001FE150003440. This may result in the change of c#t#d# values of the LUNs configured on this Array. Ignore this message if all the LUNs of this Array are deleted
Occurs when there is a failure retrieving the persistent data of the LUN during boot.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve the persistent data for the LUN 600508B4000149200001 6000005B0000. The LUN will be in unmapped state till it is configured using 'spmgr add' followed by 'ioscan'

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Indicates there is a failure in setting/retrieving the persistent data in kernel.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots.	CPQswsp: Persistence error. Cause: Insufficient system memory. Failed to retrieve/update the persistent data. May result in change/loss of Secure Path configuration/device settings across system reboots
Occurs when all the paths to the LUN have failed.	All paths for Target/LUN 0/2 (WWID=600508B4000149200001600000C00000) on Controller P4889B49IM failed.	WARNING: CPQswsp: All paths for Target/LUN 0/2 (WWID=600508B40001490C0001A00001E20000) on Controller P4889B49IM failed
Occurs when a new LUN is added or a quiesced LUN is restored to Secure Path.	Availability for LUN 600508B40001490C0001A00001E20000 changed to Alive.	CPQswsp: Availability for LUN 600508B40001490C0001A00001E20000 changed to Alive
Occurs when the path to the end LUN has failed.	Path c42t0d2 Failed (LUN 600508B40001490C0001A00001E20000 Controller P4889B49IM Array.	CPQswsp: Path c42t0d2 Failed (LUN 600508B40001490C0001A00001E20000 Controller P4889B49IM Array 50001FE100150AE0 HBA td3)
Occurs when a path to the end LUN has either quiesced the controller/ HBA connecting to that LUN, or LUN has failed.	Availability for LUN 600508B40001490C0001A00001E20000 changed to Dead.	WARNING: CPQswsp: Availability for LUN 600508B40001490C0001A00001E20000 changed to Dead

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Occurs when <code>ioscan</code> is executed in parallel to the <code>spmgr delete</code> command.		CPQswsp: Aborting scanning of Secure Path devices due to other outstanding Secure Path operations. Please reissue <code>ioscan</code> command to scan Secure Path devices
Occurs when there is are no free <code>c##d#</code> values available for mapping the LUN.		CPQswsp: Mapping error. Cause: No free <code>c##d#</code> available for mapping for the unit 600508B40001492000016000005B0000. The unit will be kept in the unattached list. To map this unit, clean up any stale undiscovered units present using ' <code>spmgr clean [option]</code> ' and run <code>ioscan</code>
Occurs when there is a failure in allocating memory required for the <code>swsp</code> node creation.		CPQswsp: Allocation error. Cause: Failed to allocate memory for the ' <code>swsp</code> ' node of the unit 600508B40001492000016000005B0000. The unit will be kept in the unattached list. To map this unit, free up memory and run <code>ioscan</code>

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
Occurs usually when the unit which was deleted in the previous boot using the <code>spmgr delete</code> command is not discovered during boot scan of this session.		CPQswsp: The unit 600508B40001492000016000005B0000 is not discovered and not associated with any of the discovered Arrays. So the persistent data of this unit will be deleted
Occurs when there is an error in reading the persistent data of the LUN and which resulted in associating this LUN's persistent data with the wrong array.		CPQswsp: Mapping error. Cause: Error in reading the persistent data in the previous boots. This will result in the change of c#t#d# value of the LUN 600508B40001492000016000005B0000
Occurs when there is an error reading the persistent data of the interface node of the array in the previous boots and thus allowing some other interface node to get the same h/w address value. In the subsequent boot, if the first interface node's persistent data is read properly, then there is more than one interface node having the same h/w address value, which results in duplicate entries.		CPQswsp: Mapping error. Cause: Due to error in reading the persistent data in the previous boots, there are duplicate entries for the swsp h/w address 2. This may result in the change of c#t#d# values of the LUNs configured for the above h/w address on the Array 50001FE150003440

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
<p>Occurs when there is an error reading the persistent data of the LUN in the previous boots and thus allowing some other LUN to get the same c##t##d## value. In the subsequent boot, if the first LUN's persistent data is read properly, then there is more than one LUN having the same c##t##d## value, which results in duplicate entries.</p>		<p>CPQswsp: Mapping error. Cause: Due to error in reading the persistent data in the previous boots, there are duplicate entries for the mapping data of hw_addr 2, target 1, lun 0. This may result in the change of c##t##d## value of the LUN 600508B40001492000016000005B0000</p>
<p>Occurs when the spmgr delete command is executed on an EVA LUN which is configured as the system dump device (for HP-UX 11iV2.0 only).</p>		<p>CPQswsp: spmgr delete Operation Error. Cause: 600508B40001492000016000005B0000 not deleted, is a dump device</p>

Table 10: Secure Path event messages (Continued)

Event description	User notification messages	Syslog messages
<p>Occurs when a device is unrepresented before deleting the device with the <code>spmgr delete</code> command, and you add new device with the same virtual disk or unit number as the old device, as the new device is bound to the WWLUNID of the old deleted device. This leaves the newly added LUN in an inconsistent state.</p>		<p>Multiple luns [lun: <WWLUNID> & lun: <WWLUNID>] present at target/lun [target]/[lun] on array <array WWN>. To obtain proper data ensure the c#t#d# at the specified target and lun is not busy/mounted and Run <code>ioscan & insf -e</code> respectively.</p> <p>Note: This message appears only if you have enabled the path polling.</p>

Table 11 defines the way that an event, such as a failure or state change, is reported to the server through the Secure Path driver (`hscx`) or agent (`spagent`). The Response Action column shows where the event is logged. LOG is the `/var/adm/syslog/syslog.log` file, CONSOLE is the root console, and NOTIFY is e-mail notification. The Level column indicates the criticality of the event and is used by `spmgr` to allow the system administrator to route events to specific users.

Table 11: Responses and severity level for supported events

Event	Response action	Level
Path failed	LOG+CONSOLE+NOTIFY	WARNING
Failover condition detected	LOG+CONSOLE+NOTIFY	CRITICAL
Failover start	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Failover complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore start	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore failed	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Excessive restores	LOG+CONSOLE+NOTIFY	WARNING - Auto-Restore has been disabled until next time quantum (1 hour)
Availability changed	LOG+CONSOLE+NOTIFY	CRITICAL
Select start	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Select complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Select failed	LOG+CONSOLE+NOTIFY	WARNING
Unit attention	LOG	INFORMATIONAL
Secure Path started	LOG+CONSOLE	INFORMATIONAL
Configuration change	LOG +CONSOLE+NOTIFY	INFORMATIONAL
Active path changed	LOG+CONSOLE+NOTIFY	INFORMATIONAL
New LUN added	LOG+CONSOLE+NOTIFY	INFORMATIONAL
New path added	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Path verification On/Off changed	LOG	INFORMATIONAL

Secure Path for Active-Active Disk Arrays

2

HP StorageWorks Secure Path V3.0F for Active-Active disk arrays provides automatic I/O path failover, failback, recovery, and load balancing for host systems configured with multiple host adapters and connections to disk arrays.

This chapter provides the following Secure Path information:

- [Features](#), page 118
- [ULM services](#), page 119
- [Dynamic load balancing](#), page 120
- [Automatic failover](#), page 121
- [Automatic path recovery](#), page 122
- [Online device discovery](#), page 123
- [Installation](#), page 125
- [Secure Path SAN boot setup for Active-Active devices](#), page 126
- [Upgrading from the Web](#), page 127
- [Uninstalling Secure Path](#), page 128
- [Command line interface](#), page 129
- [Troubleshooting Secure Path](#), page 143

Features

Secure Path provides enhanced data availability with these features:

- Automatic path failover to an alternate path
- Automatic path recovery after failed path is serviced
- Automatic failback when a path recovers from failure
- Dynamic load balancing over multiple paths
- Command-line user interface (CLI) for Secure Path management
- Ability to reestablish previous load-balancing policy after reboot through the CLI
- Ability to discover the SAN configuration changes (such as addition/deletion of devices/paths) without rebooting
- SAN boot support for Secure Path Active-Active devices
- Supports upto 32 paths to an end LUN

The HP StorageWorks Secure Path software performs dynamic load balancing of data flow through multiple paths. It detects multiple paths to each logical device and distributes the data load among the paths for optimum performance.

The user interface lets a system administrator define load-balancing policies and preferred paths, and view device path information. Secure Path manages paths according to the balancing policy, ensuring that no single path is a performance bottleneck.

ULM services

The SCSI Upper Layer Module (ULM) interface is used by Secure Path to provide flexible configuration and layering of modules above the SCSI disk drivers. For Secure Path to be configured into HP-UX 11i V1.0 64-bit operating systems (and coexist with other pseudo drivers), Secure Path must register itself with the ULM services for each LUN path that it wants to control.

Dynamic load balancing

Secure Path performs dynamic load balancing while monitoring each path to ensure that the I/O transaction is completed. The load-balancing policy is selected by the administrator.

The dynamic load-balancing policy prevents any path from becoming overloaded, and it helps to prevent the congestion that occurs when many I/O operations are directed to common devices along the same path.

If a preferred path is used for a device, the entire I/O for that particular device flows through the preferred path and no load balancing is done by Secure Path for that device.

VA disk arrays

Increased performance is not always realized with Virtual Array (VA) systems. In most cases, the best performance is provided by using preferred paths.

Automatic failover

In the event of a failure of any part of a path between the disk array and a server, Secure Path automatically switches to an alternate path, dropping the failed path out of the I/O rotation without any loss of data. The failover is not visible to applications, so normal operation continues without downtime.

For troubleshooting information, see “[Troubleshooting Secure Path](#)” on page 143.

Automatic path recovery

When a path fails, it is no longer used. After the path has been repaired and returned to normal, Secure Path automatically begins using the path with the designated load-balancing policy. No user action is necessary.

Online device discovery

If there were any changes in the SAN configuration such as addition and deletion of paths or devices, these changes can be updated in Secure Path for Active-Active arrays for maximum and efficient utilization of resources. The `autopath discover` command updates the SAN configuration changes to the list of Secure Path for Active-Active devices without a system reboot, and the `autopath delete` command removes a device from autopath control.

Note: Discovery of new Paths or LUNs is effective only if you execute `ioscan` and `insf -e` before executing the `autopath discover` command.

System requirements

To install Secure Path the system must conform to these requirements:

- HP-UX 11i V1.0 or 11i V2.0 64-bit operating system
- Administrator `root` access to the host system
- SCSI ULM Services B.11.11.01 for HP-UX 11i V1.0

For specific installation requirements for your system, contact your HP account representative.

Note: Refer to the *HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition Release Notes* for details about the supported configuration.

Installation

This section describes the procedures for installing Secure Path. You must have root account privileges to install Secure Path software. Your HP account representative can assist you in determining the supported configurations for your system.

Installing Secure Path software

Before installing Secure Path on HP-UX 11i, V1.0 ensure that SCSI ULM services is installed on the system.

To install Secure Path, you must have superuser (`root`) access on the HP-UX host.

Note: If AutoPath V2.x is installed, Secure Path V3.0F for Active-Active array uninstalls AutoPath V2.x, installs V3.0F, and then reboots. A single reboot will bring up the system with Secure Path V3.0F for Active-Active disk array.

Use the following steps to install Secure Path:

1. Log on to the HP-UX system as superuser (`root`).
2. Insert the Secure Path installation CD-ROM into the CD-ROM drive.
3. Mount the CD-ROM on your file system.
4. Change to the directory in which the CD-ROM is mounted. For example, if the CD-ROM is mounted to a directory called `/cdrom`, change the directory by entering the following command:

```
# cd /cdrom/
```

5. Install Secure Path software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```
6. Select **Secure Path V3.0F for HP-UX for Active-Active Disk Arrays** when prompted. Follow the instructions on the screen.

When the installation is complete, the server reboots (HP-UX 11iv1.0 only). Installation of the Secure Path package creates `/Autopath` and `/HPswsp` directory under `/opt` directory. The `changes.log` file is copied into `/Autopath` directory, and the `master`, `system`, and `mod.o` files are copied into `/HPswsp` directory.

Secure Path SAN boot setup for Active-Active devices

Use the following procedure for the Secure Path SAN Boot setup sequence:

1. Install HP-UX OS 11i V1.0 or 11i V2.0 on the Active-Active disk array LUN and boot the system.
2. Install Secure Path on the Boot LUN.
3. Configure LVM with alternate physical volume paths to the primary boot volume path.
4. Use the `vgextend` command to record alternate paths to the primary boot volume path.

```
# vgextend /dev/vg00 alternate_physical_device_path
```

Example:

```
# vgextend /dev/vg00 /dev/dsk/c14t0d1 /dev/dsk/c16t0d1  
/dev/dsk/c18t0d1
```

The `vgextend` command extends root volume with alternate paths.

5. Use the `setboot` command to modify the boot variables and to set alternate paths to the boot LUN.

```
# setboot -a hw_path_of_alternate_boot_path
```

Example:

```
# setboot -a 0/0/2/0.2.1
```

Upgrading from the Web

Access the upgrade package at:

<http://www.hp.com/country/us/eng/prodserv/storage.html>

This package is intended as an upgrade only. The patch depot upgrades AutoPath V2.xx.xx or Secure Path V3.0x to Secure Path V3.0F.

1. Copy the upgrade tar package to a temporary directory (for example, /tmp/HPswsp).

2. Unbundle the upgrade files by entering the following commands:

```
# cd /tmp/Securepath
# tar xvf sp_v30F_hp_web.tar
```

3. Verify that the directory contains the installation script `install.sh` and the following directories:

- HPswsp_v30F
- CPQswsp_v30F

4. Install Secure Path software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```

5. Select **Secure Path V3.0F for HP-UX for Active-Active Disk Arrays** when prompted. Follow the on-screen instructions.

When the installation is complete and the server reboots, a subsequent `swlist` displays the following Secure Path output:

```
#
# Product(s) not contained in a Bundle
HPswsp A.3.0F.00F.00F HP StorageWorks Secure Path Device
Driver and utilities for Active-Active Disk Arrays.
```

Uninstalling Secure Path

Secure Path can be removed using the HP SD utility. When you remove Secure Path, all files, including configuration files, will be removed.

Use the following steps to uninstall Secure Path:

1. Log on to the HP-UX system as superuser (`root`).
2. From the command line, execute the `swremove` command as follows:

```
# swremove -x autoreboot=true HPswsp
```

3. You can also launch the interactive session of `swremove` and select the **HPswsp HP StorageWorks Secure Path Driver and Utilities for Active-Active Disk Arrays** product for removal.

The system reboots after removal is complete (HP-UX 11i v1.0 only).

Command line interface

The Secure Path command line interface (CLI) can be used only on hosts connected to devices with the HPswsp driver installed. The commands supported by this interface and the syntax are described in the following topics:

- [The autopath delete command](#), page 129
- [The autopath add command](#), page 130
- [The autopath set command](#), page 131
- [The autopath display command](#), page 131
- [The autopath help command](#), page 139
- [The autopath recover command](#), page 140
- [The autopath discover command](#), page 140
- [The autopath retrieve command](#), page 141
- [The autopath set_lbpolicy command](#), page 141
- [The autopath set_prefpath command](#), page 141

The autopath delete command

The `autopath delete` command deletes a device or a LUN from the Secure Path control. This command succeeds only if the LUN is not busy. For example, when there is no I/O happening and when the LUN is not mounted or open.

Syntax:

```
autopath delete {device path |-l LUNWWID}
```

device path is either the primary path or an alternate path of the device.

Deleted LUNs are no longer under Secure Path control and this setting is persistent across reboots.

Deleted LUNs are listed in the unattached list of Secure Path Active-Active arrays. The unattached list maintains the WWNs of all deleted LUNs. You can view this list using the following command:

```
autopath display -u
```

Persistence data, like load balancing policies is not kept persistent across reboots for deleted LUNs. Once a LUN is deleted, persistent data maintained for that LUN is removed.

A LUN can be deleted either by passing device path or LUN WWID as an argument to the `delete` command as shown below:

■ Deleting the LUN using the Device Path:

— Syntax:

```
autopath delete <device path>
```

— Example:

```
autopath delete /dev/dsk/c0t0d0
```

■ Deleting the LUN using the LUN WWID

— Syntax:

```
autopath delete -l <LUN WWID>
```

— Example:

```
autopath delete -l 6005-08B4-0001-499C-0002-0000-0005-0000
```

Note: The `autopath delete` command is not available for HP-UX 11.00

The `autopath add` command

The `autopath add` command removes the deleted LUN from the Secure Path's unattached list, and the `autopath discover` command following this, adds the deleted LUN back to Secure Path control. You can add (using the `autopath add` command followed by the `autopath discover` command) only those LUNs that you have deleted using the `autopath delete` command.

Syntax:

```
autopath add -l <LUN WWID>
```

Example:

```
autopath add -l 6005-08B4-0001-499C-0002-0000-0005-0000
```

The `autopath add` command succeeds even if the LUN is in use. This command removes the LUN WWID entry from the unattached list.

Note: The `autopath add` command is not available for HP-UX 11.00

The autopath set command

The `autopath set` command sets load balancing policy for an autopath device.

Syntax:

```
autopath set -l <LUN WWID> -b <policy name>
```

LUN WWID is the WWN ID of the device.

policy name is the load-balancing policy to be set.

The valid load-balancing policies are:

- RR -- round-robin
- SQL -- shortest queue length
- SST -- shortest service time
- NLB* -- no load balance policy
- OFF* -- switch off load balancing

* Both options give you similar functionality.

Example:

```
# autopath set -l 6005-08B4-0001-499C-0001-F000-0163-0000 -b sql
```

The autopath display command

The `autopath display` command displays details about Secure Path devices, such as alternate paths to a Secure Path device, associated status, and load-balancing policy settings.

The `autopath display` command displays the following information:

- [List of All Arrays Connected to a Host](#)
- [Details of All LUNs Connected from an Array](#)
- [List of Array Controllers Connected to the Host](#)
- [List all LUNs in the Unattached List](#)
- [Display the LUN info of the Lun using a Device Path](#)
- [Display the LUN info of the Lun using a LUN WWID](#)
- [Display all LUNs Connected to the Host](#)

List of All Arrays Connected to a Host

The `autopath display -r` command displays a list of all connected arrays to the host.

Syntax:

```
autopath display -r
```

Example:

```
# autopath display -r
```

```
-----  
HPswsp Version: A.3.0F.00F.00F  
-----
```

```
Array IDs  
-----
```

```
5006-0b00-0010-3f42
```

```
5006-0b00-0010-3456  
-----
```

Details of All LUNs Connected from an Array

The `autopath set -r <Array ID>` displays details of all LUNs connected from an array.

Syntax:

```
autopath display -r <Array ID>
```

Example:

```
# autopath display -r 5006-0b00-0010-3f42
-----
HPswsp Version: A.3.0F.00F.00F
Array WWN: 5006 0b00 0010 3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Round Robin
-----
Device Path                                Status
-----
/dev/dsk/c10t0d0[o]                        active
/dev/dsk/c11t0d0                            failed
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-1234
Load Balancing Policy: Preferred Path
-----
Device Path                                Status
-----
/dev/dsk/c10t0d1                            active
/dev/dsk/c11t0d1 [PP]                      failed
-----
```

List of Array Controllers Connected to the Host

The `autopath display -c` displays a list of controllers connected to the host.

Syntax:

```
autopath display -c
```

Example:

```
# autopath display -c
-----
HPswsp Version: A.3.0F.00F.00F
-----
Array ID: 5006-0b00-0010-3f42
-----
Controller IDs
-----
P4889B59IM500P
P4889B59IM500J
-----
Array ID: 5006-0b00-0010-3456
-----
Controller IDs
-----
P66C5D29IO101Z
P66C5D29IO1037
-----
```

List all LUNs in the Unattached List

The `autopath display -u` command displays a list of all LUNs in the unattached list.

Syntax:

```
autopath display -u
```

Example:

```
# autopath display -u
-----
HPswsp version: A.3.0F.00F.00F
-----
Array ID: 5006-0b00-0010-3456
-----
Deleted Luns
-----
6005-08B4-0001-499C-0001-F000-0163-0000
6005-08B4-0001-550A-0001-A000-00B4-0000
-----
Array ID: 5006-0b00-0010-3FD2
-----
Deleted Lun
-----
6005-08B4-0001-550A-0001-A000-04D3-0000
-----
```

Display the LUN info of the Lun using a Device Path

The `autopath display <device path>` command displays the LUN info of the Lun using the device path.

Syntax:

```
autopath display <device path>
```

Example:

```
# autopath display /dev/dsk/c0t0d0
-----
HPswsp Version: A.3.0F.00F.00F
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                Status
-----
/dev/dsk/c0t0d0            active
/dev/dsk/c1t0d0            failed
-----
```

Display the LUN info of the Lun using a LUN WWID

The `autopath display -l<LUN WWID>` command displays the LUN info of the Lun using the LUN WWID.

Syntax:

```
autopath display -l<LUN WWID>
```


Example:

```
# autopath display -l 6005-08B4-0001-499C-0002-0000-0005-0000
-----
HPswsp Version: A.3.0F.00F.00F
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                                Status
-----
/dev/dsk/c0t0d0                            active
/dev/dsk/c1t0d0[o]                         failed
-----
```

Display all LUNs Connected to the Host

The `autopath display [all]` command displays details about all LUNs connected to the host.

Syntax:

```
autopath display
autopath display all
```

Example:

```
# autopath display
-----
HPswsp Version: A.3.0F.00F.00F
-----
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                                Status
-----
/dev/dsk/c10t0d0                            active
/dev/dsk/c11t0d0                            failed
-----
LUN WWID: 6005-08B4-0001-550A-0001-A000-00B4-0000
Load Balancing Policy: No Load Balancing
-----
Device Path                                Status
-----
/dev/dsk/c10t0d1                            active
/dev/dsk/c11t0d1                            failed
-----
Array ID: 5006-0b00-0010-3456
-----
LUN WWID: 6005-08B4-0001-550A-0001-A000-04D3-0000
Preferred Path: /dev/dsk/c16t0d0
-----
Device Path                                Status
-----
/dev/dsk/c15t0d0                            active
/dev/dsk/c16t0d0 (pp)                       failed
-----
```

```
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
```

```
Load Balancing Policy: No Load Balancing
```

```
-----
Device Path                               Status
-----
/dev/dsk/c15t0d1                          active
/dev/dsk/c16t0d1                          failed
-----
```

The autopath help command

The `autopath help` command lists all the autopath commands. It also displays syntax of an autopath command and its usage.

Syntax:

```
# autopath help [command]
```

Example:

```
# autopath help
```

```
Usage: autopath <Command>
```

command can be of:

- `add` -- Remove the LUN from the Secure Path's un-attached list
- `delete` -- Delete LUNs from the Secure Path's active device list
- `discover` -- Discover the newly added device and also recognize the status of old device
- `display` -- Display accessible storage information
- `set` -- Set Secure Path configuration parameters
- `set_lbpolicy` -- Set load balancing policy
- `set_preferredpath` -- Set preferred path
- `retrieve` -- Retrieve the persistence setting
- `recover` -- Start the recover daemon to recover the failed devices
- `help` -- Display this help message

Example:

```
# autopath help discover
Usage: autopath discover

# autopath help add
Usage: autopath add [option] [WWLUNID]
       option: -l    -- For entering the WWLUNID
       WWLUNID:    -- Unique ID of the Device

# autopath help delete
Usage: autopath delete < device path | [option] [WWLUNID] >
       device path: -- Device Special File e.g./dev/dsk/c#t#d#
       option: -l    -- For entering the WWLUNID
       WWLUNID:    -- Unique ID of the Device
```

The autopath recover command

The `autopath recover` command spawns a process to enable automatic path recovery. This process is activated during system boot.

If the process is terminated or is not invoked automatically, you can invoke this from the command line to enable the automatic path recovery feature.

Syntax:

```
autopath recover
```

For more information, see [“Automatic path recovery”](#) on page 122.

The autopath discover command

The `autopath discover` command discovers any new devices/paths added, or any existing devices/paths deleted, and updates the data to the list of Secure Path for Active-Active devices.

Syntax:

```
autopath discover
```

Example:

```
# autopath discover

Discovery of New Paths / LUNs will be effective only if ioscan
and insf -e are executed prior to autopath discover
```

```
autopath: Initiating Autopath Discover...
autopath: Discover in progress...
autopath: Discover successful.
```

The autopath retrieve command

The `autopath retrieve` command restores the Secure Path load-balancing policy, preferred path settings, and deleted LUNs across system reboots. Retrieval of settings may not be effective if SAN configuration changes have been made for the host.

Syntax:

```
autopath retrieve
```

Example

```
# autopath retrieve
```

The autopath set_lbpolicy command

The `autopath set_lbpolicy` command sets the load-balancing policy for the specified device path.

Syntax:

```
autopath set_lbpolicy policy path
```

The parameter *policy* specifies the load-balancing policy name (see the following list), and the term *path* specifies the physical device path.

- NLB/OFF -- no load balance policy
- RR -- round-robin
- SQL -- shortest queue length
- SST -- shortest service time

Example:

```
# autopath set_lbpolicy RR /dev/dsk/c0t0d0
```

The autopath set_prepath command

The `autopath set_prepath` command sets the preferred device path to a Secure Path device. When the path details are displayed with the `autopath display` command, the preferred path is marked (`pp`).

Syntax:

```
autopath set_prefpath path
```

The parameter *path* specifies the physical device path.

Example:

```
# autopath set_prefpath /dev/dsk/c4t0d0
```

Troubleshooting Secure Path

Troubleshooting can be performed by you or an HP service representative in accordance with your HP service contract. If you are unable to resolve an error condition, ask your HP service representative for assistance.

Recovering after a failure

When a path fails, it is no longer used by Secure Path. After the path is repaired, Secure Path automatically begins using the path with the designated load-balancing policy. No user action is necessary.

Note: If a path to the device has been serviced and the device recovery does not occur, check whether the `autopath recover` process has been terminated inadvertently. If so, restart the recovery process by executing the `autopath recover` command.

For more information, see “[The autopath recover command](#)” on page 140.

Secure Path messages

Secure Path reports errors, diagnostic messages, and informational messages to the `/var/adm/syslog/syslog.log` file. You can enter the `dmesg` command to view the messages reported by Secure Path. See [Table 12](#) for a list of messages that may exist in the log file.

Table 12: Secure Path for Active-Active disk array event messages

Event	Syslog message
DEVICE ACCESS FAILURE	AUTOPATH: Warning: Unable to access device 0x1f040000
MAXIMUM LUN COUNT LIMIT	AUTOPATH: Warning: LUN count reached maximum value of 65536. Last device recognized is 0x1f040000
LUN COLLISION MESSAGE	AUTOPATH: LUN collision occurred at: c4t0d1
ULM REGISTRATION FAILURE	AUTOPATH: Warning: Cannot register path 0x1f040000 as an Auto Path device. Path is already registered

Table 12: Secure Path for Active-Active disk array event messages (Continued)

Event	Syslog message
PATH FAILED MESSAGE	AUTOPATH: Path 0x1f040000 failed! Rerouting to alternate path
ALL PATHS FAILED MESSAGE	AUTOPATH: All the paths to the end device 0x1f040000 failed!
PATH RECOVERED MESSAGE	AUTOPATH: Path 0x1f040000 recovered
MEMORY ALLOCATION FAILURE	AUTOPATH: Warning: Memory Allocation failed
DEVICE BUSY MESSAGE	AUTOPATH: Device Busy: c4t0d1
DEVICE DISCOVERY FAILURE	AUTOPATH: Warning: Failed to discover the device 0x1f110400. Cause: Device is Busy

Secure Path Workgroup Edition for VA

3

HP StorageWorks Secure Path V3.0F Workgroup Edition for VA provides automatic I/O path failover, failback, recovery, and load balancing for host systems configured with multiple host adapters and connections to disk arrays.

This chapter provides the following Secure Path Workgroup Edition for VA information:

- [Features](#), page 146
- [ULM services](#), page 147
- [Dynamic load balancing](#), page 148
- [Automatic failover](#), page 149
- [Automatic path recovery](#), page 150
- [Online device discovery](#), page 151
- [Installation](#), page 153
- [Secure Path SAN boot setup for VA devices](#), page 153
- [Upgrading from the Web](#), page 155
- [Uninstalling Secure Path](#), page 156
- [Command line interface](#), page 157
- [Troubleshooting Secure Path](#), page 171

Features

Secure Path provides enhanced data availability with these features:

- Automatic path failover to an alternate path
- Automatic path recovery after failed path is serviced
- Automatic failback when a path recovers from failure
- Dynamic load balancing over multiple paths
- CLI for Secure Path management
- Ability to reestablish previous load-balancing policy after reboot through the CLI
- Ability to add new devices and paths without rebooting
- Supports upto 32 paths to an end LUN
- SAN boot support for VA devices

The HP StorageWorks Secure Path software performs dynamic load balancing of data flow through multiple paths. It detects multiple paths to each logical device and distributes the data load among the paths for optimum performance.

The user interface lets a system administrator define load-balancing policies and preferred paths and view device path information. Secure Path manages paths according to the balancing policy, ensuring that no single path is a performance bottleneck.

ULM services

The SCSI ULM interface is used by Secure Path to provide flexible configuration and layering of modules above the SCSI disk drivers. In order for Secure Path to be configured into HP-UX V11i V1.0 64-bit operating systems (and coexist with other pseudo drivers), Secure Path must register itself with the ULM services for each LUN path that it wants to control.

Dynamic load balancing

Secure Path performs dynamic load balancing while monitoring each path to ensure that the I/O transaction is completed. The load-balancing policy is selected by the administrator.

The dynamic load-balancing policy prevents any path from becoming overloaded, and it helps to prevent the congestion that occurs when many I/O operations are directed to common devices along the same path.

If a preferred path is used for a device, the entire I/O for that particular device flows through the preferred path and no load balancing is done by Secure Path for that device.

VA disk arrays

Increased performance is not always realized with VA systems. In most cases, the best performance is provided by using preferred paths.

Automatic failover

In the event of a failure of any part of a path between the disk array and a server, Secure Path automatically switches to an alternate path, dropping the failed path out of the I/O rotation without any loss of data. The failover is not visible to applications, so normal operation continues without downtime.

For troubleshooting information, see “[Troubleshooting Secure Path](#)” on page 171.

Automatic path recovery

When a path fails, it is no longer used. After the path has been repaired and returned to normal, Secure Path automatically begins using the path with the designated load-balancing policy. No user action is necessary.

Online device discovery

If there were any changes in the SAN configuration, such as addition and deletion of paths or devices, these changes can be updated in Secure Path for VA disk arrays for maximum and efficient utilization of resources. The `autopath discover` command updates the SAN configuration without a system reboot, and the `autopath delete` command removes a device from an autopath control.

Note: Discovery of new Paths or LUNs is effective only if you execute `ioscan` and `insf -e` before executing the `autopath discover` command.

System requirements

To install Secure Path the system must conform to these requirements:

- HP-UX OS 11i V1.0 or 11i V2.0
- Administrator `root` access to the host system
- SCSI ULM services Version B.11.11.01 for HP-UX 11i V1.0

For specific installation requirements for your system, contact your HP account representative.

Note: Refer to the *HP StorageWorks Secure Path V3.0F for HP-UX 11i V1.0, 11i V2.0 and HP-UX 11i V1.0, 11i V2.0 Workgroup Edition release notes* for details about the supported configuration.

Installation

This section describes the procedures for installing Secure Path. You must have `root` account privileges to install Secure Path software. Your HP account representative can assist you in determining the supported configurations for your system.

Installing Secure Path Workgroup Edition for VA

Before installing Secure Path software on HP-UX 11i, ensure that SCSI ULM services is installed on the system.

To install Secure Path, you must have superuser (`root`) access on the HP-UX host.

Use the following steps to install Secure Path:

1. Log on to the HP-UX system as superuser (`root`).
2. Insert the Secure Path installation CD-ROM into the CD-ROM drive.
3. Mount the CD-ROM on your file system.
4. Change to the directory in which the CD-ROM is mounted. For example, if the CD-ROM is mounted to a directory called `/cdrom`, change the directory by entering the following command:

```
# cd /cdrom/
```

5. Install Secure Path software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```

When the installation is complete, the server reboots (HP-UX 11i v1.0 only).

Installation of the Secure Path package creates `/Autopath` and `/HPswsp` directory under `/opt` directory. The `changes.log` file is copied into the `/Autopath` directory. The `master`, `system`, and `mod.o` files are copied into `/HPswsp` directory.

Secure Path SAN boot setup for VA devices

Use the following procedure for the Secure Path SAN Boot setup sequence:

1. Install HP-UX OS 11i V1.0 or 11i V2.0 on the VA LUN and boot the system.
2. Install Secure Path on the Boot LUN.

3. Configure LVM with alternate physical volume paths to the primary boot volume path.
4. Use the `vgextend` command to record alternate paths to the primary boot volume path.

```
# vgextend /dev/vg00 alternate_physical_device_path
```

Example:

```
# vgextend /dev/vg00 /dev/dsk/c14t0d1 /dev/dsk/c16t0d1  
/dev/dsk/c18t0d1
```

The `vgextend` command extends root volume with alternate paths.

5. Use the `setboot` command to modify the boot variables and to set alternate paths to the boot LUN.

```
# setboot -a hw_path_of_alternate_boot_path
```

Example:

```
setboot -a 0/0/2/0.2.1
```

Upgrading from the Web

Access the upgrade package at:

<http://www.hp.com/country/us/eng/prodserv/storage.html>

This package is intended as an upgrade only. The patch depot upgrades Secure Path V3.0x Workgroup Edition to Secure Path V3.0F Workgroup Edition.

1. Copy the upgrade tar package to a temporary directory (for example, /tmp/HPswsp).
2. Unbundle the upgrade files by entering the following commands:

```
# cd /tmp/Securepath
# tar xvf sp_v30F_hp_WE_web.tar
```

Verify that the directory contains the installation script `install.sh` and the directory `HPswsp_WE_v30F`.

3. Install Secure Path Workgroup Edition software on the server using the provided shell script by entering the following command:

```
# ./install.sh
```

When the installation is complete and the server reboots, a subsequent `swlist` displays the following Secure Path Workgroup Edition output:

```
#
# Product(s) not contained in a Bundle
HPswsp A.3.0F.00F.00F HP StorageWorks Secure Path Workgroup
Edition Device Driver and utilities for VA Disk Arrays.
```

Uninstalling Secure Path

Secure Path can be removed using the HP SD utility. When you remove Secure Path, all files, including configuration files, are removed. Use the following steps to uninstall Secure Path:

1. Log on to the HP-UX system as superuser (`root`).
2. From the command line, execute the `swremove` command as follows:

```
# swremove -x autoreboot=true HPswsp
```
3. You can also launch the interactive session of `swremove` and select **HPswsp HP StorageWorks Secure Path Workgroup Edition Device Driver and Utilities for VA Disk Arrays** product for removal.

The system reboots after removal is completed (HP-UX 11i v1.0 only).

Command line interface

The Secure Path CLI can be used only on hosts connected to devices with the `HPswsp` driver installed. The commands supported by this interface and the syntax are described in the following topics:

- [The autopath delete command](#), page 157
- [The autopath add command](#), page 158
- [The autopath set command](#), page 159
- [The autopath display command](#), page 159
- [The autopath help command](#), page 167
- [The autopath recover command](#), page 168
- [The autopath discover command](#), page 168
- [The autopath retrieve command](#), page 169
- [The autopath set_lbpolicy command](#), page 169
- [The autopath set_prefpath command](#), page 170

The autopath delete command

The `autopath delete` command deletes a device or a LUN from the Secure Path control. This command succeeds only if the LUN is not busy. For example, when there is no I/O happening and when the LUN is not mounted or open.

Syntax:

```
autopath delete {device path |-l LUNWWID}
```

device path is either the primary path or an alternate path of the device.

Deleted LUNs are no longer under Secure Path control and this setting is persistent across reboots.

Deleted LUNs are listed in the unattached list of Secure Path Active-Active arrays. The unattached list maintains the WWNs of all deleted LUNs. You can view this list using the following command:

```
autopath display -u
```

Persistence data, like load balancing policies is not kept persistent across reboots for deleted LUNs. Once a LUN is deleted, persistent data maintained for that LUN is removed.

A LUN can be deleted either by passing device path or LUN WWID as an argument to the `delete` command as shown below:

■ **Deleting the LUN using the Device Path:**

— Syntax:

```
autopath delete <device path>
```

— Example:

```
autopath delete /dev/dsk/c0t0d0
```

■ **Deleting the LUN using the LUN WWID**

— Syntax:

```
autopath delete -l <LUN WWID>
```

— Example:

```
autopath delete -l 6005-08B4-0001-499C-0002-0000-0005-0000
```

Note: The `autopath delete` command is not available for HP-UX 11.00

The `autopath add` command

The `autopath add` command removes the deleted LUN from the Secure Path's unattached list, and the `autopath discover` command following this, adds the deleted LUN back to Secure Path control. You can add (using the `autopath add` command followed by the `autopath discover` command) only those LUNs that you have deleted using the `autopath delete` command.

Syntax:

```
autopath add -l <LUN WWID>
```

Example:

```
autopath add -l 6005-08B4-0001-499C-0002-0000-0005-0000
```

The `autopath add` command succeeds even if the LUN is in use. This command removes the LUN WWID entry from the unattached list.

Note: The `autopath add` command is not available for HP-UX 11.00

The autopath set command

The `autopath set` command sets load balancing policy for an autopath device.

Syntax:

```
autopath set -l <LUN WWID> -b <policy name>
```

LUN WWID is the WWN ID of the device.

policy name is the load-balancing policy to be set.

The valid load-balancing policies are:

- RR -- round-robin
- SQL -- shortest queue length
- SST -- shortest service time
- NLB* -- no load balance policy
- OFF* -- switch off load balancing

* Both options give you similar functionality.

Example:

```
# autopath set -l 6005-08B4-0001-499C-0001-F000-0163-0000 -b sql
```

The autopath display command

The `autopath display` command displays details about Secure Path devices, such as alternate paths to a Secure Path device, associated status, and load-balancing policy settings.

The `autopath display` command displays the following information:

- [List of All Arrays Connected to a Host](#)
- [Details of All LUNs Connected from an Array](#)
- [List of Array Controllers Connected to the Host](#)
- [List all LUNs in the Unattached List](#)
- [Display the LUN info of the Lun using a Device Path](#)
- [Display the LUN info of the Lun using a LUN WWID](#)
- [Display all LUNs Connected to the Host](#)

List of All Arrays Connected to a Host

The `autopath display -r` command displays a list of all connected arrays to the host.

Syntax:

```
autopath display -r
```

Example:

```
# autopath display -r
```

```
-----  
HPswsp Version: A.3.0F.00F.00F  
-----
```

```
Array IDs  
-----
```

```
5006-0b00-0010-3f42
```

```
5006-0b00-0010-3456  
-----
```

Details of All LUNs Connected from an Array

The `autopath set -r <Array ID>` displays details of all LUNs connected from an array.

Syntax:

```
autopath display -r <Array ID>
```


Example:

```
# autopath display -r 5006-0b00-0010-3f42
-----
HPswsp Version: A.3.0F.00F.00F
Array WWN: 5006 0b00 0010 3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Round Robin
-----
Device Path                                Status
-----
/dev/dsk/c10t0d0[o]                        active
/dev/dsk/c11t0d0                            failed
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-1234
Load Balancing Policy: Preferred Path
-----
Device Path                                Status
-----
/dev/dsk/c10t0d1                            active
/dev/dsk/c11t0d1 [PP]                       failed
-----
```

List of Array Controllers Connected to the Host

The `autopath display -c` displays a list of controllers connected to the host.

Syntax:

```
autopath display -c
```

Example:

```
# autopath display -c
-----
HPswsp Version: A.3.0F.00F.00F
-----
Array ID: 5006-0b00-0010-3f42
-----
Controller IDs
-----
P4889B59IM500P
P4889B59IM500J
-----
Array ID: 5006-0b00-0010-3456
-----
Controller IDs
-----
P66C5D29IO101Z
P66C5D29IO1037
-----
```

List all LUNs in the Unattached List

The `autopath display -u` command displays a list of all LUNs in the unattached list.

Syntax:

```
autopath display -u
```

Example:

```
# autopath display -u
```

```
-----
HPswsp version: A.3.0F.00F.00F
-----
```

```
Array ID: 5006-0b00-0010-3456
-----
```

```
Deleted Luns
-----
```

```
6005-08B4-0001-499C-0001-F000-0163-0000
```

```
6005-08B4-0001-550A-0001-A000-00B4-0000
-----
```

```
Array ID: 5006-0b00-0010-3FD2
-----
```

```
Deleted Lun
-----
```

```
6005-08B4-0001-550A-0001-A000-04D3-0000
-----
```

Display the LUN info of the Lun using a Device Path

The `autopath display <device path>` command displays the LUN info of the Lun using the device path.

Syntax:

```
autopath display <device path>
```

Example:

```
# autopath display /dev/dsk/c0t0d0
-----
HPswsp Version: A.3.0F.00F.00F
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                Status
-----
/dev/dsk/c0t0d0            active
/dev/dsk/c1t0d0            failed
-----
```

Display the LUN info of the Lun using a LUN WWID

The `autopath display -l<LUN WWID>` command displays the LUN info of the Lun using the LUN WWID.

Syntax:

```
autopath display -l<LUN WWID>
```

Example:

```
# autopath display -l 6005-08B4-0001-499C-0002-0000-0005-0000
-----
HPswsp Version: A.3.0F.00F.00F
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                                Status
-----
/dev/dsk/c0t0d0                            active
/dev/dsk/c1t0d0[o]                         failed
-----
```

Display all LUNs Connected to the Host

The `autopath display [all]` command displays details about all LUNs connected to the host.

Syntax:

```
autopath display
autopath display all
```

Example:

```
# autopath display
-----
HPswsp Version: A.3.0F.00F.00F
-----
Array ID: 5006-0b00-0010-3f42
-----
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
Load Balancing Policy: Shortest Service Time
-----
Device Path                               Status
-----
/dev/dsk/c10t0d0                           active
/dev/dsk/c11t0d0                           failed
-----
LUN WWID: 6005-08B4-0001-550A-0001-A000-00B4-0000
Load Balancing Policy: No Load Balancing
-----
Device Path                               Status
-----
/dev/dsk/c10t0d1                           active
/dev/dsk/c11t0d1                           failed
-----
Array ID: 5006-0b00-0010-3456
-----
LUN WWID: 6005-08B4-0001-550A-0001-A000-04D3-0000
Preferred Path: /dev/dsk/c16t0d0
-----
Device Path                               Status
-----
/dev/dsk/c15t0d0                           active
/dev/dsk/c16t0d0 (pp)                      failed
-----
```

```
LUN WWID: 6005-08B4-0001-499C-0001-F000-0163-0000
```

```
Load Balancing Policy: No Load Balancing
```

```
-----
Device Path                               Status
-----
/dev/dsk/c15t0d1                           active
/dev/dsk/c16t0d1                           failed
-----
```

The autopath help command

The `autopath help` command lists all the autopath commands. It also displays syntax of an autopath command and its usage.

Syntax:

```
# autopath help [command]
```

Example:

```
# autopath help
```

```
Usage: autopath <Command>
```

command can be of:

- `add` -- Remove the LUN from the Secure Path's un-attached list
- `delete` -- Delete LUNs from the Secure Path's active device list
- `discover` -- Discover the newly added device and also recognize the status of old device
- `display` -- Display accessible storage information
- `set` -- Set Secure Path configuration parameters
- `set_lbpolicy` -- Set load balancing policy
- `set_preferredpath` -- Set preferred path
- `retrieve` -- Retrieve the persistence setting
- `recover` -- Start the recover daemon to recover the failed devices
- `help` -- Display this help message

Example:

```
# autopath help discover
Usage: autopath discover

# autopath help add
Usage: autopath add [option] [WWLUNID]
       option: -l    -- For entering the WWLUNID
       WWLUNID:    -- Unique ID of the Device

# autopath help delete
Usage: autopath delete < device path | [option] [WWLUNID] >
       device path: -- Device Special File e.g./dev/dsk/c#t#d#
       option: -l    -- For entering the WWLUNID
       WWLUNID:    -- Unique ID of the Device
```

The autopath recover command

The `autopath recover` command spawns a process to enable automatic path recovery. This process is automatically activated during system boot.

If the process is terminated or is not invoked automatically, you can invoke this from the command line to enable the automatic path recovery feature.

Syntax:

```
autopath recover
```

For more information, see “[Automatic path recovery](#)” on page 150.

The autopath discover command

The `autopath discover` command discovers any new devices or paths added or any existing devices or paths deleted, and updates the data to the list of Secure Path Workgroup Edition for VA devices.

Syntax:

```
autopath discover
```


Example:

```
# autopath discover
Discovery of New Paths / LUNs will be effective only if ioscan
and insf -e are executed prior to autopath discover
autopath: Initiating Autopath Discover...
autopath: Discover in progress...
autopath: Discover successful.
```

The autopath retrieve command

The `autopath retrieve` command restores the Secure Path load-balancing policy and preferred path settings across system reboots. Retrieval of settings may not be effective if SAN configuration changes have been made for the host.

Syntax:

```
autopath retrieve
```

Example

```
# autopath retrieve
```

The autopath set_lbpolicy command

The `autopath set_lbpolicy` command sets the load-balance policy for the specified device path.

Syntax:

```
autopath set_lbpolicy policy path
```

The parameter *policy* specifies the load-balance policy name (see the following list) and the variable *path* specifies the physical device path.

- NLB/OFF -- no load balance policy
- RR -- round robin
- SQL -- shortest queue length
- SST -- shortest service time

Example:

```
# autopath set_lbpolicy RR /dev/dsk/c0t0d0
```

The `autopath set_prepath` command

The `autopath set_prepath` command sets the preferred device path to a Secure Path device. When the path details are displayed with the `autopath display` command, the preferred path is marked (pp).

Syntax:

```
autopath set_prepath path
```

The parameter *path* specifies the physical device path.

Example:

```
# autopath set_prepath /dev/dsk/c4t0d0
```

Troubleshooting Secure Path

Troubleshooting can be performed by you or an HP service representative in accordance with your HP service contract. If you are unable to resolve an error condition, ask your HP service representative for assistance.

Recovering after failure

When a path fails, it is no longer used by Secure Path. After the path is repaired, Secure Path automatically begins using the path with the designated load-balancing policy. No user action is necessary.

Note: If a path to the device has been serviced and the device recovery does not occur, check whether the `autopath recover` process has been terminated inadvertently. If so, restart the recovery process by executing the `autopath recover` command.

For more information, see “[The autopath recover command](#)” on page 168.

Secure Path messages

Secure Path reports errors, diagnostic messages, and informational messages to the `/var/adm/syslog/syslog.log` file. You can execute the `dmesg` command to view the messages reported by Secure Path, which are listed in [Table 13](#).

Table 13: Secure Path Workgroup Edition for VA event messages

Event	Syslog message
DEVICE ACCESS FAILURE	AUTOPATH: Warning: Unable to access device 0x1f040000
MAXIMUM LUN COUNT LIMIT	AUTOPATH: Warning: LUN count reached maximum value of 65536. Last device recognized is 0x1f040000
LUN COLLISION MESSAGE	AUTOPATH: LUN collision occurred at: c4t0d1
ULM REGISTRATION FAILURE	AUTOPATH: Warning: Cannot register path 0x1f040000 as an Auto Path device. Path is already registered

Table 13: Secure Path Workgroup Edition for VA event messages (Continued)

Event	Syslog message
PATH FAILED MESSAGE	AUTOPATH: Path 0x1f040000 failed! Rerouting to alternate path
ALL PATHS FAILED MESSAGE	AUTOPATH: All the paths to the end device 0x1f040000 failed!
PATH RECOVERED MESSAGE	AUTOPATH: Path 0x1f040000 recovered
MEMORY ALLOCATION FAILURE	AUTOPATH: Warning: Memory Allocation failed
DEVICE BUSY MESSAGE	AUTOPATH: Device Busy: c4t0d1
DEVICE DISCOVERY FAILURE	AUTOPATH: Warning: Failed to discover the device 0x1f110400. Cause: Device is Busy

This page has been intentionally left blank

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

controller

A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSG80 and HSV110 controllers are supported for use with Secure Path.

controller states

- **critical**—Reported for a controller pair bound in multi-bus failover mode when only one of the controllers is available. This state may mean a failed or offline condition, since the server cannot communicate with the other controller at this time.
- **operational**—The controller is available with a good status.
- **unknown**—The server cannot communicate with this controller.

device states

Attributes that describe the current operational condition of a device. A device may exist in the following states:

- **critical**—Only one path remains available to the storage unit.
- **degraded**—At least one or more paths are failed to the storage unit.
- **operational**—The Secure Path device can be accessed on at least one path.
- **unknown**—Unable to communicate with the unit. This may indicate no available path or a failed device.
- **dead**—All paths used by this Secure Path device have failed.

fabric

A network composed of high-speed fiber connections resulting from the interconnection of switches and devices. A fabric is an active and intelligent non-shared interconnect scheme for nodes.

HBA

A Host Bus Adapter is an I/O device that serves as the interface connecting a host system to the SAN (Storage Area Network).

LUN

A Logical Unit Number is the actual unit number assigned to a device at the RAID system controller.

path

A virtual communication route that enables data and commands to pass between a host server and a storage device.

path states

- **active** – Currently used for the I/O stream.
- **available** – Available on the active controller for the I/O stream.
- **failed** – Currently unusable for the I/O stream.
- **quiesced** – Path is valid but the user has moved all I/O from it.
- **standby** – The path is valid on the standby controller.

port a

The relative number of an HBA. A specific port number is determined according to its order of discovery by the Windows operating system and includes SCSI, Fibre Channel, and IDE adapter types.

SAN

Storage Area Network. A configuration of networked devices for storage.

state

State is an attribute that describes the current operational condition of an object. See also *Path*, *Path States*, *Controller States*, and *Device States*.

Index

spmgr
add WWLUNID 94, 95
client add 99
client delete 99
display (default) 65
display -u 75
log -c 81
log -l 81
log -n 81
notify 83
notify add 82
notify delete 83
password 100
quiesce - a controller 91
quiesce - a HBA 90
quiesce - c controller 91
quiesce - c path_instance 91
quiesce - p path_instance 91
restart -a HBA 92
restart -c controller 92
restart -p path_instance 92
restore all 89
restore all paths to device 89
restore all paths to storage system 90
select -c controller_serial_number 84
select -p path_instance 85
set -f 80
set -p 80

A

active paths and load balancing 88
active state 59
adding

LUNs 93
Secure Path to an existing configuration 31
SP to an existing RA/MA8000 or
ESA/EMA12000 Configuration 31
WWLUNID 94, 95

addresses
delete 83
display 83
notify 82, 83

alias
defining 77
displaying 78
array configuration documentation 33
audience 11
authorized reseller, HP 15
available state 59

C

commands
autopath discover 140, 168
autopath display 131, 159
autopath help 139
autopath retrieve 141, 169
autopath set_lbpolicy 141, 169
autopath set_prepath 141, 170
display 64, 65
log 80
notify 82
set 79
spmgr 55
configuration information, displaying 59
configuration tool 24
console, logging 81

controllers

- I/O wind down [24](#)
- preferring a unit [38](#)
- quiesce [91](#)
- restart -c spmgr [92](#)
- states
 - critical [59](#)
 - operational [59](#)

conventions

- document [12](#)
- equipment symbols [13](#)
- text symbols [12](#)

critical state [59](#)**D**

defining

- alias [77](#)
- unalias [77](#)

deleting LUNs, adding and [93](#)device states [60](#)display command [64](#)

- # spmgr [65](#)
- log settings [81](#)

display -u, # spmgr [75](#)

displaying

- alias, an [78](#)
- configuration information [59](#)
- path states [71](#)

document

- conventions [12](#)
- related documentation [11](#)

documentation, array configuration [33](#)

drivers

- HPswsp [129](#), [157](#)
- hsx [22](#)
- sdisk [35](#)
- swsp [22](#)

dual RAID controllers [21](#)**E**enable notification, logging [81](#)

enterprise virtual array

- array, configuring [40](#)
- drivers [22](#)
- HSV element manager [41](#)
- upgrading Secure Path [102](#)

equipment symbols [13](#)EVA3000, overview [18](#)EVA5000, overview [18](#)**F**failback options [26](#)failed state [59](#)failover [26](#), [121](#), [149](#)fcmsutil utility [30](#)**G**getting help [15](#)**H**hardware setup, HSx [29](#)

HBA

- restart -a, # spmgr [92](#)
- restart -a, # spmgr [92](#)

help, obtaining [15](#)

HP

- authorized reseller [15](#)
- storage web site [15](#)
- technical support [15](#)

HP SD utility [128](#), [156](#)HPswsp driver [129](#), [157](#)

HSx

- installing software [49](#)
- removing software [101](#)
- SAN boot device [53](#)
- upgrading software [102](#)

hsx driver [22](#), [116](#)**I**

installing

- HSx software [49](#)
- new HSx configuration [30](#)

- on an HSx SAN boot device [53](#)
 - on an xp and va boot device [126](#)
 - remote management [99](#)
 - va, workgroup edition software [153](#)
 - xp and va software [125](#)
- ioscan
- commands [45](#)
 - running [94](#)
- ## L
- load balancing [27](#), [78](#), [120](#), [148](#)
 - active paths [88](#)
 - load distribution
 - described [27](#)
 - disabled [26](#)
 - enabled [26](#)
 - log command [80](#)
 - console [81](#)
 - enable [81](#)
 - settings display [81](#)
 - LUNS
 - adding and deleting [93](#)
 - restoring [89](#)
- ## M
- management tools [24](#)
 - multiple-bus mode [19](#)
- ## N
- notification [81](#)
 - notification severity levels [82](#)
 - notify
 - add [82](#)
 - address [82](#)
 - command [82](#)
 - delete address [83](#)
 - display addresses [83](#)
- ## O
- offline state [59](#)
 - operational state [59](#)
- optional array features [35](#)
- ## P
- path
- definition [25](#)
 - management behavior [28](#)
 - verification [28](#)
 - management [83](#)
 - management behavior summary [28](#)
 - recovery [122](#), [150](#)
 - selecting, controller_serial_number [84](#)
 - states [59](#)
 - verification
 - defined [28](#)
 - interval, setting [80](#)
 - parameters [78](#)
 - setting [80](#)
- path_instance
- quiesce [91](#)
 - restart -p # spmgr [92](#)
 - select [85](#)
- paths
- load balancing and active paths [88](#)
 - restoring to device [89](#)
 - restoring to storage system [90](#)
 - selecting [84](#)
- PREFERRED_PATH unit attribute [19](#)
- preferring, unit to a controller [38](#)
- ## Q
- quiesce
- a # spmgr [90](#)
 - c # spmgr [91](#)
 - p # spmgr [91](#)
- quiesced objects, restarting [91](#)
- quiescing configuration objects [90](#)
- ## R
- recovery after failure [171](#)
 - related documentation [11](#)
 - remote management [98](#)

- restarting quiesced objects 91
- restore all
 - LUNs 89
 - paths to device 89
 - paths to storage system 90
- S**
- SAN boot device
 - HSx 53
 - xp and va 126
- SCSI Upper Layer Module (ULM) 119, 147
- SCSI-2, using 103
- SCSI-3, using 39
- sdisk driver 35
- Secure Path
 - basic configuration, illustrated 18
 - HSx SAN boot device 53
 - installing
 - HSx software 49
 - new HSx configuration 30
 - va, workgroup edition software 153
 - xp and va SAN boot device 126
 - xp and va software 125
 - overview 18
 - remote management 98
 - removing HSx software 101
 - software components 22
 - spagent 23
 - spmgr 24
 - technical description 17
 - technology 19
 - uninstalling va, workgroup edition software 156
 - uninstalling xp and va software 128
 - upgrading HSx software 102
- selecting paths 84
- services
 - ULM 119
- set commands 79
 - path
 - verification interval 80
 - path verification 80
 - storage system parameters 78
- setting up additional LUNs 35
- severity levels, notification 82
- spagent 23, 116
- spmgr 84
 - alias 77
 - commands 55
 - common terms 58
 - controller states 59
 - display -u 75
 - displaying an alias 78
 - log -c 81
 - log -l 81
 - log -n 81
 - notify
 - delete 83
 - notify add 82
 - notify display 83
 - overview 55
 - quiesce - a controller 91
 - quiesce - a HBA 90
 - quiesce - c controller 91
 - quiesce - p path_instance 91
 - remote management 98
 - restart -a HBA 92
 - restart -c controller 92
 - restart -p path_instance 92
 - restore all 89
 - restore all paths to device 89
 - restore all paths to storage system 90
 - select controller_serial_number 84
 - select -p path_instance 85
 - set path verification 80
 - set path verification interval 80
 - unalias 77
- states
 - controller 59
 - device 60
 - path 59
 - standby 59
- storage system parameters, setting 78
- swsp driver 22

symbols

in text 12

on equipment 13

syslog 81

T

target/LUNS per array comparison chart 36

technical description of Secure Path 17

technical support, HP 15

text symbols 12

troubleshooting

va workgroup edition 171

VA workgroup edition messages 171

xp and va diagnostic messages 143

U

ULM services 119, 147

unalias, defining 77

uninstalling

HSx software 101

va, workgroup edition software 156

xp and va software 128

unit, preferring a controller 38

upgrading

va, workgroup edition software 155

xp and va software 127

utilities

HP SD 128, 156

V

va, workgroup edition

command line interface 157

commands

discover 168

display 159

retrieve 169

set_lbpolicy 169

set_prefpath 170

device addition and deletion 151

disk arrays, va 148

failover, automatic 149

installing 153

load balancing 148

messages, diagnostic 171

path recovery, automatic 150

recovery 171

requirements, system 152

services, ULM 147

troubleshooting 171

uninstalling 156

upgrading software 155

verifying a path 28

W

warning, symbols on equipment 13

web sites, HP storage 15

world wide name

fcmsutil utility and 30

spmgr and 80

X

xp and va

command line interface 129

commands

discover 140

display 131

help 139

retrieve 141

set_lbpolicy 141

set_prefpath 141

device addition and deletion 123

diagnostic messages 143

disk arrays, va 120

failover, automatic 121

installing 125

load balancing 120

path recovery, automatic 122

requirements, system 124

SAN boot device 126

services, ULM 119

uninstalling 128

upgrading software 127

