Compaq SANworks

Secure Path Version 3.1B for Windows Workgroup Edition

Installation and Reference Guide

Part Number: AA-RR48A-TE

First Edition (October 2001)

Product Version: 3.1B

This guide describes the SANworks Secure Path software. It includes information about Secure Path technology, installation procedures and instructions for troubleshooting connection problems.

COMPAQ

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

Compaq service tool software, including associated documentation, is the property of and contains confidential technology of Compaq Computer Corporation. Service customer is hereby licensed to use the software only for activities directly relating to the delivery of, and only during the term of, the applicable services delivered by Compaq or its authorized service provider. Customer may not modify or reverse engineer, remove, or transfer the software or make the software or any resultant diagnosis or system management data available to other parties without Compaq’s or its authorized service provider’s consent. Upon termination of the services, customer will, at Compaq’s or its service provider’s option, destroy or return the software and associated documentation in its possession.

Printed in the U.S.A.

Secure Path Version 3.1B for Windows Workgroup Edition Installation and Reference Guide
First Edition (October 2001)
Part Number: AA-RR48A-TE

Contents

About this Guide

Text Conventions vii
Symbols in Text viii
Symbols on Equipment ix
Rack Stability x
Getting Help x
Compaq Technical Support x
Compaq Website xi
Compaq Authorized Reseller xi

1 Secure Path Technology

Overview 1–1
Features 1–2
Auto-Failback 1–3
Path Verification 1–3
Static Load Balancing 1–3
Software Components 1–4
Profiles 1–4
Controller Ownership 1–4
Path Definition 1–5
Path Status 1–7
Path Mode 1–7
Path State 1–7
Failover Operation 1–7
Failback Options 1–8
Path Verification 1–8
Anti-thrash Filter 1–8
Path Management Behavior Summary 1–9

2 Hardware Setup

Hardware Installation Prerequisites 2–1
Hardware Installation Procedure 2–2

3 Installing Secure Path Software

Installation Prerequisites. 3–1
Installing Standalone Software. 3–2
Installing Server Software 3–3
Installing Client Software 3–4

4 Managing Secure Path

Secure Path Login. 4–2
Launching Secure Path Manager 4–3
SPM Storage Profiles 4–3
Creating a New SPM Storage Profile. 4–3
Editing an Existing SPM Storage Profile. 4–4
Saving an SPM Storage Profile 4–4
Creating a Storage Profile Password 4–4
Changing the Secure Path Agent Password 4–5
Stopping and Re-Starting the Secure Path Agent 4–6
SPM Client Access 4–6
Configuring Client Access 4–6
Removing Client Access 4–8
Troubleshooting Connection Problems 4–8
Monitoring Host Connections. 4–8
Responding to a Lost Host Connection 4–9
Setting Storage Profile Properties 4–10
Storage System View 4–11
Storage Systems and Controllers 4–12
RAID Array Storagesets 4–12
Physical Path View 4–12
First Path 4–14
Second Path 4–14
Polling Interval and Display Refresh 4–15
Managing Storagesets and Paths 4–15
Moving a Storageset. 4–16
Making the Alternate Path Offline. 4–16
Making a Path Online. 4–16

Verifying a Path. 4–17
Repairing a Path. 4–17
Detecting and Identifying Path and Controller Failures 4–18
Detecting Path Failures 4–18
Storage System Path Failure Detected 4–19
Storage Controller Path Failure Detected 4–19
Storageset Path Failure Detected 4–20
Total Path Failures 4–20
Identifying Path Failovers 4–21
Identifying Controller Failovers 4–21
Responding to Failover Events 4–22
Using Secure Path Manager with Microsoft Cluster Service. 4–22

5 Removing Secure Path Software

A Troubleshooting Secure Path Connection Problems
Client/Agent Considerations A–1
Network Considerations. A–2

Glossary

Index

Figures

1–1 Path Definition in an MSA1000 Secure Path FC-AL Configuration 1–6
4–1 Secure Path Login window 4–2
4–2 Secure Path Agent Configuration Utility window 4–5
4–3 Client Access Configuration window 4–7
4–4 Lost host connection 4–9
4–5 SPM single host storage profile – Storage System view 4–11
4–6 SPM single host storage profile – Physical Path view 4–13
4–7 Lost path connection 4–17
4–8 Storage system path failure detected. 4–19
4–9 Controller path failure detected. 4–19
4–10 Storageset path failure detected 4–20
4–11 Storage system failure detected. 4–20

4–12 Storage controller failure detected. 4–20
4–13 Storageset failure detected. 4–20
4–14 State of failed path. 4–20

Tables

1 Text Conventions. vii
1–1 Path Management Behavior Summary 1–9
2–1 Secure Path Fibre Channel Hardware Installation Prerequisites. 2–1
3–1 Secure Path Fibre Channel Installation Prerequisites 3–1
4–1 Identifying a Failed State. 4–21

About this Guide

The following sections are covered:

- Text Conventions
- Symbols in Text
- Symbols on Equipment
- Rack Stability
- Getting Help
- Compaq Authorized Reseller

Text Conventions

The conventions included in Table 1 apply in most cases.

Table 1: Text Conventions

Element	Convention	Examples
• **Named Keys** • **Key Sequences**	**Bold** A plus sign (**+**) between two keys means that you should press them simultaneously.	• **Home, Print Screen, Num Lock, Esc, PgUp** • **Ctrl+A**, **Ctrl+Home**, **Alt+Ctrl+Del**
• **Menu Items and Sequences** • **Buttons** • **Dialog Box Names**	**Bold** A right angle bracket (**>**) between items refers to the navigation sequence through menu selections.	• Choose **Start > Programs > Backup.** • Click **Make Backup.** • In the **Save As** dialog box, choose the drive, then the folder.
Directory Names and Paths	Initial Caps (Unless they are case sensitive).	Save the file in the C:\StorageSets\Default directory.

Table 1: Text Conventions (Continued)

Element	Convention	Examples
file names	*Italics,* unless the file name is included in a directory name/path.	- To configure storage, edit *storageset.ini.* - (Directory name/path): Errors are logged to \syslog\errors\config_errors.txt.
- User Input - Command Names	User input appears in helvetica. command names appear in helvetica, unless they are case sensitive. Entered `<variables>` are displayed in angle brackets (< >) and all lowercase.	- To exit from the program, type exit. - At the prompt, type this command: show this_controller - Use set this_controller to change parameters. (no variable) - To see your settings, give the command: SHOW <storagesets> FULL (with variable)
- System Responses (Output and Messages) - Drive Names	`Monospace font`	- You will see the `Disk Full message.` -
URLs	Sans serif font.	For update notices, visit: http://www.compaq.com

Symbols in Text

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

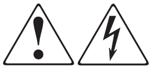
WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

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

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

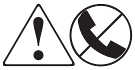
NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment



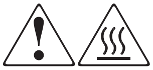
Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

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



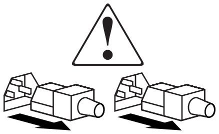
Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

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



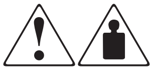
Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of 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 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.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- **The leveling jacks are extended to the floor.**
- **The full weight of the rack rests on the leveling jacks.**
- **In single rack installations, the stabilizing feet are attached to the rack.**
- **In multiple rack installations, the racks are coupled.**
- **Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.**

Getting Help

If you still have a question after reading this guide, contact your service representative or visit our website.

Compaq Technical Support

In North America, call Compaq technical support at 1-800-OK-COMPAQ, available 24 hours a day, 7 days a week.

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

Outside North America, call Compaq technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the Compaq website: http://www.compaq.com.

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.

Compaq Website

The Compaq website has the latest information on this product, as well as the latest drivers. Access the Compaq website at: http://www.compaq.com/storage. From this website, select the appropriate product or solution.

Compaq Authorized Reseller

For the name of your nearest Compaq Authorized Reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the Compaq website for locations and telephone numbers.

1

Secure Path Technology

Compaq *SANworks*^{TM} Secure Path is a server-based software product that enhances *StorageWorks*^{TM} RAID Array storage systems by providing automatic recovery of data from server-to-storage system connection component 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 pending and subsequent I/O requests to an alternate path.

This chapter provides the following Secure Path information:

- Features
- Software Components
- Controller Ownership
- Path Definition
- Path Status
- Failover Operation
- Path Management Behavior Summary.

Overview

Compaq *SANworks* Secure Path for Windows Workgroup Edition is a high-availability software product that manages and maintains continuous data access to the StorageWorks Fibre Channel RAID Array MSA1000.

You can use this software with StorageWorks RAID Arrays configured to operate on Intel-based platforms running Windows NT 4.0 Enterprise Edition, and Windows 2000 Advanced Server operating systems in single host server, Microsoft Cluster Server (MSCS), high-availability environments.

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.

Through the deployment of 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 physical "paths" in a Secure Path hardware configuration. Each path originates at an unique HBA port on a server, and ends at a unique RAID controller port in the storage system.

Secure Path enables dual StorageWorks RAID controllers to operate in an active/passive implementation, where one MSA1000 controller actively processes I/O, and an alternate controller remains passive.

Secure Path takes advantage of the MSA1000 preferred path unit attribute. Available storage units are preferred to the active controller. This attribute determines which controller is used for access at system boot time. During runtime, storage units may be moved between paths at any time through the use of the Secure Path Management utility.

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 can detect and recover from controller, switch, hub, HBA or other connection failures. Path failover is completed seamlessly, without process disruption or data loss.

Following a warm-swap of an adapter or cable component, failed controller, hub, or switch, storage units can be 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 fault tolerant configurations. Fault tolerance is the ability to recover from hardware problems without interrupting the server's performance. Fault tolerance configurations include: drive mirroring (RAID 1+0), data guarding (RA 4), distributed data guarding (RAID 5), and advanced data guarding (RAID ADG).

Features

Secure Path provides the following features:

- Provides redundant physical connectivity management along independent Fibre Channel paths between switched dual-controller RAID systems and host servers equipped with multiple HBAs.
- 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 "health" of available storage units and physical paths through the implementation of path verification diagnostics.

- Monitors and identifies failed paths and failed-over storage units.
- Facilitates online (static) load balancing between multiple storage systems.
- Automatically restores failed-over storage units to repaired paths with auto-failback capability enabled.
- Prevents failover/failback thrashing caused by marginal or intermittent conditions.
- Detects failures reliably without inducing false or unnecessary failovers.
- Implements failover/failback actions transparently without disrupting applications.
- Provides client/server remote management capability, and multiple storage system support.

Auto-Failback

When auto-failback is enabled, Secure Path monitors failed paths and automatically returns failed-over storage units to their original path once the path has been restored. Anti-thrash filters prevent “ping pong” effects (repeated failover/failback operations) caused by marginal or intermittent conditions. The user may select auto or manual failback policy using the Secure Path Management utility.

Path Verification

Path verification implements diagnostics that periodically determine the health of available storage unit paths. Path verification ensures that path status is both accurate and current. Through this background testing of active and available paths, problems may be detected and corrected, ensuring path integrity.

Static Load Balancing

Secure Path takes advantage of the potential for multiple path access and enhances I/O performance through the use of online (static) load balancing. With this feature, Secure Path can be manually configured to distribute I/O operations across multiple storage systems.

Software Components

The Secure Path Software Kit for Windows includes the following software components.

- **RDFIL** and **RaiDisk** are embedded filter drivers that provide path routing.

NOTE: RDFIL is valid for Windows 2000 only.

- **Secure Path Manager** is the client/server application used to manage multiple path StorageWorks MSA1000 configurations. This application displays a graphical representation of multiple path environments, indicating status of all configured storage units and paths. This application runs locally at the managed servers, or remotely at a management workstation. The client is compatible with any of the Windows NT and Windows 2000 operating systems.
- **Secure Path Agent** is a Windows service that communicates with the RaiDisk filter driver on the host server, and Secure Path Manager on the client side, using the TCP/IP protocol and WinSock API. The agent installs on the host server along with the RaiDisk driver.
- **Secure Path Setup** supports driver and application installation and de-installation with Windows NT and Windows 2000.

Each software component of Secure Path makes use of the Windows Event Log to post error and informational messages.

Profiles

Secure Path Manager uses the concept of “profile” to express this working configuration limit. You can manage large configurations through a single instance of the Secure Path Manager. However, there are certain practical limits on the configuration size that can be displayed and managed in a single graphical window.

The profile limits for Secure Path Manager are a maximum of 5 servers (host systems) connected to up to 5 storage systems, configured for multiple-bus failover mode.

Controller Ownership

The MSA1000 storage system contains a pair of redundant controllers and supports the active/passive implementation, or operational model.

In the active/passive model, all storagesets 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 failure on the original.

Path Definition

Within Secure Path, a path is defined as the collection (configuration) of physical interconnect components including HBAs, switches or hubs, cables, and MSA1000 Controllers. The Secure Path filter driver component, RaiDisk distinguishes physical paths by elements of the SCSI equivalent address (Bus-Target-LUN) as derived by the HBA.

In FC-AL configurations, devices are accessed within Windows NT and Windows 2000 using conventional SCSI addressing terminology as shown in Figure 1–1. Fibre Channel adapters are referred to as HBAs, which are named and numbered as SCSI ports and/or physical locations. SCSI addresses are derived from the ALPA (Arbitrated Loop Physical Address), which is soft-assigned by the MSA1000 Controller.

The LUN number is derived from the unit number assigned to the storageset within the controller using the Array Configuration Utility (ACU), included on the Compaq SmartStart CD. Each connected node on an arbitrated loop has a unique ALPA assignment.

In Figure 1–1, HBA 1, Hub 1 and Controller 1 - Port 1(P1) constitute one arbitrated loop. HBA 2, Hub 2 and Controller 2 - Port 1(P1) constitute another arbitrated loop.

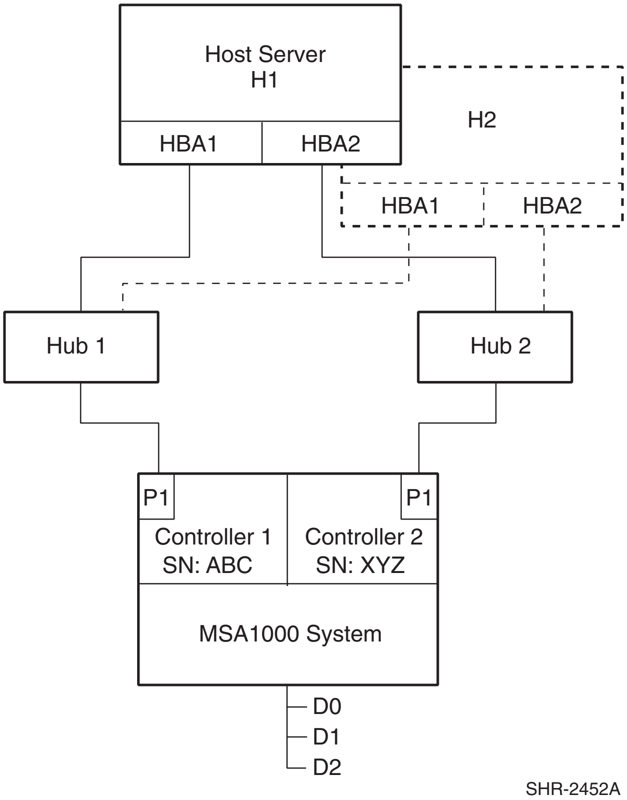


Figure 1–1: Path Definition in an MSA1000 Secure Path FC-AL Configuration

Path definition information correlating with Figure 1–1 shown as follows:

	Host	Controller Serial No.	SCSI Port	Bus-Target-LUN	HBA Slot
Drive D: (D1)	H1	ABC	1	1 – 1 – 1	2
	H1	XYZ	2	1 – 2 – 1	3
	H2	ABC	1	2 – 1 – 1	2
	H2	XYZ	2	2 – 2 – 1	3

Path Status

Secure Path displays Path Status using Path Mode (user-defined) and Path State attributes.

Path Mode

The user may set the path to the following Path Modes:

- **Preferred Path Mode** designates the user-specified path that will be used to communicate from a specific host to the specified storageset. RaiDisk declares the path to the owning controller as the Preferred path. The user may modify the default driver's path settings using Secure Path Manager.
- **Alternate Path Mode** designates paths that are not user-preferred. These paths provide redundancy in case preferred paths fail.
- **Offline Path Mode** (Alternate-Offline) include the original mode (via the prefix) and indicate the user has specified the path should never be used for I/O. Paths are marked offline only as a result of user specification.

NOTE: Offline mode can not be applied to paths that are in an Active State.

Path State

The Path State is set automatically by RaiDisk and reflects the status of the current actual path, which may deviate from user expectations because of path failures.

- **Active State** indicates that the associated path is currently servicing, or is capable of servicing I/O to the storageset.
- **Available State** indicates that the associated path belongs to the set of redundant paths to the storageset that could be used during failover.
- **Failed State** indicates that the path has encountered errors either during normal operation or as a result of Path Verification testing.

Failover Operation

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. However, it is possible for Secure Path Manager to show some units with a common failed path in the fail-over state, while other units appear to remain accessible through that path. Units remain in the failed path if there is no I/O or until polled.

- Secure Path does not change the mode of “Preferred” or “Alternate” paths in failover situations, so you can restore original path assignments after making repairs.
- Secure Path marks the “Preferred-Active” path failed and switches to an “Alternate – Available” path.
- Secure Path attempts to move the device to an “Alternate – Available” path on the other controller. Secure Path changes the “Alternate-Available” path to “Alternate-Active.”

Table 1–1 on page 1-9 provides a summary chart of path management behavior, conditioned by the several optional features of Secure Path.

Failback Options

Secure Path enables the user to set the path failback option to manual or automatic.

- In manual mode, devices are restored to their original path either through drag-and-drop operation (controller failback) or action menu items (repair). 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.

Path Verification

When enabled with the *spmgr*, Path Verification causes Secure Path to periodically test the viability of all paths to all storagesets for paths marked “Available,” “Failed,” or “Active.” Path Verification does not test paths that are in a “offline” mode.

Path Verification is useful for detecting failures that affect overall path redundancy before they affect failover capability. If an “Preferred” path fails path verification, failover occurs. If an “Alternate” 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.” If auto-failback is enabled, the “Preferred” path becomes “Active.”

Anti-thrash Filter

Secure Path implements an anti-thrash filter to avoid indefinitely moving a device back and forth in the presence of an intermittent failure mode. If, within a given period of time (currently one hour), Secure Path detects that a device has failed back twice, and the original path again causes a failover, the device will be left on the failed over path for the duration of the timer interval. At the end of the timer interval, the anti-thrash filter is reinitialized and the failover/failback process repeats if the intermittent failure cause persists.

To use the antithrash filtering, Path Verification, which is enabled by default, must be disabled.

Path Management Behavior Summary

Table 1–1 provides a summary of path management behavior conditioned by the optional features of Secure Path.

Table 1–1: Path Management Behavior Summary

Feature	Behavior/Action
Startup	1. The path to the controller on which the LUN is online is marked **preferred active.** The path to the other controller is marked **alternate available.** 2. If no online path is found, an available path online is marked as **preferred active** – and the other path is marked **alternate available.**
Active Path Failure	• Path marked preferred (or alternate) failed and fails to alternate available path. Alternate available path used is marked **alternate active**. • Behavior is the same with I/O or background path verification. • If LUN is reserved, mark path failed, but do not fail to other path on nonowning node.
Available Path Failure Path Verification	• Failed path is marked failed. • Behavior is result of background path verification.
Path Repaired	• Path is marked **available**. • If auto-failback is enabled, failback to **preferred** path from **available** path occurs as regular “autofailback” function. • If LUNs is reserved, path is marked **available** but does not autofailback on nonowning node.

2

Hardware Setup

This chapter provides installation instructions for Secure Path hardware. It includes the following topics:

- Hardware Installation Prerequisites
- Hardware Installation Procedure.

Hardware Installation Prerequisites

Verify receipt of the Fibre Channel hardware ordered for the installation. If you are missing any component, please contact your account representative, or call the Compaq Customer Services Hotline at (800) 354-9000.

The basic requirements for Secure Path operation are listed in Table 2–1.

Table 2–1: Secure Path Fibre Channel Hardware Installation Prerequisites

Host Feature	Requirement
Host Bus Adapters (and adapter driver)	Compaq Storageworks Fibre Channel Adapter FCA2101
Fibre Channel Interconnect Hardware	FC-AL hubs, switches, and connection hardware as required
Service Tools	Appropriate tools to service the equipment
Technical Documentation	The reference guides for the RAID system, HBA, host server, and Windows software

Hardware Installation Procedure

1. Install all Windows servers and all HBAs, referencing the user documentation included with your hardware.
2. Connect fibre cables to HBAs.
3. Install all of the new RAID storage system and interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the Fibre Channel equipment.
4. Install Windows to servers using the SmartStart assisted installation utility.
5. Proceed to Chapter 3, “Installing Secure Path Software.”

NOTE: For more detailed information, refer to the *Compaq ProLiant Cluster Configuration Poster* for hardware and cluster software setup and configuration.

3

Installing Secure Path Software

This chapter provides installation instructions for Secure Path software. It contains the following information:

- Reference material for high-availability connection options
- Installation prerequisites
- Installation procedures for Secure Path Fibre Channel standalone and cluster configurations
    - Server software–RDFIL (Windows 2000 only) and RaiDisk filter driver, and Secure Path Agent
    - Client software–Secure Path Manager GUI.

IMPORTANT: Before attempting to install Secure Path software, read the *Secure Path Version 3.1B Windows for Workgroup Edition* Release Notes.

Installation Prerequisites

IMPORTANT: Verify receipt of the Secure Path software kit and the Fibre Channel hardware ordered for the installation. If you are missing any component, please contact your account representative, or call the Compaq Customer Service Hotline at (800) 354-9000.

The basic requirements for Secure Path operation are listed in Table 3–1.

Table 3–1: Secure Path Fibre Channel Installation Prerequisites

Host Feature	Requirement
Platform	ProLiant or other x86
Operating System	• Windows NT 4.0 EE Edition Service Pack 6A • Windows 2000 Advanced Server Edition, Service Pack 2
Secure Path Software Kit	SANworks Secure Path for Windows Workgroup Edition Version 3.1B

Table 3–1: Secure Path Fibre Channel Installation Prerequisites

RAID Storage Systems	• StorageWorks RAID Array MSA1000 • MSA1000 Controller Firmware
Solution Software Kit	• *Modular SAN Array 1000 Support Software Version 5.31* CD • *SmartStart, Version 5.30* CD
Cluster Kit (optional)	Compaq ProLiant Cluster Kit (for Cluster services)
Technical Documentation	The reference guides for the RAID system, HBA, host server, and Windows software

Installing Standalone Software

To install and configure a Secure Path Fibre Channel topology for standalone (non-clustered) systems:

1. Perform all hardware setup procedures as described in Chapter 3.
2. Create storagesets and provide unit attributes for LUNs using the Array Configuration Utility (ACU) included with SmartStart V5.30.
3. Configure basic disk storage:
   - In Windows 2000, use Disk Management.
   - In Windows NT 4.0, use Disk Administrator.
4. Install Secure Path software on the Windows servers.

   The Secure Path software is installed using the Secure Path setup wizard. Refer to the Installing Server Software or Installing Client Software section below to complete the Secure Path software installation.
5. Shutdown and restart the server.
6. Verify that the Windows system Event Log shows a successful RaiDisk driver start event.
7. Verify that the Windows application Event Log shows a successful Secure Path Agent start event.

Installing Server Software

Install Secure Path Server software on the Windows host system to which the RAID storage system is connected. TCP/IP installation is a requirement for the host system. For cluster configurations, Secure Path must be installed on each member of the cluster.

IMPORTANT: The installation of Secure Path requires that a Temp directory be available on the system drive. For example: C:\Temp

Install the Secure Path Server software as described in the following procedure:

1. Insert the *Compaq SANworks Secure Path Software* CD into your CD-ROM drive.
2. If you have AutoRun enabled on your server, the Secure Path setup program will start automatically. Otherwise, Choose **Run** from the **Start** menu and enter the following command:

   ```
   drive_letter:\spinstal\setup.exe
   ```

   where: *drive_letter* is the drive letter assigned to the CD-ROM.
3. Choose the destination path when Setup starts.
4. Choose the **Secure Path Server Install** option to install the required drivers and Agent on your server.

   The Server Install option prompts you to designate clients permitted to manage the host. Setup, by default, lists the proper DNS name to use for accessing the local host from a client (Secure Path Manager) running on the local host. For MSCS cluster configurations, setup will include the local host names for each cluster member.

NOTE: Check with your system administrator to ensure proper TCP/IP network configurations and protocols.

5. Enter a validation password. For cluster configurations, make sure the password is the same for each member of the cluster.

Installing Client Software

Install Secure Path Client software on either the same Windows host system as the Server software, or any Windows (TCP/IP-capable) workstation. Install the Secure Path Client software according to the following procedure:

1. Insert the *Compaq SANworks Secure Path Software* CD into your CD-ROM drive.
2. If you have AutoRun enabled, the Secure Path setup program will start automatically. Otherwise, Choose **Run** from the **Start** menu and enter the following command:

   ```
   drive_letter:\spinstal\setup.exe
   ```

   where: *drive_letter* is the drive letter assigned to the CD-ROM.
3. Choose the destination folder when the setup starts.
4. Choose the **Secure Path Client Install** option to install the Secure Path Manager software.

You have now completed the software installation procedures required to support the Secure Path environment. See Chapter 4, Managing Secure Path for information on monitoring and managing Secure Path activity using Secure Path Manager.

4

Managing Secure Path

Use Secure Path Manager (SPM) to perform the following actions:

- Monitor and manage a Secure Path environment.
- Display specific information about the state of RAID storage systems and I/O paths configured for high-availability storage access.
- Set various properties and modes associated with a managed storage profile, and to set failback policy.
- Detect and identify path failures.

This chapter provides the following SPM operational information:

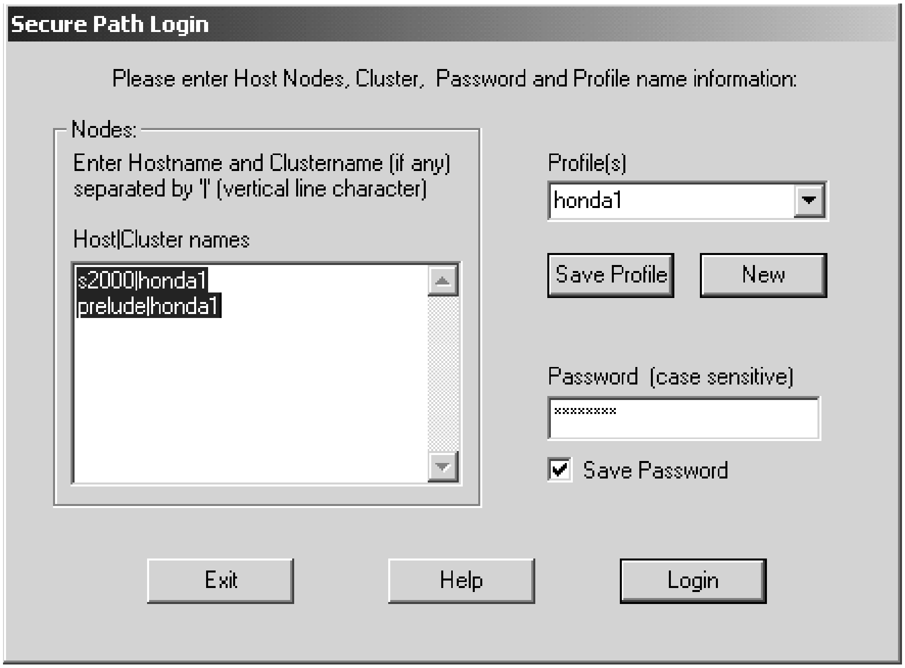
- Secure Path Login
- Changing the Secure Path Agent Password
- SPM Client Access
- Troubleshooting Connection Problems
- Monitoring Host Connections
- Storage System View
- Managing Storagesets and Paths
- Detecting and Identifying Path and Controller Failures
- Responding to Failover Events
- Using Secure Path Manager with Microsoft Cluster Service.

Secure Path Login

The **Secure Path Login** window enables you to perform the functions described in this section.

- Login to the SPM GUI interface.
- Define and edit SPM storage profiles.
- Edit the SPM Password.

Figure 4–1 shows the **Secure Path Login** window.



Secure Path Login

Please enter Host Nodes, Cluster, Password and Profile name information:

Nodes:

Enter Hostname and Clustername (if any) separated by '|' (vertical line character)

Host|Cluster names

s2000|honda1
prelude|honda1

Profile(s): honda1

Password (case sensitive): ********

☑ Save Password

Figure 4–1: Secure Path Login window

Launching Secure Path Manager

To launch SPM from the Windows **Start** menu, perform the following procedure:

1. Select **Programs > SecurePath > SPM**.
2. Click the **Secure Path Manager (SPM)** application icon to access the **Secure Path Login** window shown in Figure 4–1.

SPM Storage Profiles

SPM displays a *storage-centric* view of Secure Path-managed RAID storage resources. All Secure Path-protected RAID storage systems common to a given host (or set of hosts) are presented in an SPM display. During SPM login, you can enter hosts that share these RAID storage systems while defining storage profiles.

More than one instance of SPM is required to manage installations that include a mix of non clustered and clustered hosts.

Creating a New SPM Storage Profile

To create additional SPM storage profiles while in the **Secure Path Login** window:

1. Click **New**.
2. Enter host names in the **Host|Cluster Names** field.
   - To create a non-clustered host profile, enter a host name (or set of host names) in the **Host|Cluster Names** field.
   - To create a clustered host profile, enter a host name (or set of host names) followed by a pipe (|) and then the name of your cluster. This entry identifies your cluster membership.
3. Enter a profile name in the **Profiles** field.
4. Click **Save Profile**.
5. Stop and start the Agent as described in "Stopping and Re-Starting the Secure Path Agent" on page 4–6.

Editing an Existing SPM Storage Profile

To edit an existing SPM storage profile while in the **Secure Path Login** window:

1. Click on the drop down arrow in the **Profiles** box.
2. Select the profile you want to edit.
3. Make the desired changes to the profile.
4. Click **Save Profile**.
5. If you did not choose to save the password when you originally created the profile, enter the password in the **Password** field
6. Click **Login**.

Saving an SPM Storage Profile

To save an SPM profile while in the **Secure Path Login** window:

1. Create or edit a storage profile as described in the previous sections.
2. Enter a unique name in the **Profiles** field.
3. Save the profile by clicking **Save Profile**.
4. Stop and start the Agent as described in "Stopping and Re-Starting the Secure Path Agent" on page 4–6.

Creating a Storage Profile Password

SPM uses the Storage Profile password to establish a network connection with the Secure Path hosts. For storage profiles, including more than one host, the connection password must be the same on each of the Secure Path hosts.

To create a storage profile password:

1. Add the host names to your storage profile as described in SPM Storage Profiles.
2. Enter the connection password in the **Password** field.

   This is the same password that you defined for the Secure Path Agent during setup, or when you ran the Secure Path Agent Configuration utility after installation.
3. Check **Save Password** if you want SPM to use the saved password automatically each time you login with this storage profile.

Changing the Secure Path Agent Password

To change the Secure Path Agent's password:

1. Select **Start** > **Programs > SecurePath > SecurePathCfg**. You access the **Secure Path Agent Configuration Utility** window as shown in Figure 4–2.

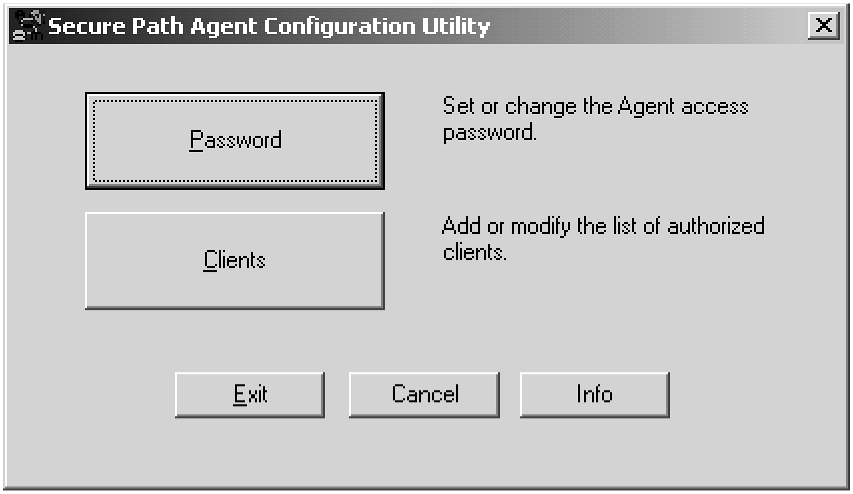

Secure Path Agent Configuration Utility
Password
Set or change the Agent access password.
Clients
Add or modify the list of authorized clients.
Exit
Cancel
Info

Figure 4–2: Secure Path Agent Configuration Utility window

2. Click **Password**.
3. Enter the new password.
4. Enter the new password again to verify accuracy.
5. Click **OK**
6. Stop and start the Agent as described in Stopping and Re-Starting the Secure Path Agent in the next section.

Stopping and Re-Starting the Secure Path Agent

After modifying a password or configuring client access, stop and restart the Agent by performing the following procedure:

1. Select **Start > Settings > Control Panel > Administrative Tools Services**.
2. Find and select the Secure Path Agent in the list of services and click **Stop**.
3. Wait for the Agent to stop, then select Secure Path Agent again and click **Start**.

SPM Client Access

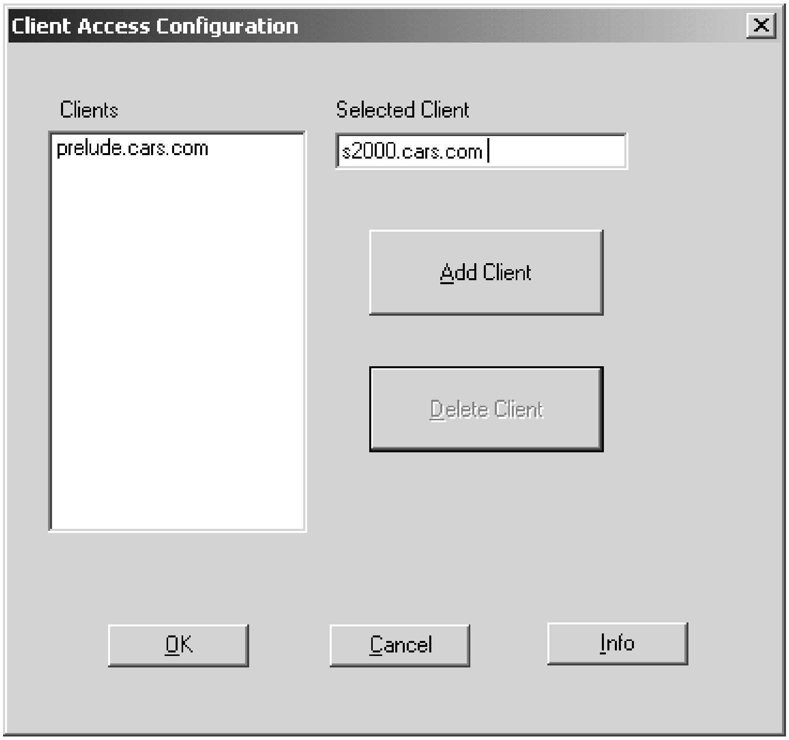
Secure Path incorporates an authorized client database on the storage servers. Only clients authorized by the server may connect to the Secure Path Manager.

Configuring Client Access

1. Access the host where you want to authorize a client.
2. Select **Start** > **Programs > SecurePath > SecurePathCfg**.

   The **Secure Path Agent Configuration Utility** window is displayed as shown in Figure 4–2.

3. Click **Clients.** The **Client Access Configuration** window is displayed as shown in Figure 4–3.



Clients: prelude.cars.com

Selected Client: s2000.cars.com

Figure 4–3: Client Access Configuration window

4. Enter a new client in the **Selected Client** field.
5. Enter a fully qualified domain name (FQDN) in the **Clients** field.
6. Click **Add Client**.
7. Click **OK**.
8. Stop and start the Agent as described in "Stopping and Re-Starting the Secure Path Agent" on page 4–6.

Removing Client Access

1. Access the host where you want to authorize a client.
2. Select **Start** > **Programs > SecurePath > SecurePathCfg**.

   You access the **Secure Path Agent Configuration Utility** window as shown in Figure 4–2.
3. Click **Clients.** The **Client Access Configuration** window is displayed as shown in Figure 4–3**.**
4. Highlight the client you want to remove in the **Selected Client** field.
5. Click **Delete Client**.
6. Click **OK**.
7. Stop and start the Agent as described in "Stopping and Re-Starting the Secure Path Agent" on page 4–6.

Troubleshooting Connection Problems

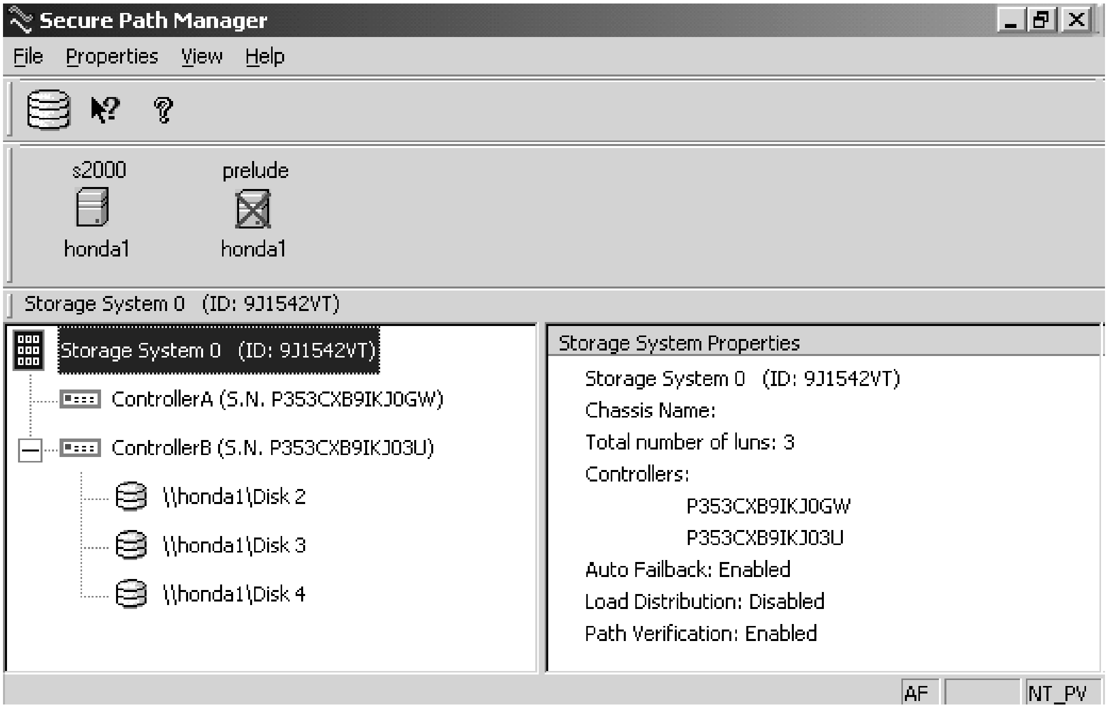
If you experience problems attempting to login to SPM, see Appendix A, Troubleshooting Secure Path Connection Problems, for more information.

Monitoring Host Connections

SPM monitors the connection status for each active host that is a member of the current storage profile.

A server icon is displayed for each host in the window frame located immediately below the tool bar. The host’s name is listed above the icon, and a cluster name is listed below if it is a member of a cluster.

SPM monitors its connection with each member of a storage profile and indicates a loss of connection to a particular host with a red “X.” Figure 4–7 shows SPM has lost connection to the “Honda1” cluster member “prelude.”



Storage System 0 (ID: 9J1542VT)

Storage System 0 (ID: 9J1542VT)
ControllerA (S.N. P353CXB9IKJ0GW)
ControllerB (S.N. P353CXB9IKJ03U)
\\honda1\Disk 2
\\honda1\Disk 3
\\honda1\Disk 4

Storage System Properties

Storage System 0 (ID: 9J1542VT)
Chassis Name:
Total number of luns: 3
Controllers:
P353CXB9IKJ0GW
P353CXB9IKJ03U
Auto Failback: Enabled
Load Distribution: Disabled
Path Verification: Enabled

Figure 4–4: Lost host connection

Responding to a Lost Host Connection

When investigating possible problems with lost host connections, consider the following:

- A loss of connection does not necessarily mean that you have lost Secure Path's protection capability for storage on that host. If the host is still running, the problem is most likely due to a network connectivity problem and you have lost Secure Path remote management functions. Secure Path's RaiDisk multiple path driver is still protecting availability to your storage.
- One node of the management cluster has failed.
- If the host is a member of a cluster, SPM will continue to report storage information based on data received from the surviving host or hosts.

- If the host is a member of a cluster, check your cluster management utilities to determine whether storage resources have failed-over to a surviving host.
- If the host is still running or following a reboot, run the **Windows Event Viewer** and examine the Application and System logs to determine what happened prior to and during the loss of connection. In particular, check for network issues that may have caused a connectivity problem between the host and the SPM client.
- SPM will automatically re-establish communication to a host when the connection becomes available.

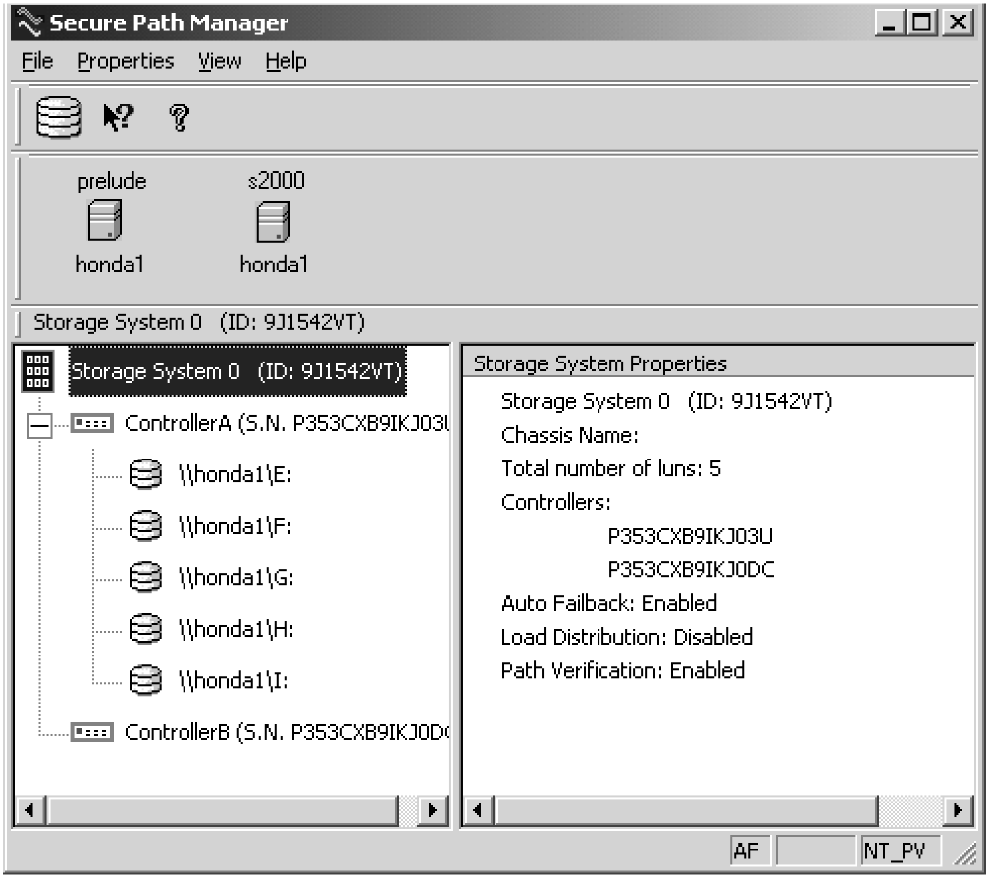
Setting Storage Profile Properties

After logging-on to SPM for the first time, examine and adjust the ***Properties*** settings for the current storage profile. These ***Properties*** have a global effect on all resources managed by an SPM storage profile. Use the **Properties** drop-down menu to:

- Enable or Disable the **Auto-Failback** policy (default = *disabled*). When Auto-Failback is enabled, all storagesets that have failed-over to an alternate path will automatically failback to their Preferred path when access to that path is restored. Storagesets will failback automatically only if I/O operations to those storagesets are in process. Auto-failback enabled in conjunction with Path Verification, permits failback to occur for quiescent storagesets.
- Enable or Disable **Path Verification** (default = *enabled*). With Path Verification enabled, Secure Path periodically runs diagnostics on all Preferred and Alternate paths to determine their current state. If a path is diagnosed with a problem that would prevent reliable I/O operations to complete, it is marked as FAILED and no further I/O operations are permitted on that path.
- Set the **Polling Interval** (default = *90 seconds*) to determine the rate at which SPM will request configuration change information from the Secure Path Agents in the storage profile. Polling Interval only affects the rate at which displayed information is updated and has no affect on the current configuration. The Polling Interval is user-selectable from a minimum 5 seconds to a maximum of 30 minutes.

Storage System View

Physical storage objects are displayed in the SPM Storage System view located in the left frame (Figure 4–5). Browsing this view will display each of the RAID storage systems, controllers, and associated storagesets that comprise your Secure Path storage profile. Objects in the Storage System view are described in the following sections.



Storage System 0 (ID: 9J1542VT)

Storage System 0 (ID: 9J1542VT)

ControllerA (S.N. P353CXB9IKJ03

\\honda1\E:

\\honda1\F:

\\honda1\G:

\\honda1\H:

\\honda1\I:

ControllerB (S.N. P353CXB9IKJ0D

Storage System Properties

Storage System 0 (ID: 9J1542VT)
Chassis Name:
Total number of luns: 5
Controllers:
P353CXB9IKJ03U
P353CXB9IKJ0DC
Auto Failback: Enabled
Load Distribution: Disabled
Path Verification: Enabled

Figure 4–5: SPM single host storage profile – Storage System view

Storage Systems and Controllers

- **Storage System ID**–Each MSA1000 storage system is identified by a unique 64-bit value.

  For MSA1000 storage systems, the Storage System ID is determined at the time of manufacture and stored in controller NVRAM. The Storage System ID remains constant for the life of the RAID storage system.

- **Controller Serial Number**–The individual controllers of an MSA1000 storage system are identified by a unique alphanumeric value assigned during controller manufacture.

RAID Array Storagesets

Select the method SPM uses to identify storagesets with the **View** drop-down menu located above the toolbar. SPM will always display the owning host's name or clustered name (for clustered hosts) along with whatever storageset identifier you choose.

- **Disk LUN UUID**–A unique 128-bit value assigned by Secure Path.
- **Disk Number**–The logical disk number assigned by the Windows Disk Administrator, or Disk Management.
- **Drive Letter**–The logical drive letter assigned by the Windows Disk Administrator, or Disk Management.
- **Bus/Target/LUN**–The physical address representing the connection to the host server.
- **Volume Label–**The label assigned to the volume by the user with Windows Explorer, Disk Administrator or Disk Management.

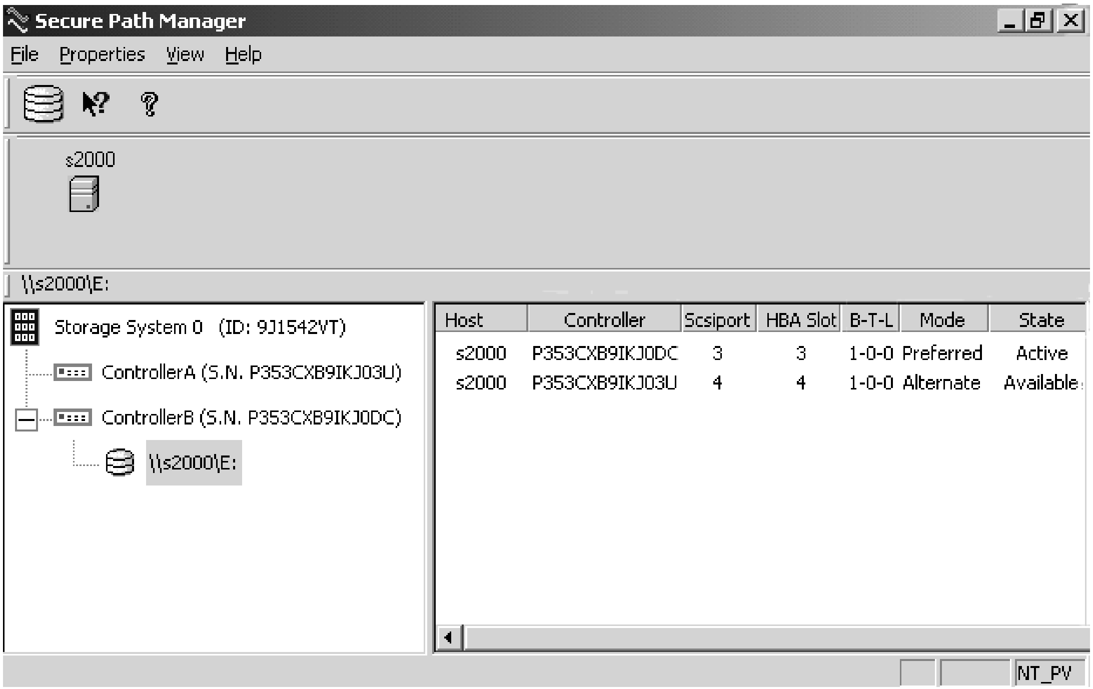
Physical Path View

When you highlight a storageset from the Storage System view, SPM displays information about the physical paths that have been configured for access to that storageset in the right-hand frame. The Physical Path view includes the following information for each path:

- **Host**–The Secure Path host system which has an established access path to the storageset.
- **Controller**–The RAID storage system controller servicing the path.

- **Scsiport**–The physical port number of the HBA servicing the path. The HBA is a relative number determined by the "order of discovery" for adapters on that host.
- **B-T-L**–The physical Bus, Target, and LUN number describing the path address for the storageset.
- **HBA Slot**–Identifies the host node PCI slot containing the identified HBA (Windows 2000 only).
- **Mode**–A user-selectable parameter that specifies path behavior during nominal and failure conditions. Path mode may be set to Preferred, Alternate, or Alternate-Offline. See "Path Mode" on page 1–7 for more information.
- **State**–A set of attributes that describe the current operational condition of the path. Paths may exist in Active, Failed, or Available states. See "Path State" on page 1–7 for more information.

The **Secure Path Manager** window presented, in Figure 4–6, shows a single host configuration with the host "S2000" attached to two Secure Path-protected RAID storage systems.



Secure Path Manager
File
Properties
View
Help
s2000
\\s2000\E:
Storage System 0 (ID: 9J1542VT)
ControllerA (S.N. P353CXB9IKJ03U)
ControllerB (S.N. P353CXB9IKJ0DC)
\\s2000\E:
NT_PV

Host	Controller	Scsiport	HBA Slot	B-T-L	Mode	State
s2000	P353CXB9IKJ0DC	3	3	1-0-0	Preferred	Active
s2000	P353CXB9IKJ03U	4	4	1-0-0	Alternate	Available

Figure 4–6: SPM single host storage profile – Physical Path view

The storageset with Windows logical drive letter `E` is highlighted in the Storage System view, and its corresponding physical path information is presented in the right-hand frame. Each line in the Physical Path view represents a discrete path to this particular storageset.

The display information in this example shows two paths configured from host "S2000" to drive `E`.

First Path

Information for the first path indicates that it is in a Preferred mode and Active state.

- The initial starting state is derived from the controller's preferred path attribute or the last owning controller.
- The Preferred mode is selected by a user for a given path to specify its use for all I/O operations during normal conditions.
- A path with a Preferred mode that is in the Active state is one that is currently used for access to a storageset under normal operating conditions.

Second Path

Information from the second path indicates that it is in an Alternate mode and Available state.

- The Alternate mode is selected by a user for a given path to specify its use for access to a storageset only after all Preferred paths have failed.
- A path with an Alternate mode that is in the Available state is one that is currently ready to be used for access to a storageset in the event that a Preferred path fails.

The controller serial number displayed for the Preferred path is the same as the one shown in the Storage System view for the controller owning drive `E`.

The path in the Available state that has a different serial number than that of the Preferred mode path indicates that it is providing standby access through the other controller. Should the controller currently servicing the Preferred path completely fail, the path on the surviving controller will transition to the Preferred state.

Polling Interval and Display Refresh

To keep the displayed path status current, SPM periodically requests updates from all Secure Path hosts. To minimize network traffic, SPM performs display updates only when a configuration change is reported and updates only the information that has changed. The rate at which status changes are requested is determined by the Polling Interval that you set from the **Properties** menu.

A display Refresh operation, which you invoke through the **View** menu item or with the **F5** hotkey, causes SPM to request fresh configuration information from all hosts included in the storage profile. SPM updates all displayed information in response to a Refresh request. Since a Refresh will update the entire display, it can take longer to perform than a normal polling operation. How long the Refresh takes depends upon the number of hosts, RAID storage systems, and storagesets in the monitored storage profile.

Managing Storagesets and Paths

This section describes the following actions you can perform on the storagesets and paths managed by SPM:

- Move a storageset from one controller to the other
- Make a path offline
- Make a path online
- Verify a path
- Repair a path.

The following SPM actions are built into the SPM GUI, but appear grayed-out, as they are not applicable to MSA1000 storage systems.

- Make a path Alternate
- Make a path Preferred
- Change the Preferred path
- Load Distribution.

Moving a Storageset

Choose **Move a Storageset** to change the ownership from the current RAID Array controller to the other. This action is useful if you need to balance I/O loading across controllers or to manually return a failed-over storageset to its Preferred path when Auto-Failback has been disabled.

NOTE: All LUNs on the specified MSA1000 storage systems move together, as a group, between controllers.

There are two methods available to move a storageset.

1. Click the drive to highlight it in the storage system view.
2. Choose one of the following:
   - Drag the drive to the other controller
   - Right click to select the **Move To Other Controller** action.

Making the Alternate Path Offline

Choose **Make a Path Offline** to prevent a path from being used for any I/O operations under any circumstances. For instance, use the Offline mode to replace or work on a storage interconnect component. To make an alternate path offline:

1. Click a Alternate path.
2. Right click and select **Make Offline**.

The selected Alternate path’s mode will change to Alt-Offline.

Making a Path Online

Choose **Make a Path Online** to return a path that is currently in the Alt-Offline or Pre-Offline mode to its original mode. To make a path online:

1. Click a path in the Alt-Offline or Alt-Online mode.
2. Right click to select the **Make Online** action.

If the path was Alt-Online, its mode will change to Alternate. If the path was Pre-Offline, its path will change to Preferred.

Verifying a Path

Choose **Verify a Path** when you want SPM to determine the current state of a path. To verify a path:

1. Click the path.
2. Right click to select the **Verify Path** action.

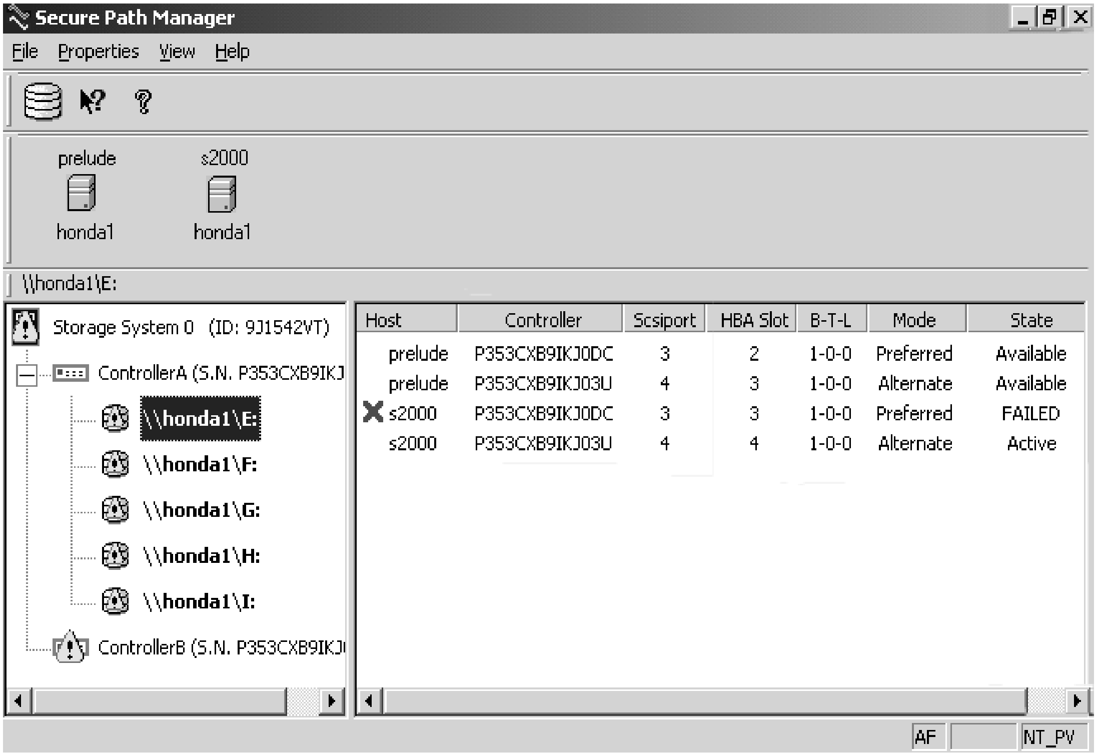
SPM will generate a pop-up message when the verification completes to indicate the result of the operation. No state change will occur as a result of this operation.

Repairing a Path

Choose **Repair a Path** when you want SPM to restore access to a failed path after the problem has been corrected. To Repair a path:

1. Select a path in the Failed state.

   A red X beside a path, as shown in Figure 4–7, indicates a path in a failed state.



Host	Controller	Scsiport	HBA Slot	B-T-L	Mode	State
prelude	P353CXB9IKJ0DC	3	2	1-0-0	Preferred	Available
prelude	P353CXB9IKJ03U	4	3	1-0-0	Alternate	Available
✗ s2000	P353CXB9IKJ0DC	3	3	1-0-0	Preferred	FAILED
s2000	P353CXB9IKJ03U	4	4	1-0-0	Alternate	Active

Figure 4–7: Lost path connection

2. Select **Verify Path**.
3. You see a message box stating if the path verification was successful.
   - If path verification is successful right click and select **Repair Path**.

     If the Repair action is completed successfully the path's state will change to Available if its mode is Alternate, or Active if its mode is Preferred.
   - If path verification was unsuccessful, check the Windows Event Log to find the reason for the failure.

Detecting and Identifying Path and Controller Failures

SPM periodically monitors the status of all systems in your storage profile at a rate determined by the Polling Interval. To indicate failures, icons are used in the Storage System view, and path states are set to FAILED in the Physical Path view.

In addition, failover events are logged by the RaiDisk driver in the **Windows Event Viewer**. You should routinely monitor SPM status to check for occurrences of failover events that might compromise either the performance or availability of storage resources.

The SPM client is not required to be running for Secure Path to protect path availability. RaiDisk device driver running on the host handles Secure Path's automated path protection capability.

Detecting Path Failures

Several types of icons appear in the SPM display to indicate the presence of a path failure. Recognizing these icons will help you to determine the specific storageset and path associated with the failure. The icons shown below are displayed in the storage System View to indicate that a path failure has been detected by Secure Path.

Storage System Path Failure Detected

The icon shown in Figure 4–8 indicates that a failure of at least one, but not all paths to that RAID Array storage system, was detected by Secure Path. Browse the storage system to determine the affected controller and storagesets.

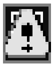


Figure 4–8: Storage system path failure detected

Storage Controller Path Failure Detected

The icon shown in Figure 4–9 indicates that a failure of at least one, but not all paths to that storage controller were detected by Secure Path. Browse the storage controller to determine the affected storagesets.

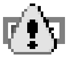


Figure 4–9: Controller path failure detected

Unless you have the Path Verification property enabled, Secure Path only detects failures for paths with active I/O processing. This means that it is possible that one or more paths may be failed to other storagesets owned by the same controller, but not yet detected by Secure Path. However, Secure Path will perform path or controller failover of these drives, and indicate the failure if subsequent I/O occurs to any or all of the storagesets.

If you have Path Verification enabled, Secure Path will automatically detect the failure of paths to all of the affected storagesets on the controller and immediately perform whatever path or controller failover activity is necessary to maintain availability.

Storageset Path Failure Detected

The icon shown in Figure 4–10 indicates that a failure of at least one, but not all paths to that storageset was detected by Secure Path. Click on the storageset to highlight it and examine the Physical Path view information to determine the specific nature of the path failure.

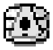


Figure 4–10: Storageset path failure detected

Total Path Failures

Each of the icons shown below indicates that all paths to the affected storage object have failed.

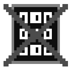


Figure 4–11: Storage system failure detected

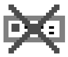


Figure 4–12: Storage controller failure detected

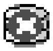


Figure 4–13: Storageset failure detected

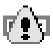


Figure 4–14: State of failed path

Identifying Path Failovers

To identify the source of path failover activity,

1. Check the Storage System view for path failed icons.
2. Examine the Physical Path view of the affected storageset.
3. Check for paths that indicate Failed status.

Whether you see one or more paths to a particular storageset in the Failed state, will depend upon the following conditions:

Table 4–1: Identifying a Failed State

Condition	Description
Was I/O active on the affected storageset?	Secure Path determines path failures by detecting the failure of I/O operations to complete. This means that if I/O was not active on a broken Preferred path, the fault will not be detected and the path's state will not be marked as FAILED until I/O operations occur.
Is Path Verification enabled?	Path Verification periodically tests the viability of all paths and will automatically detect faults on all Preferred and Alternate paths. This means that a controller failover on installations with multiple paths to a storageset, will result in FAILED states for both the Preferred and Alternate paths to the failed controller.

Identifying Controller Failovers

A RAID Array controller failure will cause Secure Path to change the ownership of a given storageset to the surviving controller. Failover will occur only for those storagesets with active I/O operations. If you suspect that a controller failover has occurred, use the Path Verification feature to check the viability of all configured paths. Although you may enable it at anytime, Path Verification will require approximately two minutes per storageset to verify the integrity of all paths in the storage profile.

The Path Verification diagnostics will identify the specific failing controller in the Storage System view. Check for the failed storage controller icon shown in Figure 4–12. SPM will show that all storagesets previously on this controller have been failed-over to the surviving controller. Because all of the Alternate paths to the faulty controller have transitioned to the Failed state because of Path Verification, storageset path failure icons will be displayed for each storageset on the surviving controller.

Responding to Failover Events

When investigating possible problems with failovers, consider the following:

- Are there additional Available paths remaining to the storageset, or has this failure totally eliminated the ability to survive any subsequent failures?
- What caused the failure?

Most storage channel problems are caused by failures in the interconnect hardware. To determine what occurred prior to and during a failure, perform the following actions:

1. Examine the **Windows Event Viewer** and review the System log for events entered by the RaiDisk and/or host bus adapter device drivers.
2. Check the Application Log for events entered by the Secure Path Agent and SPM.
3. Visually inspect your switches or hubs for LED, LCD or HBA hardware fault indications.

Using Secure Path Manager with Microsoft Cluster Service

In MSCS environments, the SPM display will always show the associated cluster name alongside the storageset in the Storage System view. When you highlight a storageset, SPM will display all of the physical paths from each cluster host to that particular storageset in the Physical Path view.

MSCS uses hardware device reservation as a mechanism to synchronize drive access. Device reservation means that a shared storageset is in effect “owned” by a single cluster host at any given time. You can determine the owning host from SPM by looking for the storageset path in the Active state. A non-owning host is indicated by a storageset path in the Preferred mode and Available state.

5

Removing Secure Path Software

This chapter describes how to remove Secure Path software from your server as required to resume a single path RAID storage environment.

To remove Secure Path software from your system:

1. Select **Start** > **the Settings > Control Panel**.
2. Choose **Add/Remove Programs**.
3. Select **SANworks Remove Secure Path Client**, if applicable.
4. Click **OK** in the resulting window.
5. Select **SANworks Remove Secure Path Server**.
6. Click **OK** in the resulting window.
7. Shut down the system.
8. Remove redundant paths from the controller pairs.

The Secure Path software removal process is complete.

NOTE: To aid in the reinstallation of Secure Path, the file *client.ini* is not removed.

A

Troubleshooting Secure Path Connection Problems

This appendix provides the following Secure Path network connectivity troubleshooting information:

- Client/Agent Considerations
- Network Considerations.

If further assistance is required, please contact in North America, the Compaq technical support at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week.

Outside North America, call the nearest Compaq technical support. Telephone numbers for worldwide Technical Support Centers are listed on the Compaq website. Access the Compaq website: http://www.compaq.com.

Client/Agent Considerations

The following Client/Agent considerations may be useful in troubleshooting network connection problems:

- Add each client’s NetBIOS name or Fully Qualified Domain Name (FQDN) to the Agent's list of authorized clients using the Agent Configuration utility, and set the password in the Password Dialog Box. Once you have made the modifications, stop then restart the Secure Path Agent to update the database using the Services applet from Control Panel.
- Make sure that you use the same name type, either NetBIOS or FQDN, during Secure Path client login that you have entered in the Agent's database.
- Each name you use must be mapped to its network IP address using one of the following:
  - — *HOSTs* file (static text file with either NetBIOS or FQDN mapped to IP)
  - — Windows Internet Naming Service (WINS with a NetBIOS name)

— Domain Name System (DNS with an FQDN).

See Network Considerations below for more information.

- In cluster configurations, make sure that the password you choose is common for both agents in the cluster.
- Secure Path does not use domain authentication to authorize clients. Client authentication is handled for each Agent using name-to-IP address resolution and password verification from the Secure Path configuration database.
- If multiple volume letters are displayed under one LUN, go to the Disk Manager and check basic disks. Dynamic Disks are not supported.

Network Considerations

The following network considerations may be useful in troubleshooting network connection problems:

- Client names up to 15 letters without a dot (".") can be resolved by NetBIOS broadcast resolution, as long as the client and agent nodes are configured on the same subnet. If the client and agent are located on different subnets, then you must use the *LMHOSTs* file, *HOSTs* file, WINS, or DNS to resolve the address.
- If you use the *LMHOSTs* file, make sure that the **Enable LMHOSTs Lookup** box is checked in the TCP/IP protocol properties of the client system.

1. On the client system, enter the NETBIOS name and the IP address, of the Agent you wish to connect with in the *LMHOSTs* file and save it.
2. Click the **Import LMHOSTs** button to specify the location of the *LMHOSTs* file. The *LMHOSTs* and *HOSTs* files are normally located in the \system32\drivers\etc subdirectory.
3. Issue the `NBTSTAT -R` command to purge and reload the remote name table.

- Client names that exceed 15 letters or carry a dot require an entry for that name in the *HOSTs* file or resolution by a DNS server. It is also possible to have DNS resolve NetBIOS names as long as the DNS server is updated with the appropriate information. Make sure you have checked the **Enable DNS for Resolution** box in the TCP/IP protocol properties of the client system.
- If you are using DNS for host name-to-IP resolution, then the DNS database on the DNS server must be updated with the appropriate information.
- For best network connection results, use the FQDN with DNS.

- For production environments, where management and security are a concern, use the FQDN with DNS name resolution.
- For test and evaluation environments, it is usually easier to add the server's name to the client's *HOSTs* file and the client's name to the server's *HOSTs* file.
- Make sure that you can ping the Secure Path host, both locally and from a remote host using the host name, not the IP address.
- If you are using MCS Software, ensure that you have the proper network adapter binding order.

  a. On the Windows **Start** menu, select **Settings** > **Control Panel**.

  b. Double-click **Network** and **Dial-up Connections**.

  c. Select **Advanced** settings, on the **Advanced** menu.

  d. In the **Connections** box, make sure your bindings are ordered as follows:

     — First: external public network

     — Second: internal private network

     — Third (if applicable): remote access connections.

  e. Re-order your bindings if necessary.

Glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

Bus

- For parallel SCSI configurations, the bus is a number assigned to the physical interconnects emitted by an HBA.
- For Fibre Channel configurations, HBAs may use multiple bus numbers as an artificial method of expanding bus address space.

Controller

A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSG80, RA4X00, MSA1000 and HSG60 array 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 comprised 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 SCSI bus or SAN (Storage Area Network).

Host

A host is a computer system on which the Secure Path server software (RaiDisk driver and Agent service) is running.

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.

Mode

Mode is a user-selectable parameter that specifies path behavior during nominal and failure conditions. Paths may be set to one of the following modes:

- **Preferred**–Indicates the desired I/O paths. When Load Distribution is enabled, I/O is distributed to a LUN using all available preferred paths according to a round-robin policy. When Path Verification is enabled, all preferred paths would be verified.
- **Alternate**–Indicates a path is used only for device access once all Primary Paths to the device have failed. Paths in this mode participate in path-verification, if enabled.
- **Offline**–Indicates a path that will not be used for I/O to a LUN. The Offline mode is logically or'd with one of the other two path modes.

Path States

Attributes that describe the current operational condition of a path. A path may exist in the following 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.

PortA

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.

SCSI

Small Computer System Interface. A parallel interface standard.

State

State is an attribute that describes the current operational condition of an object. See Path, Path States and Attribute, Controller States, and Device States.

Target

- For parallel SCSI configurations, the target is the actual target number assigned to a device.
- For Fibre Channel configurations, the target number is assigned by a mapping function at the mini-port driver level and is derived from ALPA (Arbitrated Loop Physical Addresses) in a FC-AL topology.
- For SAN switched fabric, a target is assigned to a WWPN. This target can have values between 16 and 125.
- For a fabric topology, target is a mapping function derived from the order of discovery according to port connections at the SAN (Storage Area Network) switch.

Topology

An interconnection scheme that allows multiple servers and storage devices to communicate. Arbitrated Loop and switched fabric are examples of Fibre Channel topologies.

Index

A

active/passive implementation 1–4
addressing, SCSI 1–5
agent password 4–5
agent, stopping and re-starting, Secure Path Agent, stopping and restarting 4–6
anti-thrash filter 1–3, 1–8
array configuration utility 1–5
authorized reseller, Compaq xi
auto-failback 1–3

B

B-T-L 4–13
Bus/Target/LUN 4–12
bus/target/LUN 4–12
button names, convention defined vii

C

caution, symbol and definition viii
changing the Secure Path Agent password 4–5
client access
  cancelling 4–8
  configuring 4–6
client access, configuring 4–6
client access, SPM 4–6
Client Software, installing 3–4
Client/Agent considerations A–1
cluster server setup 2–2
command names, convention defined viii
Compaq
  authorized reseller xi
  technical support x
  website xi
connection problems 4–8
connections, monitoring host 4–8
controller 4–12
  operational model 1–4
  ownership 1–4
  serial number 4–12
  states 4–1
controllers, reconfiguring the RAID 5–1
conventions
  button names, defined vii
  command names, defined viii
  dialog box names, defined vii
  directory names, defined vii
  drive names, defined viii
  file names, defined viii
  key sequences, defined vii
  keyboard keys, defined vii
  menu items, defined vii
  menu sequences, defined vii
  named keys, defined vii
  system responses, defined viii
  URLs, defined viii
  user input, defined viii
creating a storage profile password 4–4
creating storage profile 4–3

D

detecting and identifying path and controller failures 4–18
dialog box names, convention defined vii
directory names, convention defined vii
disk LUN ID 4–12
Disk LUN UUID 4–12
Disk Number 4–12
disk number 4–12

display refresh 4–15
drive letter 4–12
drive names, convention defined viii

E

electrical shock hazard, symbol and definition ix
equipment symbols ix
events, responding to failover 4–22
excessive weight, symbol and definition ix

F

failback
  anti-thrash filter 1–8
failback options 1–8
failover events, responding to 4–22
failover operation 1–7
failovers
  controller 4–21
  path 4–21
  responding to events 4–22
features 1–2
file names, convention defined viii
files, storage, defining 4–3

G

getting help x
  Compaq technical support x
  Compaq website xi

H

hardware installation prerequisites 2–1
hardware installation procedures 2–2
HBA Slot 4–13
Help, obtaining x
Host 4–12
host connections
  lost connection icon 4–17
  monitoring 4–8
  responding to lost connection 4–9
hot surface, symbol and definition ix

I

icons
  controller path failure 4–19
  storage controller total path failure 4–20
  storage system path failure 4–19
  storage system total path failure 4–20
  storageset failure 4–20
  storageset total path failure 4–20
important, defined viii
installation
  client software 3–4
  de-installing Secure Path software 5–1
  hardware prerequistes 2–1
  hardware procedures 2–2
  prerequisites 3–1
  Secure Path server software 3–3
installing
  Client Software 3–4
  Server Software 3–3
  Standalone Software 3–2

K

key sequences, convention defined vii
keyboard keys, convention defined vii

L

launching SPM 4–3
load balancing 1–3
login SPM 4–2
login window 4–2

M

managing Secure Path 4–1
managing storagesets and paths 4–15
menu items, convention defined vii
menu sequences, convention defined vii
Microsoft Cluster Service environment 4–22
mode 4–13
monitoring host connections 4–8
multiple power source, symbol and definition ix

N

named keys, convention defined vii
network considerations A–2
network interface connection, symbol and definition ix

note, defined viii

P

password
  changing the Secure Path 4–5
password, changing the Secure Path Agent 4–5
password, creating a storage profile 4–4
path
  repairing 4–17
  verifying 4–17
path definition 1–5
  management behavior 1–9
  path status 1–7
  verification 1–8
path management behavior summary 1–9
path mode 1–7
path state 1–7
path states
  active 1–7
  available 1–7
  failed 1–7
path status
  alternate paths 1–7
  mode and state 1–7
  preferred path 1–7
  two offline modes 1–7
path verification 1–3, 1–8
physical path view 4–12
  display refresh 4–15
  polling interval 4–15
  single host storage profile 4–13
polling interval 4–15
profile limits 1–4
profile, creating 4–3
profile, saving 4–4
profile, selecting 4–4
profiles 1–4, 4–3

R

RA4000/4100 components 3–1
rack stability x
RAID Controllers, reconfiguring the 5–1
reconfiguring the RAID Controllers 5–1
removing Secure Path software 5–1
repairing a path 4–17
responding to Failover Events 4–22

S

SCSI addressing 1–5
Scsiport 4–13
Secure Path
  Agent defined 1–4
  auto-failback 1–3
  manager defined 1–4
  managing 4–1
  overview 1–1
  path verification 1–3
  profiles 1–4
  setup defined 1–4
  software components 1–4
  technology 1–2
Secure Path environment
  physical path view 4–12
  RAID Array storagesets 4–12
  storage system view 4–11
  system view window 4–11
Secure Path functions 1–3
Secure Path login 4–2
Secure Path Manager
  about 4–1
  changing Agent password 4–5
  creating storage profile 4–3
  defining storage files storage files, defining 4–3
  launching 4–3
  login window 4–2
  saving storage profile 4–4
  selecting storage profile 4–4
  setting Storage Profile properties 4–10
  storage profile password 4–4
  system view window 4–11
Secure Path software, removing 5–1
Secure Path, technical description 1–1
server setup, standalone 3–2
Server Software, installing 3–3

setup, standalone server 3–2
software components 1–4
SPM 4–1
  configuring client access 4–6
  storage profile password 4–4
  storage profiles 4–3
SPM client access 4–6
standalone server setup 3–2
Standalone Software, installing 3–2
state 4–13
static load balancing 1–3
stopping and re-starting the Secure Path Agent 4–6
storage profile
  setting properties 4–10
storage profile, creating 4–3
storage profile, saving 4–4
storage profile, selecting 4–4
storage profiles 4–3
storagesets
  controller path failure 4–19
  detecting path failures 4–18
  making a path offline 4–16
  making a path online 4–16
  managing 4–15
  moving 4–16
  path failure icons 4–19
  repairing a path 4–18
  storageset path failure icon 4–20
  total path failures 4–20
storagesets and paths, managing 4–15
symbols
  in text viii
  on equipment ix
system responses, convention defined viii

T

technical description of Secure Path 1–1
technical support, Compaq x
text symbols viii
troubleshooting
  client/agent considerations A–1
  connection problems 4–8
  detecting path failures 4–18
  host connection monitor 4–9
  identifying controller failovers 4–21
  identifying path failovers 4–21
  lost host connection icon 4–17
  monitoring host connections 4–8
  network considerations A–2
  path failure icons 4–19
  responding to failover events 4–22
  responding to lost host connection 4–9
  total path failures 4–20

U

uninstall Secure Path software 5–1
URLs, convention defined viii
user input, convention defined viii
using SPM with MSCS Clusters 4–22

V

verifying a path 1–8, 4–17
volume label 4–12

W

Warning
  electrical shock hazard symbol, defined ix
  excessive weight symbol, defined ix
  hot surface symbol, defined ix
  multiple power source symbol, defined ix
  network interface connection symbol, defined ix
warning
  symbol and definition viii
websites
  Compaq storage xi
  Compaq technical support x