Compaq SANworks™

Secure Path Version 3.0 for Novell NetWare

Installation and Reference Guide

First Edition November 2000
Part Number: AA-RN72A-TE
Compaq Computer Corporation

Compaq SANworks Secure Path Version 3.0 for Novell NetWare Installation and Reference Guide
First Edition (November 2000)
Part Number: AA-RN72A-TE

Contents

Chapter 3

Hardware Setup for Fibre Channel

Chapter 4

Installing Secure Path Software

Chapter 5

Managing Secure Path

Chapter 6

Using Secure Path with SWCC

Figures

Tables

About This Guide

This guide is designed to be used as step-by-step instructions for installation and as a reference for operation, troubleshooting, and future upgrades.

Text Conventions

This document uses the following conventions to distinguish elements of text:

Keys	Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously.
USER INPUT	User input appears in a different typeface and in uppercase
FILENAMES	File names appear in uppercase italics.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital letters.
COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in upper case. **NOTE:** UNIX commands are case sensitive and will not appear in uppercase.
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to enter information, type the information and then press the **Enter** key.

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 loss of information.

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

These icons may be located on equipment in areas where hazardous conditions may exist.

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

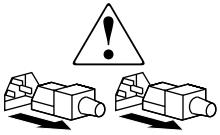
WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

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. If this surface is contacted, the potential for injury exists.

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 equipment is supplied by multiple sources of power.

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

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 manual material handling.

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.
- The stabilizing feet are attached to the rack if it is a single rack installations.
- The racks are coupled together in multiple rack installations.
- A rack may become unstable if more than one component is extended for any reason. Extend only one component at a time.

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

Compaq Technical Support

You are entitled to free hardware technical telephone support for your product for as long you own the product. A technical support specialist will help you diagnose the problem or guide you to the next step in the warranty process.

In North America, call the Compaq Technical Phone Support Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week.

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

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for world wide Technical Support Centers are listed on the Compaq website. Access the Compaq website by logging on to the Internet at http://www.compaq.com.

Be sure to have the following information available before you call Compaq:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level
- Detailed, specific questions

Compaq Website

The Compaq website has latest information on this product as well as the latest drivers. You can access the Compaq website by logging on to the Internet at http://www.compaq.com/storage.

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.

Chapter 1

Theory of Operation

Overview

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

- StorageWorks Fibre Channel Modular RAID Array 8000
- RAID Array 4000/4100
- Enterprise Storage Array 12000

Secure Path eliminates the RAID controller, host bus adapter (HBA), and interconnect hardware (cables, hubs or 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 a unique HBA port on the server, and ends at a unique RAID controller port in the storage system.

Features

Secure Path provides the following features:

- Allows a single instance of Secure Path Manager (SPM) to control Novell and Windows hosts simultaneously.

- Allows StorageWorks dual-controller RAID systems and host servers equipped with multiple HBAs redundant physical connectivity along Fibre Channel Arbitrated Loop (FC-AL) or Fibre Channel switched fabric paths.
- Monitors each path and automatically re-routes I/O to a functioning alternate path if an HBA, cable, hub, switch, or controller failure occur.
- 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.
- 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 on HSG80 based controllers.
- 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.

Secure Path Technology

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 will seek alternate paths through available Fibre Channel hubs or switches, controllers, controller ports, and/or host bus adapters. 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 the RAID Levels on MA8000 and RA4000/4100.

Auto-Failback

With auto-failback 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 (SPM) utility.

Load Balancing

Load balancing applies to Windows, in a non-clustered mode. It does not apply to NetWare and RA4000/4100.

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.

Software Components

The Secure Path Software Kit for NetWare includes the following software components:

- Secure Path Manager is the client/server application used to manage multiple path StorageWorks RAID Array configurations. It displays a graphical representation of multiple path environments, indicating status of all configured storage units and paths.
- Secure Path Agent is a NetWare service that communicates with the cpqfc.ham driver on the host server, and Secure Path Manager on the client side. It installs on the host server with the cpqfc.ham driver.
- The cpqfc.ham driver provides the primary failover capability in the Secure Path product. The cpqfc.ham driver supports StorageWorks RAID Array multiple path access.

Each software component of Secure Path makes use of the native error Log to post informational messages as required.

Chapter 2

Technical Description

Overview

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

This chapter provides technical details on the following Secure Path subjects:

- Reference material for managed entity profiles
- Controller ownership requirements
- Path definition details
- Failover operations and options
- Path management behavior summary

Managed Entity Profiles

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. Secure Path Manager uses the concept of the “managed entity” or “profile” to express this working configuration limit.

The profile limits for Secure Path Manager are a maximum of 16 servers (host systems) connected to and sharing up to 16 storage systems, configured for multiple-bus failover mode. The host servers may be standalone servers or grouped into clusters and may contain a mixture of NetWare and Windows systems. All servers in the profile must have access to all of the storage systems listed in that profile.

Secure Path does not provide any mechanism for synchronizing access to or guaranteeing the data integrity of storagesets shared across multiple standalone hosts or clusters. Access to storagesets must be restricted to a single standalone server or a single “clustered” host set.

The Secure Path Manager lets you create multiple profiles stored as separate files in the same directory. Any given server, cluster or storage system may exist in multiple profiles as long as the profile configuration rules described above are followed.

Controller Ownership

HSG80 based 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
- active/active

In the active/passive model, all storagesets are assigned to one of the controller pair for I/O processing with the other controller inactive, but available as a substitute in case of failure on the original. RA4000/4100 activates the active/passive redundancy model.

In the active/active model, I/O may be routed through both controllers simultaneously, providing better performance in addition to high availability.

The MA8000 and EMA12000 RAID Arrays, supported by Secure Path, implement a modified version of the active/active model. While I/O can be processed simultaneously by both controllers, any given storageset is “owned” or online to a host through only one controller. Ownership of a storageset may be transferred to the other controller at any time through a host- initiated command sequence. Since the ownership transfer results in controller cache flushing and I/O wind down, the storageset may become inaccessible for a period of several seconds to complete this sequence. Arbitrary ownership transfers should be avoided by the user, and are never automatically initiated by Secure Path.

Path Definition

Within Secure Path, a path is defined as the collection of physical interconnect components including HBAs, switches or hubs, cables, RAID array controllers and the ports on the controllers.

Some configurations include multiple cascaded switches within a fabric with the switches connected by one or more inter-switch links. These paths are neither directly visible to nor manageable by Secure Path. 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.

Path Definition for Fibre Channel Arbitrated Loop

In FC-AL configurations, devices are accessed within NetWare using conventional SCSI addressing terminology as shown in Figure 2–1. Fibre Channel adapters are referred to as HBAs, which are named and numbered as SCSI ports. The rest of the SCSI address, except for the LUN, is created within the Fibre Channel's driver and is derived from the Arbitrated Loop Physical Address (ALPA) assigned to each port on the MA8000/EMA12000 and RA4000/RA4100 controllers.

The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. Each connected node on an arbitrated loop must have a unique ALPA assigned.

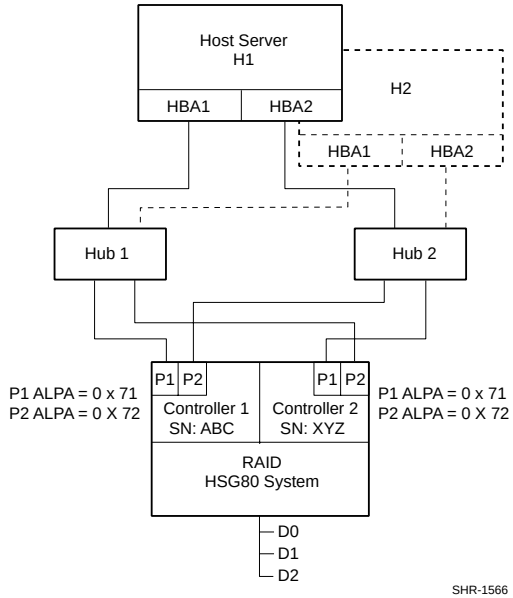


Figure 2–1. Path definition in a Secure Path FC-AL configuration

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

The cpqfc.ham driver for the Compaq 64 bit Fibre Channel Host Bus adapter uses a fixed mapping scheme to translate ALPA assignments to SCSI bus and target ID values.

In most configurations, the same ALPAs are assigned to the respective ports of the MA8000/EMA12000 controllers. Since the ALPA to SCSI address mapping is fixed, this results in identical SCSI B-T-L values for the pair of P1 ports and the pair of P2 ports. The controller serial number information in the display provides a mechanism to correlate path information to a specific controller for maintenance purposes.

> **NOTE:** In FC-AL topology, knowing the ALPA assignment for a particular controller port, allows explicit path resolution to the port level.

Figure 2-2 also shows how the Secure Path Manager displays path information in the event that multiple hosts have access to the same device, as would occur in an MSCS environment.

Path Definition for Fibre Channel - Dual Switched Fabric

Figure 2–2 depicts a dual cascaded switch Fibre Channel topology and the resulting path connection information displayed by Secure Path Manager. Fibre Channel adapters are referred to as HBAs and are named and numbered by NetWare as SCSI ports. The rest of the SCSI address, except for the LUN, is created through the Fibre Channel mini-port driver. It is derived ultimately from Fibre Channel addressing information, which is influenced by connections between the controller, and the switch domain and port number.

In Figure 2–2, Hub 1; Controller 1, Port 1 (C1-P1; ALPA = 0x71) and Controller 2, Port 2 (C2-P2; ALPA = 0x72) constitute one arbitrated loop. Hub 2, Controller 1, Port 2 (C1-P2; ALPA =0x72) and Controller 2, Port 1 (C2-P1; ALPA = 0x71) constitute a second loop.

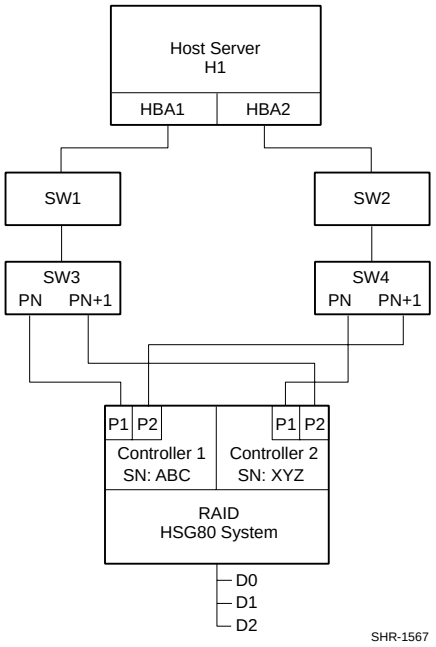


Figure 2–2. Path definition in a Secure Path Dual Cascaded Switch Fibre Channel configuration

The LUN corresponds directly to the Unit Number assigned to the storageset through SWCC or CLI command.

	Host	Controller Serial No.	Host Bus Adapter	Bus-Target-LUN
Drive D: (D1)	H1	ABC	1	1 – 0 – 1
	H1	XYZ	1	1 – 1 – 1
	H1	XYZ	2	1 – 0 – 1
	H1	ABC	2	1 – 1 – 1

In Figure 2–2, devices found on SW3-Pn are assigned the first available bus/target numbers: 1 and 0, respectiv

NOTE: Port driver cpqfc.ham normally reserves Bus 0.

The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. The next port, SW3-Pn+1, gets the next sequential value of 1 - 1. If there were additional storage systems connected, the address mapping would continue incrementing Target numbers up to 31, at which point Bus 2 Target 0 would be assigned.

Because the two independent fabric connections in Figure 2-3 are symmetrical (the lower switch port number is connected to the lower controller port number), the address mapping for the second fabric is identical to the first. The HBA number is the only exception. Although not required for correct operation of Secure Path, symmetric cabling is strongly recommended in Fabric topologies. By following this cabling convention, the controller port number corresponding to a given path in the Secure Path Manager is implied.

Path Status

Secure Path displays Path Status using Path Mode and Path State attributes.

Path Mode may be one of Preferred, Alternate, and Preferred-Offline (pre-offline) or Alternate-Offline (alt-offline).

- **Preferred Path Mode** indicates the user-specified path that will be used to communicate from a specific host to the specified storageset. The user may modify the default driver's path settings using Secure Path Manager.
- **Alternate Path Mode** indicates those that are not user-preferred. These paths provide the redundancy in case preferred paths fail.
- **Offline Path Modes** (Preferred-Offline or 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.

Path State may be Active, Available, or Failed. State is set automatically by cpqfc.ham and reflects current actual path status, which may deviate from user expectations because of path failures.

- **Active State** indicates the associated path is currently servicing, or is capable of servicing I/O to the storageset.
- **Available State** indicates the associated path belongs to the set of redundant paths to the storageset that could be utilized during failover.

- **Failed State** indicates the path has encountered errors either during normal operation or as a result of Path Verification testing.

Chapter 5, ”Managing Secure Path,” provides a more detailed discussion of Path Modes and Path States, and provides illustrative examples of the effects of failover, failback, and user intervention.

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 failed over state while other units appear to remain accessible through that path.

Initially, failover consists of marking a bad path “failed,” which effectively removes it from the list of usable paths for the storageset.

If no Preferred - Active paths remain for the device, Secure Path activates an Alternate - Available path on the same controller, if one exists.

If no Alternate - Available paths remain on the same controller Secure Path attempts to move the device to an Alternate - Available path on the other controller. Additionally, Secure Path sets all Alternate-Available paths to Alternate-Active.

Failover policy is optimized to minimize performance impact to the overall configuration.

Table 2–1 provides a summary chart of path management behavior, conditioned by the several optional features of Secure Path.

Failback Options

Secure Path allows manual or automatic path failback. 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 regardless of whether there is system I/O in process to the selected device.

When set to 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.

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 re-initialized and the failover/failback process repeats if the intermittent failure cause persists.

Path Verification

When enabled, Path Verification causes Secure Path to periodically test the viability of all paths to all storagesets for paths marked Available, Failed, or Active. However, Path Verification does not test paths that are in an offline mode.

Path Verification is useful for detecting failures that affect overall path redundancy before they affect failover capability. If a 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.

Path Management Behavior Summary

Reference the chart in Table 2–1 for a summary of path management behavior conditioned by the optional features of Secure Path.

Table 2–1 Path Management Behavior Summary

No I/O Distribution	Startup	Choose the first path to controller on which LUN is online as **preferred active**. Port does not matter – all other paths on both controllers are marked **alternate available**. If no online path is found, make any available path online and use as **preferred active** – all other paths marked **alternate available.**
	Active Path Failure	Path marked **preferred (or alternate) failed** and fails to any other **alternate available** path on same controller, then other controller – port does not matter. **Alternate available** path used is marked **alternate active**. Behavior is the same with I/O or background path verification. If a LUN is reserved, mark paths **failed**, but do not fail to other path on non-owning node.

Table 2–1 Path Management Behavior Summary (Continued)

	Available Path Failure Path verification	Failed path marked **failed**. Behavior is result of background path verification.
	Path Repaired	Path marked **available.** If autofailback is enabled, failback to **preferred** path from **available** path as regular "autofailback" function. If LUNs reserved, mark path **available** but do not autofailback on non-owning node.
With I/O Distribution (LUN reservation not supported)	Startup	Choose all paths to controller on which LUN is online as preferred active. Port does not matter – all paths to other controller marked alternate available. If no online path is found, make any available path online and use as preferred active – all other paths marked alternate available.
	Active Path Failure	Path marked (**preferred or alternate**) **failed**. If path is **preferred active**, change to **alternate available** on same controller, then other controller. Behavior is the same with I/O or background path verification.
	Available Path Failure Path Verification	Path marked **failed**. Behavior is result of background path verification.
	Path Repaired	Path marked **available.** Path made **active** if **preferred**, and other preferred paths are active. If autofailback is enabled, failback to **preferred** paths from **available** as regular "autofailback" function.

Chapter 3

Hardware Setup for Fibre Channel

Overview

This chapter contains two sections:

- *Installing an RA4000/4100 Secure Path Configuration*, on page 3–2
- *Components Required for MA8000/EMA12000 Fibre Channel Secure Path Installation*, on page 3–4

This chapter provides the following Secure Path Fibre Channel hardware setup information:

- Reference material for high-availability connection options
- Installation prerequisites
- Installation procedures for new Secure Path Fibre Channel configurations
- Installation procedures for building Secure Path into existing Fibre Channel configurations

Before installing Secure Path on a new or existing Fibre Channel (FC) configuration, first review the MA8000/EMA12000 found on the Compaq website. This information will familiarize you with various high-availability connection layouts for FC devices and cabling.

Components Required for RA4000/4100 Fibre Channel Secure Path Installation

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 Technical Phone Support Center at 1-800-OK-COMPAQ.

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

Table 3–1 Secure Path RA4000/41000 Fibre Channel Installation Prerequisites

Host Feature	Requirement
Platform	ProLiant and other x86
Operating System	Novell NetWare 5.x with upgrade service packs
Secure Path Software Kit	SANworks Secure Path for Version 3.0 for Novell NetWare
RAID Storage System(s)	StorageWorks RAID Array 4000 StorageWorks RAID Array 4100 RA4100 Controller Firmware Version 2.58
Cluster Kit (optional)	Novell NetWare Cluster Services V1.01
Host Bus Adapter(s) (and adapter driver)	StorageWorks 64-Bit/66-MHz Fibre Channel Host Adapter StorageWorks Fibre Channel Host Adapter/P
Fibre Channel Interconnect Hardware	FC-AL Switches, SAN (Fabric) Switches, and Fibre Hubs

Installing an RA4000/4100 Secure Path Configuration

This section provides procedures to install and configure a Secure Path topology for Fibre Channel hardware installation.

Hardware and Standalone Software Setup

New System

1. Install all NetWare servers and all HBAs, referencing the user documentation included with your hardware. Do not connect HBAs to hubs or switches at this time.
2. Install Novell NetWare 5.x Server using SmartStart 4.90 assisted installation utility.
3. Install Secure Path software on all NetWare 5.x servers.
   - ❑ The Secure Path software is installed using the Novell PINSTALL utility. Please refer to Chapter 4. to complete the Secure Path software installation.
4. Shutdown the server
5. Install all of the new RAID Array storage system and all interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the Fibre Channel equipment.
6. Restart the server
7. Create storagesets and provide unit attributes for LUNs using the Array Configuration Utility (ACU) included with SmartStart 4.90.
8. Use NWCONFIG to create volume(s)

Existing System

1. Power system down.
2. Install HBAs on all NetWare 5.x servers, referencing the user documentation included with your hardware. Do not connect HBAs to hubs or switches at this time.
3. Install and connect all interconnect hardware (hubs/switches) and according to the instructions provided with the installation documentation shipped with Fibre Channel equipment.
4. Power up System.
5. Load CPQFC.HAM driver from the Secure Path CD-ROM. See Chapter 4 for details.
6. Install Secure Path software on all Novell NetWare 5.x server(s).
7. Install the Secure Path software using Novell's PINSTALL utility. Please refer to Chapter 4 to complete the Secure Path software installation.

NOTE: The following restrictions apply to the initial release of the RA41000 SAN Solution:

- RA4x00s can not be shared by more than one cluster
- An RA4x00 owned by a cluster can not be shared with a standalone server(s)
- Redundant RA4x00s can not be shared with non-redundant servers
- Redundant RA4x00s can not be shared by a mix of NT and NetWare servers (all NT or all NetWare is acceptable)
- A server can only support a single or redundant path to the SAN (i.e. a server can not attach to multiple SANs)

Components Required for MA8000/EMA12000 Fibre Channel Secure Path Installation

Verify receipt of the Secure Path software kit and the Fibre Channel (FC) hardware ordered for the installation. If you are missing any component, please contact the account representative or call the Compaq Customer Services Hotline at (800) 354-9000. The basic requirements for Secure Path operation are listed in Table 3–2.

Table 3–2 Secure Path MA8000/EMA12000 Fibre Channel Installation Prerequisites

Host Feature	Requirement
Platform	Proliant and other x86 servers
Operating System	Novell NetWare 5.x with upgrade service packs
Secure Path Software Kit	SANworks Secure Path V3.0 for Novell NetWare
RAID Storage System(s)	StorageWorks dual-redundant MA8000/ EMA12000 (FC)
Host Bus Adapter(s)	Supported models for Novell NetWare: StorageWorks 64-Bit/66-MHz Fibre Channel Host Adapter StorageWorks Fibre Channel Host Adapter/P
FC Interconnect Hardware	FC-AL Switches, SAN (Fabric) Switches, and Fibre Hubs
Service Tools	Appropriate tools to service the equipment

Installing a New MA8000/EMA12000 Secure Path Configuration

This section provides procedures to install and configure a Secure Path topology for new FC hardware installation.

1. Install all of the new RAID storage system and FC interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the FC equipment.
2. 2. Establish a serial link to the RAID system. You may use a serial line connection from the host server or from any PC workstation. Obtain RAID controller status using the StorageWorks Command Console (SWCC) Command Line Interface (CLI) or a terminal emulation program, such as HyperTerminal.
3. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation. For FC-AL configurations, perform step a. For FC Switched Fabric configurations, perform step b. For either, continue with step c.
   a. For FC-AL configurations, set the Arbitrated Loop Physical Address (ALPA) for HSG80 controllers in the RAID system using the following commands:

      ```
      HSG80> set this_controller port_1_topology=offline
      HSG80> set other_controller port_1_topology=offline
      HSG80> set this_controller port_1_al_pa=n+1
      HSG80> set other_controller port_1_al_pa=n+1
      ```

      Where n+1 is an available address:

      ```
      HSG80> set this_controller port_1_topology=loop_hard
      HSG80> set other_controller port_1_topology=loop_hard
      HSG80> set this_controller port_2_topology=offline
      HSG80>set other_controller port_2_topology=offline
      HSG80> set this_controller port_2-_al_pa=n
      HSG80> set other_controller port_2_al_pa=n
      ```

      Where n is an available address:

      ```
      HSG80> set this_controller port_2_topology=loop_hard
      HSG80>set other_controller port_2_topology=loop_hard
      ```

b. For FC Switched Fabric configurations, use the following commands:

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

c. Configure the RAID system controllers for multiple-bus failover mode using the commands below.

```
HSG80 > set nofailover
```

IMPORTANT: The “other” controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel. Wait for two minutes for the controller to boot before proceeding.

```
HSG80 > set multibus copy=this
```

The controllers will restart in multiple-bus mode.

After the other controller has restarted, verify that both controllers are configured for multiple-bus mode by issuing the following commands:

```
HSG80 > show this
```

Verify that the data returned to this command includes the statement that the controller is in a multiple-bus dual redundant configuration.

The controllers are now configured for multiple-bus operation.

IMPORTANT: Do not connect HBAs to any switches/hubs at this time.

---

4. Please refer to Chapter 4 for software installation.

   The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the SANworks Secure Path Software v3.0 for Novell NetWare into the CD-ROM drive. Refer to Chapter 4, ”Installing Secure Path Software,” to complete the Secure Path software installation setup.

5. Shut down the server(s).
6. Connect all HBAs to the switches/hubs.
7. Restart the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.

a. Using SWCC double-click on the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names are listed in the Application Notes. Refer to the SWCC documentation if you need more information about managing connections.

b. Create storagesets and provide unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC.

c. Set Access IDs for each LUN to selectively present it to the appropriate standalone server or clustered servers.

8. Shut down the controllers in all RAID Array cabinets. Refer to MA8000/ ESA 12000 documentation for any timing restrictions that may apply to storageset creation and controller shutdown. Shut down all servers and turn off power. Power-cycle all RAID Array storage systems. If the RAID Array cabinet contains redundant power supplies, be sure to power cycle them simultaneously.
9. Restart all servers and verify the configuration.

You have now completed the configuration procedures required to support the new Secure Path environment. See Chapter 5, "Managing Secure Path," for information on monitoring and managing Secure Path activity using the Secure Path Manager.

Adding Secure Path to an Existing MA8000/EMA12000 Configuration

This section presumes that a single FC path exists between an MA8000 or EMA12000 system and host server.

WARNING: For each RAID system in a production environment being converted to Secure Path operation, be sure that all users have logged off the Novell NetWare server(s) and that all I/O to the RAID system(s) has ceased. Follow normal procedures to backup the storage systems before proceeding.

1. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation:

   a. Configure the RAID system controllers for multiple-bus failover mode, using the following command:

   ```
   HSG80 > set nofailover
   ```

IMPORTANT: The “other” controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel. Wait for two minutes for the controller to boot before proceeding.

```
HSG80 > set multibus copy=this
```

The controllers restart in multiple-bus mode.

After the other controller has restarted, verify that both controllers are configured for multiple-bus mode by issuing the following command:

```
HSG80 > show this
```

Verify that the data returned to this command includes the statement that the controller is in a multiple-bus, dual redundant configuration.

The controllers are now configured for multiple-bus operation.

b. Specify the preferred controller assignment for each storage unit in the configuration, using the following commands:

NOTE: Compaq recommends that, initially, that storagesets be balanced across the controllers. As storage demands are defined, and individual drive throughput requirements are understood, adjustments to the disk I/O path configuration can be made using the StorageWorks Secure Path Manager, as described in Chapter 5.

Use the following command to obtain a list of all units defined in the RAID system:

```
HSG80 > show units
```

Use the following commands to specify preferred_path for units:

```
HSG80 > set (unit #) preferred=this
```

or:

```
HSG80 > set (unit #) preferred=other
```

c. Cycle power on the RAID cabinet for the preferred path settings to take effect.

2. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation. For FC-AL configurations perform step a. For FC Switched Fabric configurations perform step b.

a. For FC-AL configurations, if the configuration entails utilizing additional ports on existing RAID system controllers, or if you are installing additional (new) RAID systems, use SWCC to establish the Arbitrated Loop Physical Address (ALPA) assignments for all new controller ports by typing the following commands:

```
HSG80> set this_controller port_1_topology=offline
HSG80> set other_controller port_1_topology=offline
HSG80> set this_controller port_1_al_pa=n+1
HSG80> set other_controller port_1_al_pa=n+1
```

Where n+1 is an available address:

```
HSG80> set this_controller port_1_topology=loop_hard
HSG80> set other_controller port_1_topology=loop_hard
HSG80> set this_controller port_2_topology=offline
HSG80>set other_controller port_2_topology=offline
HSG80> set this_controller port_2-_al_pa=n
HSG80> set other_controller port_2_al_pa=n
```

Where n is an available address:

```
HSG80> set this_controller port_2_topology=loop_hard
HSG80>set other_controller port_2_topology=loop_hard
```

b. For FC Switched Fabric environments enter the following commands:

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

3. Shut down the server(s).
4. Install all FC interconnect hardware, including additional HBAs required to establish additional path(s) necessary to configure the desired High Availability topology. Reference the installation guides provided with the FC equipment for assistance.

   NOTE: Do not connect new HBAs to the hubs/switches at this time.

5. Restart the server(s).
6. Please refer to Chapter 4 for software installation.

   The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the SANworks Secure Path Software v3.0 for Novell NetWare CD into the CD-ROM drive. See Chapter 4, ”Installing Secure

Path Software," to complete the Secure Path software installation setup. If no additional paths to the storagesets are being added at this time, you should skip to step 9.

7. Restart the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.
   a. Using SWCC, double-click the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names can be found in the Application Notes. Refer to the SWCC documentation if you need more information about managing connections.
   b. Create any additional storagesets and/or modify unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC.
   c. Set Access IDs for each LUN to selectively present it to the appropriate standalone server or clustered servers.
8. Restart the server(s).
9. Verify the Secure Path configuration.

You have now completed the configuration procedures required to support the new Secure Path environment. See Chapter 5 for information on monitoring and managing Secure Path activity using the Secure Path Manager.

Chapter 4

Installing Secure Path Software

Overview

This chapter provides installation instructions for Secure Path Version 3.0 for Novell NetWare software.

The Secure Path installation media contains the following software components:

- Secure Path for NetWare which consists of the cpqfc.ham driver and the NetWare Agent
- Secure Path Manager (SPM) which must be installed on a windows client system.

  NOTE: Secure Path NetWare 3.0 is accessed through a Windows management application.

- Updated Secure Path Agent for Windows which must be installed on any existing Windows Secure Path version 3.x servers for compatibility with the Secure Path Manager supplied with this kit.

  NOTE: To ensure a successful installation, be sure to read the Secure Path for NetWare "Release Notes" and "Read Me" files before starting the installation process.

Secure Path NetWare Server Software Installation

This Secure Path software release comprises three installs:

- The installation of the ***Secure Path (SP) Agent*** (cpqspagt.nlm) and **driver** (cpqfc.ham) onto the Novell NetWare 5.x Server,
- The installation of the **Secure Path Client Manager** (SPM) onto the remote Client workstation running Windows NT or Windows 200.

  NOTE: Throughout this document, SPM (Secure Path Manager) means the GUI.

- The optional installation of an updated ***Secure Path Agent*** and **driver** for Windows servers currently running Secure Path 3.0 or 3.1 to make them compatible and manageable with this version of the heterogeneous SPM Client software.

Installation Prerequisites

Before you perform an installation procedure for any of the three installs you must have the following configurations:

- NetWare 5.X or above with latest Novell Support Packs.
- NetWare 5.X server OS updated with latest Compaq Support software NSSD, including driver updates, utilities, and services.
- TCP/IP Networking services configured on all units in the LAN.

The following prerequisites are optional:

- Compaq Insight Manager (CIM) software installation if remote management of the server with problem reporting is desired.
- SNMP service installed if remote management is used.

  NOTE: Secure Path NetWare software MUST be installed on the server BEFORE the SPM Client software is installed on the workstation.

  A maximum of 16 profiles containing a maximum of 16 Hosts each can be configured in the SPM.

Installation Overview

The following steps provide an overall view of the Secure Path installation process, including the three installs.

IMPORTANT: Secure Path NetWare software must be installed before SPM client software is installed.

A maximum of 16 profiles can be set up in the SPM.

1. Verify that all NetWare 5.x servers have the latest support pack installed.
2. Verify that all NetWare 5.x servers have TCP/IP installed and configured.
3. Verify that CPQFC.HAM driver and Secure Path for NetWare software are installed on all NetWare 5.x servers.
4. Install Secure Path Manager (GUI) client software on remote client computers running Windows NT 4.0 Workstation or Windows 2000 Professional.
5. Update all HOSTS files on all Servers and Clients.
6. Upgrade the Secure Path Agent on any Windows NT server(s) or Windows 2000 server(s) currently running Secure Path version 3.0 or 3.1.
   - ❏ This is for heterogeneous environment only.
7. Configure Secure Path for NetWare agent on the server with Client names and password.
8. Configure SPM software profiles and passwords on the client computers.
9. Add Novell NetWare 5.x servers to the cluster.

Configure HOSTS File to Add Client IP Address to Name Resolution

The HOSTS file must be edited to add the network Host names and Client names to ALL servers and Clients that will be using SecurePath. This will enable the “lookup” of Clients that will be authorized to access the SecurePath Hosts through the Agent software. This will map IP addresses of Hosts and Clients to their names.

1. Access the server running SecurePath software.
   - ❏ Use the text editor locally (EDIT.NLM Sys:Etc/Hosts console command) on the NetWare OS server to open the SYS:ETC/HOSTS file on the NetWare server.

   or:

- ❏ Use the Windows Network icon for remote access to open the SYS:ETC/HOSTS file on the NetWare server. The user must have a User account with Supervisor rights and permissions to the NetWare server's file system to gain access. This can be set through the NetWare Administrator program by making the user account a 'Trustee' of the File System object.

2. Add the Client or Server in the form of:

   IP address (at least 5 spaces) name

   example: 10.100.100.9 shark

IMPORTANT: Password is case sensitive. You must use the same letter case each time you enter the password.

---

3. Save the Hosts file to make active.
4. Client names in the server's SP Agent administration area MUST match the case in the HOSTS file or the DNS name. If they do not match, a message will appear on the NetWare console screen indicating a client name was not found. This is usually a result of an upper/lower case problem or a misspelling.

   The error messages will be as follows:

   On the Windows SPM side:

   "Wrong password or current Client running SPM is NOT authorized to access Secure Path Agent on <unit name>."

   On the Server console screen:

   "SecurePath: Warning: SPCP unable to determine <Client name> Client definition."

IMPORTANT: The SPM screen profile password MUST match the server's SP Agent's password.

The SP Agent's Client name is case sensitive and MUST match the Client workstation's name as listed in the HOSTS file.

SecurePath "Stop Agent" Configuration option:

5. Select "4) Stop Agent" to close SecurePath.

   - ❏ **Optional**: Verify that entries have been made in the Autoexec.NCF file to auto-start CPQSPAGT.NLM.

6. Use "CPQSPAGT.NLM" to start the SP Agent from the NetWare console screen.

7. Configure SPM Client profiles and passwords on the ‘Client’ workstation.

Installing Secure Path 3.0 for RA4000/4100, MA8000 on Novell 5.x Servers

“Non-Interactive” Automatic Server Software Install Procedure

1. Insert Secure Path software CD into CDROM drive of a NetWare server.
2. Mount the SP CD as a NetWare volume by entering “CDROM” at the console.
3. On the NetWare console screen, enter “Volumes”. This will display a complete list of all volumes mounted. The install CD volume name is “NWSPV30”.
   If this volume is not mounted, enter “Mount NWSPV30”.
4. On the NetWare console screen, enter “Load NWCONFIG.NLM”.
5. Under Product Options, enter “Install product not listed and press enter. The following screen appears.

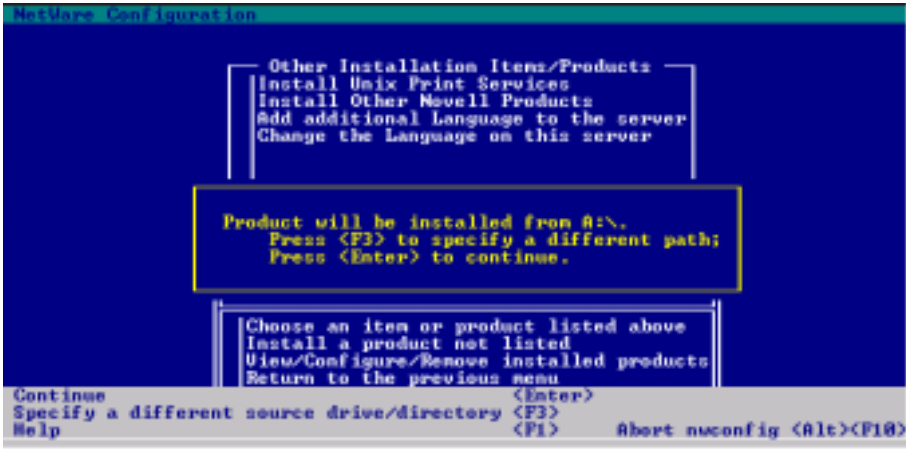


Figure 4–1. Install product not listed Screen

The screen message states: “NWCONFIG is loading another NLM…”.

The screen switches from the NetWare NWCONFIG screen to the SecurePath installation Program, which:

- ❏ Checks the HAM and other drivers and lists them on screen.

- ❏ Starts installing files from CD.
- ❏ Returns to the NetWare NWCONFIG screen when complete. (Exit NWCONFIG.)
- ❏ The "CPQSPAGT.NLM version 1.0 build 011" line is now available on the NetWare OS "Available Screens" menu (when CTRL+ESC is used). At this point, the "Secure Path V3.0 NetWare Loadable Module" screen is shown, displaying the following options:

  1. Main Menu
  2. Agent Administration
  3. Client Administration
  4. Storage Subsystems
  5. Stop Agent

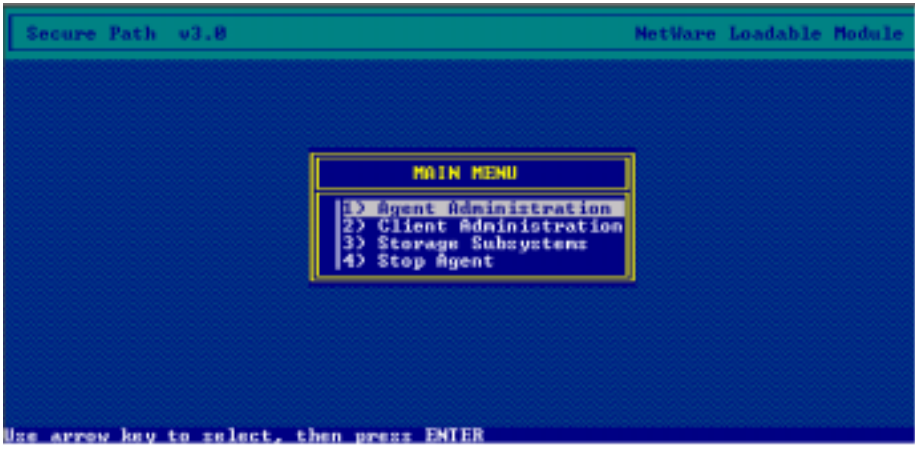


Figure 4–2. Secure Path V3.0 NetWare Loadable Module Screen

Installation is complete. Now configure the server Agent with the Main Menu options.

SecurePath "Agent Administration" Configuration Option

1. Select the Agent Administration option.
2. Select Set Password that authorizes remote stations to access this unit.

   NOTE: Password is case sensitive. You must use the same letter case each time you enter the password.

   This password must be the same for all servers in the same profile.
3. Enter new password and verify it.
4. Press the "ESC" button and you return to the Agent Administration options:
   - ❑ 2) Load Distribution. (Is unavailable and is 'grayed' out)
   - ❑ 3) Path Verification.
   - ❑ 4) Auto Failback.

SecurePath "Client Administration" Configuration Option

1. Through the "1) View Clients "selection: verify correct Clients listed when added.
2. Use "2) Add a Client" to add all Client machines that need access to SPM.

   NOTE: This entry along with the password entry above gives the Client access to SPM.

   This entry is case sensitive and MUST match the Client's HOSTS file entry. (for upper/lower/mixed case).
3. Use "3) Remove a Client" if access is denied.

   NOTE: If any changes are made to the SP Agent, the NLM MUST be stopped and restarted in order for the changes to become active.

Installing Secure Path Manager (SPM) on a Windows Client Workstation

The following options description the prerequisites you must have before installing SPM on a Windows Client workstation:

- A workstation running Windows NT or Windows 2000.
- Networking configured for TCP/IP and connected to LAN.
- HOSTS file modified with IP addresses & HOST names of this unit, all server HOSTS (also called 'nodes'), and all other Client SPM units on the network.

SPM Client Installation Procedure

The following procedure describes how to install the SPM on a Windows Client workstation.

1. Insert the SPM install CD into the Client workstation CD-ROM drive.
2. The CD should auto-start the "Setup.exe" program and provide the "Installing Secure Path v3.0 for NetWare" GUI.
3. Continue through the screens accepting the License Agreement with the [YES] button.
4. Either accept the default installation path (recommended) or [Browse] to the desired location where you want the files installed.
5. Two option paths are provided:
   - ❏ Installation of the Windows SP Agent and driver on a Windows Server OS machine,

   or

   - ❏ Installation of the SecurePath Client Management GUI software on a workstation.
6. Select the SecurePath Client option on the Installation screen.
7. Accept the default SecurePath Program Folder (recommended) or rename it if desired.
8. A summary of the previous choices is displayed before the files are copied. If acceptable, select [Next] to start the file copy.
9. If a previous copy of SPM has been installed, it will be detected:

   NOTE: Be sure the old version of SPM is currently NOT running or a 'file locked' error condition is generated later that will stop the installation.

10. A message that "Secure Path Setup needs to uninstall any old version in order to successfully complete the installation. Uninstall old version now?" Choose [Yes] to continue.
11. You will be prompted again: "Do you want to completely remove the selected application and all of its components?" Choose [OK] to continue the install.
12. The installation Status bar will display as the files are installed and the "Setup Complete" window will open when Secure Path is installed. Click [Finish] to complete the Setup.
13. To start Secure Path, from the Windows Start icon on the Task Bar, select: <Programs> <SecurePath> <SPM>.
14. Configure the SPM Client. See Chapter 5

Chapter 5

Managing Secure Path

Overview

This chapter provides the following Secure Path Manager (SPM) operational information:

- Hosts can be heterogeneous / homogeneous systems of Novell NetWare and Windows
- Launching SPM
- Logging on to SPM
- Monitoring host connections
- Managing storagesets and paths
- Detecting and identifying path and controller failures
- Responding to failover events

You can use Secure Path Manager, from a Windows environment, to monitor and manage a Secure Path environment. SPM displays specific information about the state of RAID storage systems and I/O paths configured for high-availability storage access. Use SPM to set various properties and modes associated with a managed storage profile, and to set failback policy. SPM automatically detects and indicates path failures, and provides the capability to move RAID Array storagesets across controller pairs.

Launching Secure Path Manager

To launch SPM:

1. From the START menu, select Programs, then SecurePath, and then the SPM submenu.
2. Click the Secure Path Manager (SPM) application icon.

Logging on to Secure Path Manager

Logging on to SPM incorporates entering user and storage profiles definitions directly from the login window.

Defining 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, enter hosts that share these RAID storage systems while defining storage profiles from the login window.

- To create a non-clustered host profile, start by entering 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) with each followed by a “-your clustername” designation to identify cluster membership.

  NOTE: Hyphens are not allowed in Host names. Hyphens are allowed in cluster names.

A single profile of SPM is capable of managing:

- Heterogeneous / homogeneous configurations of Novell NetWare and Windows systems

  Multiple non-clustered hosts sharing one or more RAID storage systems
- Multiple sets of clustered-hosts sharing one or more RAID storage systems.

IMPORTANT: The clusters must be either Windows NT, Windows 2000 or NetWare, but you can have heterogeneous clusters within the configuration.

Figure 5–1 shows an example of an SPM login display.

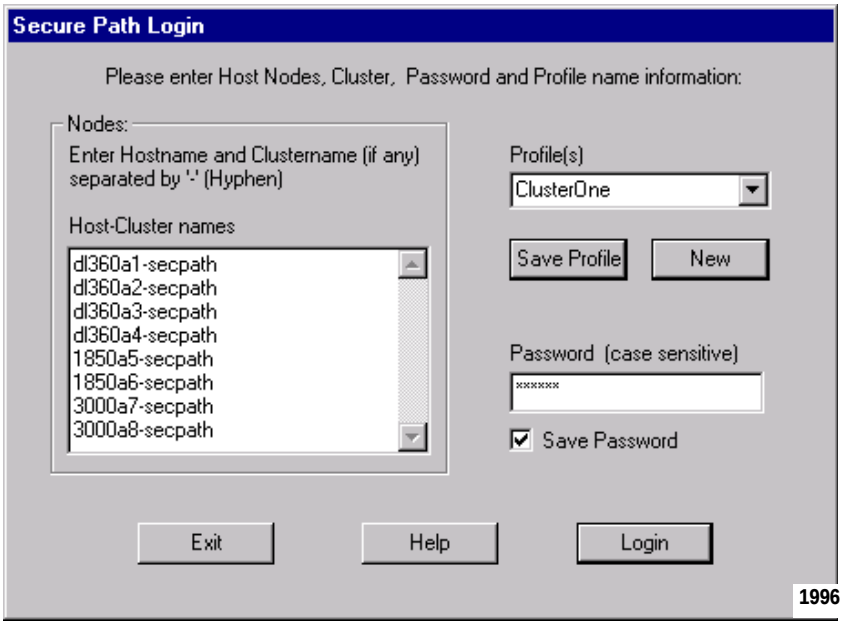


Figure 5–1. Secure Path Login window with a clustered host storage profile

After you have added all the host names to your storage profile, enter the connection password in the “Password” field. This is the password that you defined for the Secure Path Agent during setup, or when you run the Secure Path Agent Configuration utility after installation.

IMPORTANT: Password is case sensitive. You must use the same letter case each time you enter the password.

SPM uses this password to establish a network connection with the Secure Path agents running on host(s). For storage profiles including more than one host, the connection password must be the same on each of the Secure Path host agents.

Check “Save Password” if you want SPM to use the saved password automatically each time you login with this storage profile.

Saving an SPM Storage Profile

To save an SPM profile:

1. Enter a unique name in the “Profile(s)” field once you have defined a storage profile.
2. Save the profile by clicking “Save Profile.”

NOTE: Each profile can have a maximum of 16 hosts. There can be a maximum of 16 profiles.

Creating A New SPM Storage Profile

To create additional SPM storage profiles:

1. Click “New.”
2. Add host name(s) in the “Host-Cluster Names” field.
3. Enter a profile name in the “Profile(s)” field.
4. Add a password to the password field, if desired. Save the password and be sure the check box next to the password field is set.
5. Click the “Save Profile” button.

Selecting an Existing SPM Storage Profile

To choose an existing SPM storage profile, use the pull down arrow on the “Profile(s)” box to find and select the profile.

If you did not choose to save the password when you originally created the profile, enter the password in the “Password” field and click “Login.”

Editing an Existing SPM Storage Profile

To edit an existing storage profile, select the profile to be edited. Make the desired changes to the profile and click “Save Profile.”

Changing the NetWare Secure Path Agent Password

To change the Secure Path Agent's password:

1. From cpqsdagt.nlm, select <Agent Administration>.
2. Select <Change Password>.
3. Enter the new password and confirm it.

4. Stop and then reload cpqspagt.nlm.

Repeat steps 1 through 4 for each of the hosts in an SPM storage profile.

Troubleshooting Connection Problems

If you experience problems attempting to log on to SPM, see Chapter 7, ”Troubleshooting Secure Path Connection Problems,” for more information.

Monitoring Host Connections

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

As shown in Figure 5–2, 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.

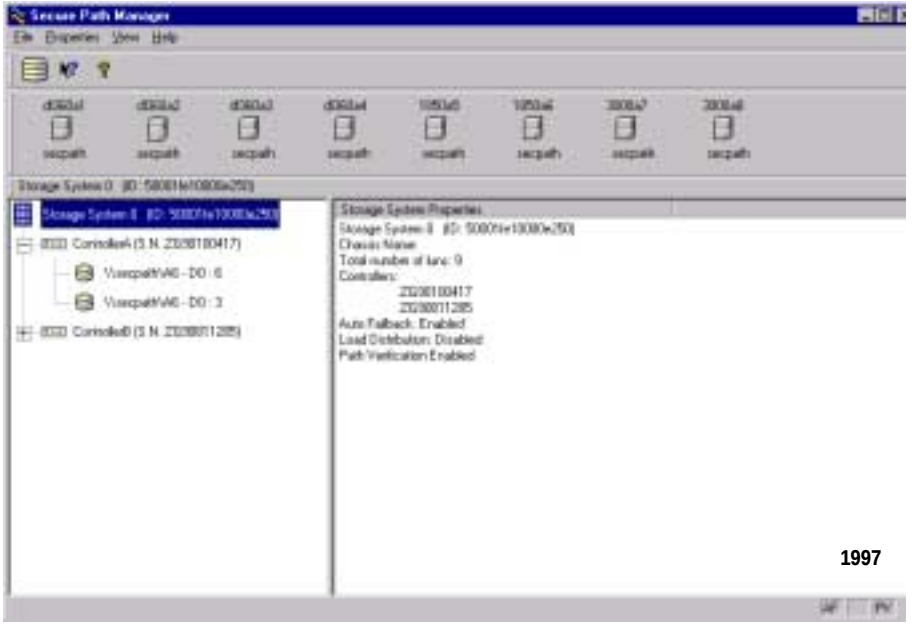


Figure 5–2. Host connection monitor

SPM monitors its connection with each member of a storage profile and will indicate a loss of connection to a particular host with a red “X.” The red “X” can also indicate that the Secure Path agent is not running on the host.

Figure 5–3 shows that SPM has lost connection to host dl360a2.

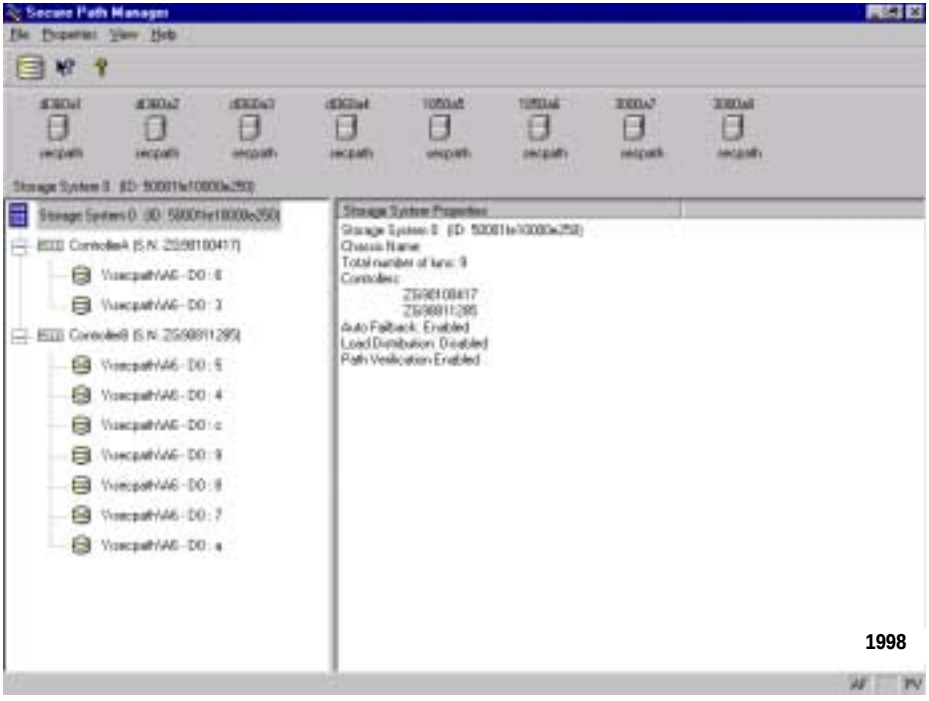


Figure 5–3. Lost host connection Icon

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 or the Secure Path agent is not running and you have only lost Secure Path remote management functions. Secure Path's cpqfc.ham multiple path driver is still protecting availability to your storage.
- 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.
- 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. It is important to note that these Properties have a global effect on all resources managed by an SPM storage profile. Using the Properties pull-down menu you can:

- 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 enabled, permits failback to occur for quiescent storagesets. If Auto-Failback is enabled, "AF" will show in the bottom right hand corner of the SPM window in the status bar.
- Enable or Disable Load Distribution (default = disabled). Load Distribution allows multiple paths between a host and a specific storageset to be used in parallel for I/O, in order to maximize performance potential.

IMPORTANT: Note that Load Distribution is valid only in Windows, and is disabled in Cluster Server (MSCS) and NetWare systems.

- Enable or Disable Path Verification (default = enabled for NetWare). 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. If Path Verification is enabled, "PV" will show in the bottom right hand corner of the SPM window in the status bar.

  NOTE: Path Verification must not be disabled for NetWare.

- Set the Polling Interval (default = 90 seconds) to determine the rate at which SPM will request configuration change information from the Secure Path Agent(s) 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 of 5 seconds to a maximum of 1800 seconds (30 minutes).

Storage System View

Physical storage objects are displayed in the SPM Storage System view located in the left frame (Figure 5–4). 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 identified as follows:

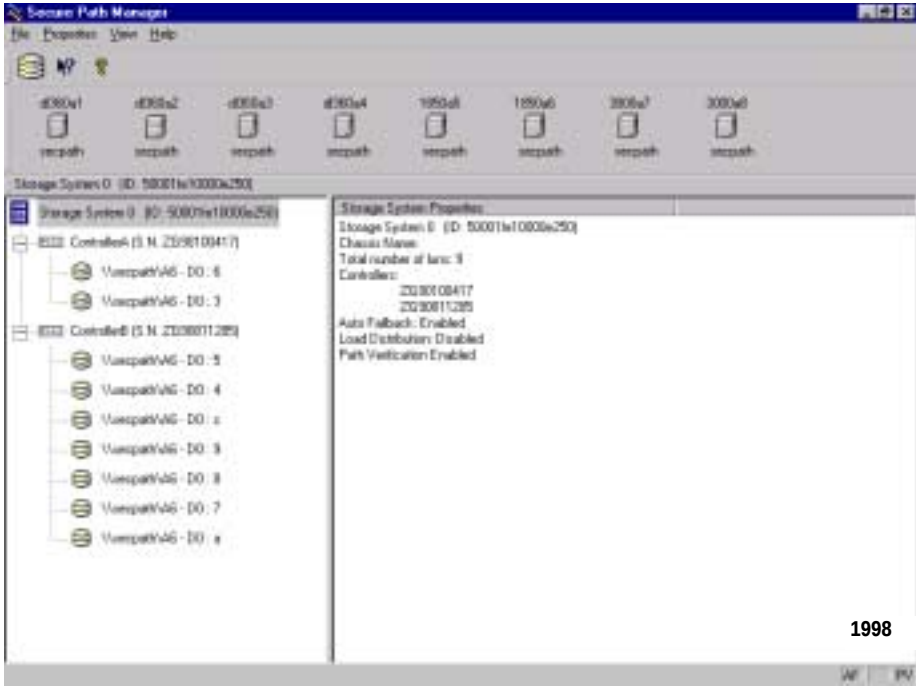


Figure 5–4. SPM single host storage profile - Storage System view

Storage Systems and Controllers

- Storage System ID–Each RAID Array storage system is identified by a unique 64-bit value. For MA8000/EMA12000, the Storage System ID is the 64-bit (ULONGLONG) FC name. For the RA4000/RA4100, the Storage System ID is an 8-character string which contains a Secure Path modified version of the chassis number.

- Chassis Name–For the MA8000/EMA12000, the FC Node Name is persistent to the subsystem. For the RA4000/RA4100 the chassis number is persistent to the subsystem. Swapping a controller will not affect the Storage System ID for either RAID storage type. It will remain constant for the life of the RAID storage system.
- Controller Serial Number–The individual controllers of a RAID Array storage system are identified by a unique alphanumeric value assigned during controller manufacture.

  NOTE: For each subsystem, the controllers are ordered based on the serial numbers. The controllers are listed in numerical sequential order, lowest to highest. This list order does not relate to the physical order of the controllers in the rack.

RAID Array Storagesets

You can select the method SPM uses to identify storagesets with the “View” pull-down menu located above the toolbar. SPM will always display the owning host's name, or clustered name (for clustered hosts) including whatever storageset identifier you choose.

RAID Array Storageset information varies according to the Operating System running on the server. To obtain this information, select <View> <Device Identifier> <Operating System>.

RAID Array Storagesets - NetWare

- LUN UUID–a 128-bit value that uniquely identifies a LUN.
- Volume Label–the label assigned to the volume by the user with NetWare. This is the default used by Secure Path for Novell NetWare systems.

  NOTE: There can be more than one label assigned to each LUN.
- Adapter - Device: Unit–NetWare specific device identifier.

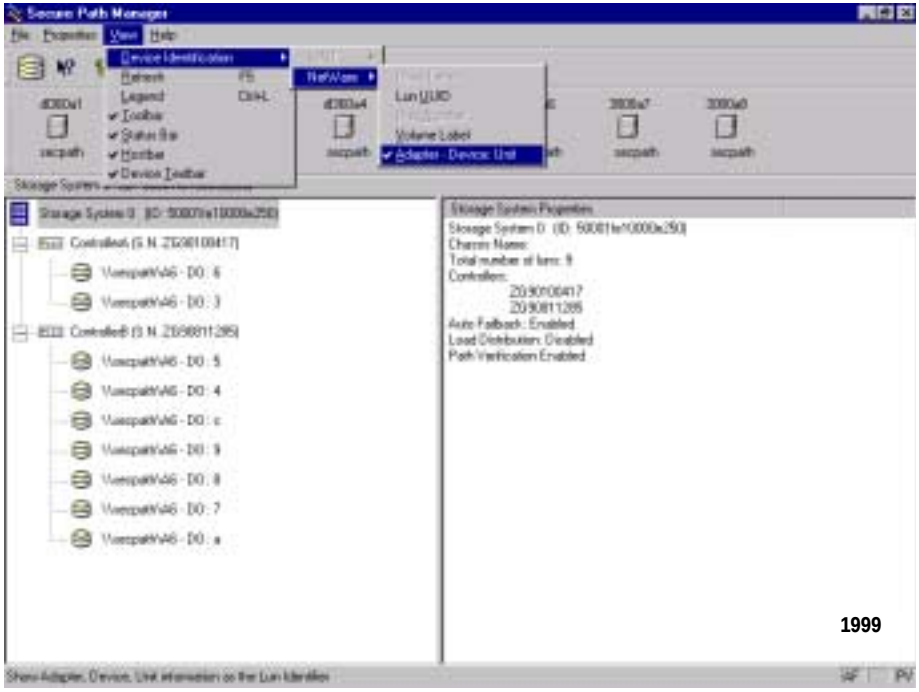


Figure 5–5. Novell NetWare SPM Window showing Adapter - Device Unit Path

RAID Array Storagesets - Windows

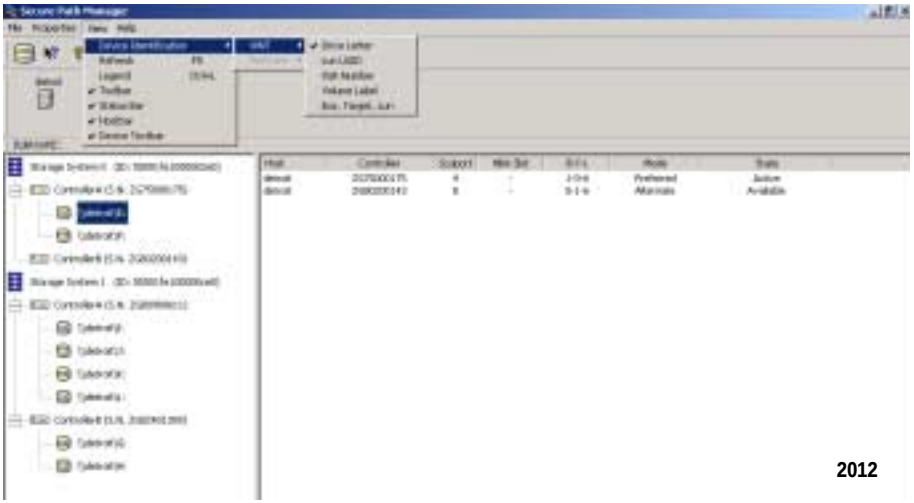


Figure 5–6. Windows SPM Window showing Drive Letter Path

- Disk LUN UUID–a 128-bit value that uniquely identifies a LUN.
- Drive Letter–the letter assigned to the volume by the user.

  NOTE: There can be more than one Drive Letter assigned to each LUN.
- Bus/Target/LUN–the physical address representing the connection to the host server.
- Volume Label–the label assigned to the volume by the user.

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–is the Secure Path host system, which has an established access paths to the storageset.
- Controller–is the RAID storage system controller servicing the path.
- SCSI Port–represents the physical port number of the Host Bus Adapter 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.
- Mode–A user selectable parameter that specifies path behavior during nominal and failure conditions. Path mode may be set to Preferred, Alternate, Pre-Offline (Preferred and Offline), or Alt-Offline (Alternate and Offline).
- State–A set of attributes that describe the current operational condition of the path. Paths may exist in Active, Failed, or Available states.

The SPM screen (Figure 5–7) shows a multi host configuration with the host "\\d1306a1" attached to two Secure Path protected RAID storage systems. Browsing the controllers of Storage System 1 shows three storagesets owned by controller A, and six storagesets owned by controller B.

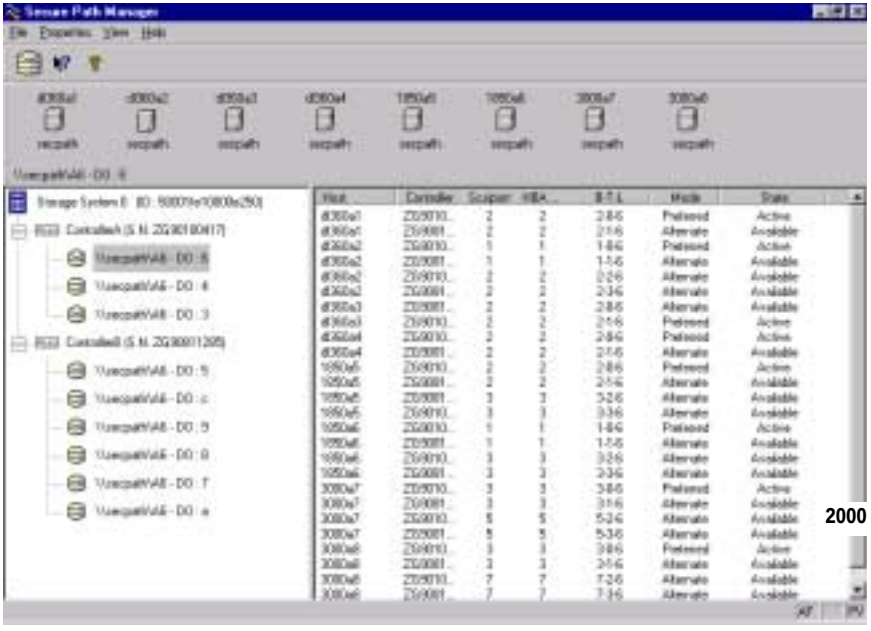


Figure 5–7. SPM multi host Novell NetWare profile - Physical Path view

The display information in this example shows nine servers configured in a cluster.

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.

Information from the second, third, and fourth lines of this path view indicate that these paths are 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 Volume Label x.

Two of the paths in the Available State have a different serial number than that of the Preferred Mode path, indicating that they are providing standby access through the other controller. Should the controller currently servicing the Preferred path completely fail, one of the paths on the surviving controller will transition to the Preferred State.

Polling Interval and Display Refresh

To keep the displayed path status current, SPM will periodically request 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 use of 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 will depend upon the number of hosts, RAID storage systems, and storagesets in the monitored storage profile.

Managing Storagesets and Paths

You can perform the following actions on the storagesets and paths managed by SPM:

A right mouse click will pop up a menu with the following action menu items.

- Move a storageset from one controller to the other
- Make a path Alternate
- Make a path Preferred
- Change the Preferred path
- Make a path Offline
- Make a path Online
- Verify a path
- Repair a path

Moving a Storageset

Choose Move a Storageset when you want 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 (available only with MA8000/EMA12000) or to manually return a failed-over storageset to its Preferred path when Auto-Failback has been disabled.

There are two methods available to move a storageset.

1. Click the drive to highlight it in the storage system view.
2. Drag the drive to the other controller or right click to select the “Move To Other Controller” action.

Making a Path Alternate

Choose Make a Path Alternate when you have Load Distribution enabled and you want to disable I/O operations to one or more paths. To make a path Alternate:

1. Click the Preferred path you wish to change.
2. Right click to select the “Make Alternate” action.

NOTE: “Make a Path Alternate” is a selection only for Windows with MA8000/ESA1200.

Making a Preferred Path

Choose Make a Path Preferred when you have Load Distribution enabled and you want to re-enable I/O operations to a path that you have previously disabled using "Make Alternate." To make a path Preferred:

1. Click the Alternate path you wish to change.
2. Right click to select the "Make Preferred" action.

NOTE: "Make a Path Preferred" is a selection only for Windows with MA8000/ESA1200.

Changing a Preferred Path

Choose Change a Preferred Path when Load Distribution is disabled. There are multiple paths available to a storageset on the same controller and you wish to select a new Preferred path for normal I/O operations. To change a Preferred path:

1. Click the Alternate path you wish to change to Preferred.
2. Right click to select the "Change Preferred" action.

Making a Path Offline

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

1. Click a Preferred or Alternate path.
2. Right click to select the "Make Offline" action.

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

Making a Path Online

Choose Make a Path Online when you want 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. Click a path in the FAILED State.
2. Right click to select the “Repair Path” action.

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.

NOTE: “Repair a Path” throughout this manual is referred to as “Manual Failback.”

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.

The Secure Path Agent will also notify SWCC clients immediately when a fault is detected.

You should routinely monitor SPM status to check for occurrences of failover events that might compromise either the performance or availability of storage resources. Availability is compromised if your configuration includes only two configured paths to a storageset and one is lost due to component failure. Secure Path will be unable to failover to a redundant path should a subsequent fault occur in this situation.

The SPM client is not required to be running in order for Secure Path to protect path availability. The cpqfc.ham 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.

The icon shown in Figure 5–8 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 5–8. Storage system path failure detected

Storage Controller Path Failure Detected

The icon shown in Figure 5–9 indicates that a failure of at least one, but not all paths to that storage controller was detected by Secure Path. Browse the storage controller to determine the affected storageset(s).

Figure 5–9. Controller path failure detected

Unless you have the Path Verification property enabled, Secure Path only detects failures for paths with active I/O. 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 storageset(s).

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 5–10 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 in the right pane to determine the specific nature of the path failure.

Figure 5–10. 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 5–11. Storage system failure detected

Figure 5–12. Storage controller failure detected

Figure 5–13. Storageset failure detected

Identifying Path Failovers

To identify the source of path failover activity, first check the Storage System view for path failed icons, then examine the Physical Path view of the affected storageset. 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:

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 6-10. 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. See Chapter 7. Use StorageWorks Command Console to check for RAID array system faults. Visually inspect your switches or hubs for LED or LCD hardware fault indications.

Chapter 6

Using Secure Path with SWCC

Overview

This chapter provides the following Secure Path and StorageWorks Command Console (SWCC) interoperability information:

- Adding Secure Path to the network
- Using SWCC to monitor the Secure Path system

SWCC is a Windows-style Secure Path Manager (SPM) that uses standard Windows navigation features and command selection. Folders are used to arrange Secure Path managed storage systems and non-Secure Path managed storage systems.

The SWCC Navigation window provides a list of all the host computers and storage systems to which SWCC is connected. You can use the Navigation window to monitor storage systems for failures. SWCC will monitor your network connection and storage system and report status by changing the icons in the Navigation window.

Adding a Secure Path System to the Network

To add a Secure Path System to the network:

1. From the SWCC File menu, click Add System.
2. Enter a Domain Name Service (DNS) name or the IP address in the Host name or TCP/IP address: text box.
3. Click Apply. After you click Apply, the SWCC Client adds an icon in the Navigation window for the host running the Secure Path Agent.
4. Click Close when the second Add System dialog box appears.

When SWCC connects to a Secure Path system, it will add the following folders in the Navigation window:

- Host Folder–which has the host name
- Storage System Folder
- SPM Window

The SPM window does not support the launching of Secure Path Manager (SPM). To launch SPM, select the SPM icon from START/Programs/Secure Path submenu.

NOTE: Attempting to launch SPM from the SWCC Navigation window will result in an object creation failure error generated by the Applet Manager.

Using SWCC to Monitor the Secure Path System

SWCC monitors all storage systems displayed on the Navigation window. Failures occurring in the Secure Path system are indicated in the Navigation window by a change in the appearance of the controller folder icon, as defined in Table 6–1.

A Controller Folder shows all the storage associated with a controller.

Table 6–1 lists the four states of a Controller Folder.

Table 6–1 Controller Folder States

Controller Folder Icon	State
	The Secure Path system contained in this folder is working properly.
	A Secure Path component has failed. For details, launch SPM from the START/Programs/Secure Path menu.
	A grayed out folder indicates no connection to the Secure Path Agent.
	This state is not currently supported by Secure Path software.

NOTE: A failure indicated by a change in the controller folder icon will also be reflected in the corresponding host folder icon.

SWCC offers a variety of methods for notifying the user about any system failures. For details of error notification and other SWCC related issues, consult your Solution Software kit's *Compaq StorageWorks Command Console Guide* that supports the RAID storage system.

Chapter **7**

Troubleshooting Secure Path Connection Problems

Overview

This chapter 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 Phone Support Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week.

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

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for world wide Technical Support Centers are listed on the Compaq website. Access the Compaq website by logging on to the Internet at http://www.compaq.com.

Client/Agent Considerations

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

- Add each client's system name and client name 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, and Restart the Secure Path Agent to update the database using the Services applet from Control Panel.

For example, from console type:

```
Unload CPQSPAGT

Load CPQSPAGT
```

- Each name you use must be mapped to its network IP address using one of the following:
  - ❏ HOSTs file (server and/or client name mapped to IP)
  - ❏ Domain Name System (DNS with a fully qualified domain name)

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 NetWare 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.

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, 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.

On the client system, you must enter, in the LMHOSTs file, the NETBIOS name and the IP address of the Agent you wish to connect with and save it.

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.

Finally, from a command prompt issue the NBTSTAT -R command to purge and reload the remote name table.

- Client names that exceed 15 letters or include 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 Novell NetWare 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, COMPAQ recommends that you use fully qualified domain names with DNS.
- For production environments, where management and security are a concern, COMPAQ recommends that fully qualified domain names be used with DNS name resolution.
- For test and evaluation environments it is usually easier to simply 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.

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, a number assigned to the physical interconnect(s) 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 hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSZ70 and HSG80 are array controllers supported for use with Secure Path. Each controller in an HSZ70 or HSG80 RAID system is identified by a unique serial number, which is displayed next to the controller icons by Secure Path Manager (SPM). Secure Path Manager identifies a pair of controllers configured in multiple-bus mode by a unique 64-bit identifier that is displayed next to the subsystem icon.

HBA

Host Bus Adapter is an I/O device which serves as the interface connecting a host system to the SCSI bus or Storage Area Network (SAN). HBAs are assigned a relative port number by the Windows operating system according to order of discovery. *See also* Port.

Host Bus Adapter

See HBA.

host

A computer system on which the Secure Path server software (cpqfc.ham driver and Agent service) is running.

LUN

The actual unit number assigned to a device at the RAID system controller.

mode

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 path(s). When Load Distribution (Windows only) 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

A virtual communication route that enables data and commands to pass between a host server and a storage device.

port

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.

reduced mode

The condition of a system where one or more redundant components fail, but the system is operational.

SPM

Secure Path Manager

state

An attribute that describes the current operational condition of a path. A path may exist in the following state(s):

Active - indicates a path that is currently servicing I/O requests.

Failed - indicates a path that is disabled and not actively servicing I/O requests.

Available - indicates a path that is neither Active nor Failed.

Remote - indicates a path that connects to a remote member of a PPRC (Point-to-Point Remote Copy) configuration. Remote state may be logically or'd with any of the other states.

target

For parallel SCSI configurations, the actual target number assigned to a device.

Index