

release notes

HP StorageWorks

Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition

Product Version: 3.0F

Fourteenth Edition (April 2005)

Part Number: T3549-96405

For the latest version of these release notes and other Secure Path documentation, access the HP storage web site at: <http://www.hp.com/country/us/eng/prodserv/storage.html>.



i n v e n t

© Copyright 2001–2005 Hewlett-Packard Development Company, L.P.

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

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Compaq Computer Corporation is a wholly-owned subsidiary of Hewlett-Packard Company.

UNIX is a trademark of The Open Group in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

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

Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition
release notes

Fourteenth Edition (April 2005)

Part Number: T3549-96405

About this document

This document summarizes the most recent product information about the HP StorageWorks Secure Path 3.0F for HP-UX 11i v1.0 and 11i v2.0 systems, including:

- [Release notes information](#), page 3
- [Intended audience](#), page 4
- [Related documentation](#), page 4

Release notes information

These release notes cover the following topics:

- [Secure Path 3.0F kit contents](#), page 5
- [Secure Path 3.0F for active-passive disk arrays](#), page 6
 - [Differences between Secure Path for active-passive 3.0E and 3.0F](#), page 6
 - [Operating system support](#), page 8
 - [Avoiding problem situations](#), page 11
- [Secure Path 3.0F for active-active disk arrays](#), page 33
 - [Differences between Secure Path 3.0E and 3.0F for active-active disk arrays](#), page 33
 - [Operating system support](#), page 34
 - [Avoiding problem situations](#), page 36
- [Secure Path 3.0F for Workgroup Edition Virtual Array \(VA\) disk arrays](#), page 38
 - [Differences between Secure Path 3.0E and 3.0F for Workgroup Edition](#), page 38
 - [Operating system support](#), page 39
 - [Avoiding problem situations](#), page 41

Intended audience

This document is intended for customers who have purchased the HP StorageWorks Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 on active-passive and active-active disk arrays and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition, and are responsible for installing, configuring, and maintaining this product in their HP-UX server environment.

Related documentation

Additional documentation that you may find helpful includes:

- *HP StorageWorks Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition* installation and reference guide, part number AA-RR4VH-TE
- Additional documentation is available at HP web site: <http://www.hp.com..>

Secure Path 3.0F kit contents

The Secure Path 3.0F for HP-UX kit includes:

- *Secure Path 3.0F for HP-UX readme.txt* document.
- *HP StorageWorks Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition* installation and reference guide, part number AA-RR4VH-TE.
- Secure Path 3.0F for HP-UX 11i v1.0 and HP-UX 11i v2.0 CD-ROM

The Secure Path 3.0F for HP-UX 11i v1.0 and 2.0 web kit includes:

- *Secure Path 3.0F for HP-UX readme.txt* document
- HP StorageWorks Secure Path 3.0F for HP-UX 11i v1.0, 2.0 compressed tar package, which includes the software and the release notes.

Note: The Secure Path 3.0F `swlist` displays the version as A.3.0F.00F.00F.

Note: Secure Path 3.0F release notes supersede all earlier versions of the release notes. Refer to your Secure Path 3.0F kit documentation for Secure Path operating details.

Secure Path 3.0F for active-passive disk arrays

This section contains the following information:

- [Differences between Secure Path for active-passive 3.0E and 3.0F](#)
 - [Issues resolved by Secure Path 3.0F](#)
 - [Changes made in this release](#)
- [Operating system support](#)
- [Avoiding problem situations](#)
- [Managing Event Monitoring Service \(EMS\)](#)

Differences between Secure Path for active-passive 3.0E and 3.0F

Issues resolved by Secure Path 3.0F

The following issues have been resolved in this release of Secure Path 3.0F for active-passive disk arrays:

- The Path polling threads that were inadvertently terminated during parallel execution of `ioscan` and the `spmgr delete` command are now fixed.
- The failed condition of I/O errors in all paths during I/O to a non- Logical Volume Manager (LVM), Hierarchical File System (HFS), Logical Unit Number (LUN) has been resolved.
- Loss of the path verification period and deleted LUN information during the upgrade from A.3.0B.01F.00F, has been resolved.
- The problem of displaying all the active LUNs in the deleted LUN list while migrating from an earlier versions of Secure Path 3.0E to 3.0F is now fixed.
- The device special file name in the message logged into `syslog` when all the paths to a LUN fails is fixed. The device special file name now corresponds to the LUN and not to the path for that device.
- The LUN now no longer moves from the unattached list to the discovered list after an upgrade.
- The installation failure issue when multiple paths exist in your local disk has been resolved.
- The core dump generated by the `spmgr delete` command when any Secure Path communication issues occurred has been fixed. The system now displays an appropriate error message when any issue occurs.

- The issue related to failback resulting a new CTD for the same WWLN has been resolved. The host now displays the same CTD when failback occurs.
- The issue of retrieving the verification interval after upgrading from 3.0BSP1 to later versions has been resolved.
- The memory leak that occurs while an event or mail notification is enabled in `spagent` has been fixed.
- The `spagent` core dump caused by un-handled exception has been fixed.
- When an array controller was replaced online, the `spmgr display` command displayed the previous controller's ID until the system was rebooted. This problem has been resolved. The controller IDs are now updated to reflect the new controller's ID without a system reboot. (Enable the proactive path polling while doing the controller replacement).

Changes made in this release

This release of Secure Path includes the following changes:

- The `spmgr prefer` and `spmgr unprefer` commands are reintroduced. (These commands were removed for SecurePath 3.0E).
- A new LUN gets added as a new C T D when a LUN collision occurs.

Operating system support

Table 1 lists the system features and requirements by Secure Path 3.0F. For additional support information, check the HP web site: <http://www.hp.com/support>.

Table 1: Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 requirements

System feature	Requirement
Operating system versions	HP-UX 11i (V1.0, V2.0) 64-bit HP-UX 11i (V1.0) 32-bit
HP-UX server system types	A-class: rp24xx K-class (64-bit only): Kx60, Kx70, Kx80 L-class: rp54xx N-class: N4000, rp74xx V-class: V2200, V2250, V2500 V2600 rp3440, rp4440, rp7410, rp7420, rp8400 rx1600, rx2600, rx4640, rx5670, rx7650, rx8620 zx2000, zx6000 Superdome, Superdome Integrity
File systems	HFS (UFS) JFS (VxFS)
Controllers	Dual HSG60 controllers operating ACS 8.6L or later Dual HSG80 controllers operating ACS 8.6F or later Dual HSV100 controllers operating VCS 3.010 or later Dual HSV110 controllers operating VCS 3.010 or later
SCSI modes	SCSI-2 with or without CCL SCSI-3 with CCL
Volume managers	HP logical volume manager
Clustering	HP MC/ServiceGuard 11.15 or later
Fibre Channel modes	Switched fabric

Note: Secure Path 3.0F supports the Fibre Channel switches and firmware listed in the *HP StorageWorks SAN Design* reference guide at: <http://h18006.www1.hp.com/products/storageworks/san/documentation.html>.

Table 2 lists the supported devices and the driver requirements for this release, and earlier releases of Secure Path.

Table 2: Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11i v1.0	A5158A A6795A A6685A	Fibre Channel B.11.11.01	RA8000/ESA1200 0 (HSG80) MA8000/EMA120 00 (HSG80) MA6000 (HSG60) EMA16000 (HSG80) EVA5000 (HSV110) EVA3000 (HSV100)
11i v1.0	A6826A A9782A A9784A	Fibre Channel B.11.11.03	RA8000/ESA1200 0 (HSG80) MA8000/EMA120 00 (HSG80) MA6000 (HSG60) EMA16000 (HSG80) EVA5000 (HSV110) EVA3000 (HSV100)
11i v2.0	A6795A A6826A A9782A A9784A	Fibre Channel B.11.23.01	EVA3000 (HSV100) EVA5000 (HSV110)

Table 3 lists the patch revisions for this release and earlier releases of Secure Path.

Table 3: Patch revisions for Secure Path 3.0F

HP-UX version	Patch revisions (minimum)
11i V1.0	Hardware Enablement Bundle June 2004 HWEEnable11iB.11.11.0406.5 or later PHKL_27266 – (u)mount performance PHKL_27321 Early KRS PHKL_28569 WSIO Patch PHKL_28695 VM Patch PHKL_28984 – Fibre Channel Mass Storage Patch PHKL_30833 (VxFS cumulative) PHKL_30219 Dump Patch1 for EVA support PHKL_30510 SCSI IO Cumulative Patch PHKL_30557 – getmount_entry PHKL_30605 Dump Patch2 for EVA support PHKL_30622LVM cumulative Patch PHCO_27957 umount(1M) cumulative PHCO_27958 mountall cumulative PHCO_27959 umountall(1M)cumulative PHCO_28651 VxVM Enterprise Administrator Srvc patch PHCO_28656 VxVM Enterprise Administrator Patch PHCO_29905 mount(1M) cumulative PHCO_30530 libc cumulative patch
11i V2.0	N/A

Table 4 shows the configuration limits for Secure Path 3.0F.

Table 4: Configuration limitations for Secure Path 3.0F

Parameter	Minimum	Max qualified	Max supported
Adapter support	Single HBA	8 arrays	Platform limit
Storage arrays per host	1 HBA	8 arrays	128 arrays

Table 4: Configuration limitations for Secure Path 3.0F (Continued)

Parameter	Minimum	Max qualified	Max supported
LUNs per storage array per host	1 HBA	256 arraya	Array limit

Avoiding problem situations

The following section lists problems that may arise during Secure Path operation, and provides information on how to avoid those problems.

General

- When Secure Path is installed on HP-UX 11i v2.0, the following warning messages are displayed. You can ignore these messages.


```
ld: (Warning) Ignoring .IA_64.unwind_hdr section in file
"/usr/conf/mod/hsx".
ld: (Warning) Ignoring .IA_64.unwind_hdr section in file
"/usr/conf/mod/swsp".
ld: (Warning) Ignoring .IA_64.unwind_hdr section in file
"/usr/conf/mod/swspBus" . 3 warnings.
```
- After adding new LUNs and executing `ioscan`, a `syslog` message indicates that the `ioscan` operation aborted. If the newly added LUNs are owned by `sdisk` instead of `hsx` (Secure Path), run `rmsf - H h/w_addr` for that `sdisk` entry, and then run `ioscan` to enable ownership of the LUNs by Secure Path.
- Concurrent or overlapping `ioscans` can result in the first `ioscan` reporting the intermediate path states of the second `ioscan` while the second `ioscan` correctly reports the state of the paths. An application that performs `ioscan` comparisons could erroneously detect an error when overlapped by another `ioscan`.
- During an `ioscan`, `sdisk` drivers attach to `swsp` interface drivers instead of to the `fcpararray` (SCSI-3) or `fcpdev` (SCSI-2). Be careful with applications that use `ioscan` outputs that depend on the hardware tree that existed prior to Secure Path installation.
- When a path to a device managed by LVM becomes unavailable because of a controller, path link, switch, or HBA failure, I/O requests can be delayed by up to one minute immediately after the failure. As a result, the responsiveness of mirrored logical volumes could be briefly affected.

When a physical volume becomes unavailable, applications normally experience a delay while an I/O request to that physical volume times out. By default, this delay lasts 30 seconds, (although you can change the duration of the delay by using the `pvchange (1M)` command).

- In the case of a read operation, LVM selects another mirror and tries again.
- In the case of a write operation, LVM records the error and continues as long as the data has been successfully written to at least one mirror.

In either case, with Secure Path installed, this initial timeout can last up to one minute. After the time-out, LVM keeps track of the physical volume status as “Unavailable”, and future I/O requests will not suffer this delay.

- Do not make any SAN configuration changes to the system during the upgrade/installation of Secure Path 3.0F. For example, do not add new arrays or LUNs, or delete arrays/LUNs during upgrade/installation of 3.0F.
- Due to constraints imposed by the software distributor (SD) tools, the server’s network must be configured prior to the installation of Secure Path.
- Stopping `spagent` using the `spinit stop` command, and then starting `spagent` using the `spinit start` command results in `stderr` messages. To keep these messages from printing, start `spagent` in a new session and then exit that session.
- Do not use the HP system administration manager (SAM) to create or extend volume groups. Creating and extending volume groups must be done using HP-UX commands. When SAM scans for hardware, any HSGxx/HSVxxx LUNs created after the first LUN are not parsed correctly by SAM and cannot be selected to create a volume group. Use HP-UX commands to create or extend volume groups, and then use SAM to create and manage logical volumes.
- Ensure that 2-GB Fibre Channel switches have port speeds correctly set, and that they are not set to auto-negotiate.
- When creating snapshots or clones of a device that is managed by LVM, be careful not to misconfigure LVM. After creating a snapshot or clone of a physical volume, always run `vgchgid (1M)` to break the association between the volume group and the snapshot or clone. Otherwise, LVM will assume that the snapshot or clone is an alternate path to the original physical volume. This misconfiguration could lead to data corruption if the snapshot or clone was added later to the volume group by means of `vgextend (1M)`, `vgimport (1M)`, or `vgscan (1M)`.

- When replacing array controllers online, enable the path verification to update controller IDs in Secure Path data structures. You can also enable the path verification after replacing the array controllers to update the controller IDs in Secure Path data structure.
- For HP-UX 11.0, when you upgrade from an earlier version of Secure Path 3.0F to Secure Path 3.0F, all the LUNs move to the unattached list. You can view all the unattached LUNs using `spmgr display -u` command. To add the LUNs back to the list, use the `spmgr add` command.

Problem with setboot command

The `setboot` command fails to set the alternate or high availability hardware path on HP-UX 11i v2.0 PI-IA for SAN boot disks on EVA active-passive disk arrays.

Follow the steps below to set the primary, alternate, and high availability hardware paths from the EFI shell, which requires a system reboot.

1. If Secure Path is not installed on your system, run `ioscan -fneC disk` and record the EFI path given for each bootable device along with its physical hardware path. If Secure Path is installed on your system, refer to the sub-section "Identifying the EFI path of the physical hardware path on systems with Secure Path installed" later in this advisory.

```

Class I  H/W Path Driver   S/W State   H/W Type Description
=====
disk    2  0/0/2/1.3.0   sdisk    CLAIMED    DEVICE    HP
DVD-ROM 305
                                /dev/dsk/c1t3d0   /dev/rdisk/c1t3d0

Acpi(HWP0002,0)/Pci(2|1)/Scsi(Pun3,Lun0)/\EFI\HPUX\HPUX.EFI
disk    0  0/1/1/0/1/1.0.0   sdisk    CLAIMED    DEVICE
HP 36.4GST336753LC
                                /dev/dsk/c3t0d0   /dev/dsk/c3t0d0s2   /dev/rdisk/c3t0d0
                                /dev/rdisk/c3t0d0s2

                                /dev/dsk/c3t0d0s1   /dev/dsk/c3t0d0s3   /dev/rdisk/c3t0d0s1
                                /dev/rdisk/c3t0d0s3

Acpi(HWP0002,100)/Pci(1|0)/Pci(1|1)/Scsi(Pun0,Lun0)/HD(Part1,Sig
gC44D04A0-0672-11D9-8002-D6217B60E588)/\EFI\HPUX\HPUX.EFI
disk    6  0/2/1/0.16.1.0.0.0.3   sdisk    CLAIMED    DEVICE
COMPAQ HSV110 (C)COMPAQ

Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN5002B36C,Lun0)/HD(Part1,Sig
C8FB3EDE-79D3-11D9-8002-D6217B60E588)/\EFI\HPUX\HPUX.EFI
disk    14  0/2/1/0.16.4.0.0.0.3   sdisk    CLAIMED    DEVICE
COMPAQ HSV110 (C)COMPAQ

Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN5002B36D,Lun0)/HD(Part1,Sig
C8FB3EDE-79D3-11D9-8002-D6217B60E588)/\EFI\HPUX\HPUX.EFI
disk    17  0/5/1/0.16.1.0.0.0.3   sdisk    CLAIMED    DEVICE
COMPAQ HSV110 (C)COMPAQ

Acpi(HWP0002,500)/Pci(1|0)/Fibre(WWN5002B36C,Lun0)/HD(Part1,Sig
C8FB3EDE-79D3-11D9-8002-D6217B60E588)/\EFI\HPUX\HPUX.EFI
disk    26  0/5/1/0.16.4.0.0.0.3   sdisk    CLAIMED    DEVICE
COMPAQ HSV110 (C)COMPAQ

Acpi(HWP0002,500)/Pci(1|0)/Fibre(WWN5002B36D,Lun0)/HD(Part1,Sig
C8FB3EDE-79D3-11D9-8002-D6217B60E588)/\EFI\HPUX\HPUX.EFI

```

2. During the system boot, interrupt the boot process at EFI boot manager

```
EFI Boot Manager ver 1.10 [14.60] Firmware ver 2.21 [4306]
```

```
Please select a boot option
```

```
    HP-UX Primary Boot: 0/5/1/0.16.4.0.0.0.3
```

```
    HP-UX HA Alternate Boot: 0/1/1/0/1/1.0.0
```

```
    HP-UX Alternate Boot: 0/1/1/0/1/1.2.0
```

```
    EFI Shell [Built-in]
```

```
    Boot option maintenance menu
```

```
    Security/Password Menu
```

```
    Use ^ and v to change option(s). Use Enter to select an option
```

3. Select the **Boot option maintenance** menu

```
    Boot from a File
```

```
    Add a Boot Option
```

```
    Delete Boot Option(s)
```

```
    Change Boot Order
```

```
    Manage BootNext setting
```

```
    Set Auto Boot TimeOut
```

```
    Select Active Console Output Devices
```

```
    Select Active Console Input Devices
```

```
    Select Active Standard Error Devices
```

```
    Cold Reset
```

```
    Exit
```

4. Select Add a Boot Option

```
IA64_EFI
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36C,Lun400300
0000000000)/HD(Part1,SigC8FB3EDE-79D3-11D9-800)

IA64_EFI
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36C,Lun400300
0000000000)/HD(Part3,SigC8FB3F38-79D3-11D9-800)

IA64_EFI
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36D,Lun400300
0000000000)/HD(Part1,SigC8FB3EDE-79D3-11D9-800)

IA64_EFI
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36D,Lun400300
0000000000)/HD(Part3,SigC8FB3F38-79D3-11D9-800)

IA64_EFI
[Acpi(HWP0002,100)/Pci(1|0)/Pci(1|1)/Scsi(Pun2,Lun0)/HD(Part1,S
ig8CC0A96A-6072-11D9-800)

IA64_EFI
[Acpi(HWP0002,100)/Pci(1|0)/Pci(1|1)/Scsi(Pun2,Lun0)/HD(Part3,S
ig8CC0A9BA-6072-11D9-800)

Removable Media Boot [Acpi(HWP0002,0)/Pci(2|1)/Scsi(Pun3,Lun0)]
Load File [EFI Shell [Built-in]]

Load File
[Acpi(HWP0002,100)/Pci(1|0)/Pci(4|0)/Mac(00306E495F6F)

Exit
```

Note: To have the LUNs from other controller to be listed in the options, refer to sub-section Enumerating all Fibre Channel devices later in this advisory

5. Select any of the Fibre options (as mentioned in step1). Select the boot partition **Part1**.

Example:

```
IA64_EFI
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36D,Lun400300
0000000000)/HD(Part1,SigC8FB3EDE-79D3-11D9-800)

02/08/05 08:18a <DIR> 4,096 EFI

[Treat like Removable Media Boot]

Exit
```

6. Next, select EFI directory

```
02/08/05 08:18a <DIR>      4,096 .
02/08/05 08:18a <DIR>          0 ..
02/08/05 08:18a <DIR>      4,096 HPUX
02/08/05 08:18a <DIR>      4,096 Intel_Firmware
02/08/05 08:18a <DIR>      4,096 DIAG
02/08/05 08:18a <DIR>      4,096 HP
02/08/05 08:18a <DIR>      4,096 TOOLS
Exit
```

7. Now, select HPUX directory

```
02/08/05 08:18a <DIR>      4,096 .
02/08/05 08:18a <DIR>      4,096 ..
02/08/05 08:33a           521,494 HPUX.EFI
02/08/05 08:33a           24,576 NBP.EFI
Exit
```

8. Next, select HPUX.EFI

```
Filename: \EFI\HPUX\HPUX.EFI
DevicePath:
[Acpi(HWP0002,200)/Pci(1|0)/Fibre(WWN50001FE15002B36D,Lun400300
0000000000)/HD(Part1,SigC8FB3EDE-79D3-11D9-8002-D6217B60E588)/\
EFI\HPUX\HPUX.EFI]
IA-64 EFI Application 02/08/05 08:33a      521,494 bytes
Enter New Description:
```

Note: If the display is Edit Existing Boot Option or make a new entry [E-Edit N-New]:, means the particular device is already existing in the boot option. Proceed further but do not save the changes to NVRAM, i.e. proceed till step 10 and enter 'N' when prompted.

9. Enter a description that you want to display in the available boot options in the EFI boot manager.

For example:

```
Enter New Description: 0/2/1/0.16.4.0.0.0.3
```

```
New BootOption Data. ASCII/Unicode strings only, with max of 240 characters
```

```
Enter BootOption Data Type [A-Ascii U-Unicode N-No BootOption] :
```

10. Enter 'N'

```
Enter BootOption Data Type [A-Ascii U-Unicode N-No BootOption] :  
None
```

11. Enter 'Y'

```
Save changes to NVRAM [Y-Yes N-No]:
```

12. Select **Exit** to return to the **Boot option maintenance** menu as described in step 3. Select **Change Boot Order**.

13. Select the newly added boot option and using the keys 'U' or 'u' move it to the desired position in the boot order.

14. Select **Save changes to NVRAM** to use the newly added boot option in the chosen position in the EFI boot manager.

Next, you need to identify the EFI path of the physical hardware path on systems that has the Secure Path installed.

15. Now, note down the active controller serial number using `spmgr display -dv <HSx boot device>`. In this example it is P5849D5AAPN00W.

For example:

```
Server:  aphia3.india.hp.com    Report Created:  Fri, Feb 25
18:33:19 2005
```

```
Command: spmgr display -dv c24t0d2
```

```
Device:      c24t0d2
```

```
Status:      Operational [8 paths (4/0/4)]
```

```
Storage:     5000-1FE1-5002-B360
```

```
LUNID:       6005-08B4-0001-3680-0001-0000-0083-0000
```

```
Preferred Controller: None
```

```
HBAs:                td0  td3
```

```
Item Device          Controller      HBA          H/W_Path
Instance
```

```
=====
```

```
0  c24t0d2          P5849D5AAPN00W td0          255/255/0/0.2
c4t0d3
```

```
      WWPN: Unknown          Path State: Active [P]
```

```
1  c24t0d2          P5849D5AAPN00W td0          255/255/0/0.2
c10t0d3
```

```
      WWPN: Unknown          Path State: Active
```

```
2  c24t0d2          P5849D5AAPU05E td0          255/255/0/0.2
c6t0d3
```

```
      WWPN: Unknown          Path State: Standby
```

```
3  c24t0d2          P5849D5AAPU05E td0          255/255/0/0.2
c8t0d3
```

```
      WWPN: Unknown          Path State: Standby
```

16. Note down the port WWNs of this active controller. You can obtain this by the Command View EVA. For this controller P5849D5AAPN00W the port WWNs are 50001FE15002B36C and 50001FE15002B36D.

To enumerate all fibre channel devices:

17. Select EFI Shell [Built-in] from the EFI boot manager as described in step 2.

```
Shell> drivers
V  VERSION    E G G #D #C  DRIVER NAME IMAGE NAME
== ===== = = = == == =====
14 00000010    B - - 8 17          PCI Bus Driver
PciBus
25 00000110    B X X 1 6          HP Tachyon XL2 Fibre Channel
Mass S PciRom Seg=00000000
27 00000140    D X X 1 -          HP 2 Gb Fibre Channel Driver
PciRom Seg=00000000
28 00000140    D X X 1 -          HP 2 Gb Fibre Channel Driver
PciRom Seg=00000000
2B 00000110    B X X 1 6 HP Tachyon XL2 Fibre Channel Mass S
PciRom Seg=00000000

Choose the fibre channel drivers of the system
Shell> drvcfg 25
Configurable Components
  Drv[25] Ctrl[26] Lang[eng]
Shell> drvcfg -s 25 26
Current policy: Enumerate all Fibre Channel devices
Please select the desired enumeration policy:
  0 : Enumerate all Fibre Channel boot devices in the boot
option list
  1 : Enumerate all Fibre Channel devices
  Q : exit with no change
Policy >
Choose 1.
Repeat the steps for the other driver instance too (in this
example 2B)
Shell> reconnect -r
Shell> exit
```

Reconfiguring dump devices in the event of path failover

Note: This section applies only to HP-UX 11i v1.0. Reconfiguration of dump devices in the event of a path failover is automatic in later versions of HP-UX.

In the event of a path failure to a device that is configured as a system dump device, a reconfiguration using an alternate active path to the device is automatically attempted.

Under certain extreme circumstances, dump reconfiguration using the new path may fail (for example, dump configuration through `crashconf (1M)` occurring in parallel to a path failover event and the event, timing out).

If this occurs, an error message is logged in `/var/adm/syslog/syslog.log`, with the device name for the failed automatic path reconfiguration.

Use the following procedure to recover from this situation:

1. Note the `ctd/volume` name of the device for which configuration has failed (based on information in the error message).
2. Ensure that this device is a dump device using the `crashconf (1M)` command.
3. Reconfigure this device as dump device using the `crashconf (1M)` command.

LUN collision

If path polling is disabled and if a device is unrepresented before deleting the device with the `spmgr delete` command, and a new device is added with the same virtual disk or unit number as the old device, the new device is bound to the WWLUNID of the old deleted device. This leaves the newly added LUN in an inconsistent state. Do not perform any operations until you perform the following recovery procedure:

1. Ensure that the old LUN is not in use (for example, suspend I/O).
2. Put the LUN in an inactive state:
 - If the LUN is mounted, unmount it.
 - If the LUN is part of LVM volume group, deactivate it.

3. When the LUN is in an inactive state, enter the following commands:

```
spmgr delete old_device
ioscan
insf -e
```

4. Confirm that the new LUN is discovered by entering the `spmgr display` command.

Note: Prevent the LUNs from being left in an inconsistent state by always deleting a device with `spmgr delete` before unrepresenting the device.

If path polling is enabled, the LUN collision is identified and displays an appropriate message in the syslog. Follow the instructions in syslog to recover from this problem.

Problem in analyzing crash dumps

If the system is not rebooted after a installation of Secure Path, you may not be able to analyze the dump that results from a subsequent system crash. This occurs because the kernel in the memory during the dump differs from the kernel on the disk as the dynamic modules of Secure Path are converted to a static state after the installation.

Use one of the following procedures to analyze these dumps.

If you are running HP-UX 11i v1.0

To analyze a crash dump if you are running HP-UX 11i v1.0:

1. Enter the following commands:

```
cp /usr/conf/km.d/hsx/mod.o /stand/dlkm/mod.d/hsx
cp /usr/conf/km.d/swsp/mod.o /stand/dlkm/mod.d/swsp
cp /usr/conf/km.d/swspBus/mod.o /stand/dlkm/mod.d/swspBus
```

2. Enter the following command to save the crash image and related files in the directory `dirname/crash.n`. (The extension `n` is a number that increases by one each time `savecrash` runs with the same `dirname`).

```
savecrash -r dirname
```

`dirname` is the name of the existing directory in which to store the crash dump. The default is `/var/adm/crash`.

3. Enter the following commands:

```
cp /tmp/vmunix.CPQswsp dirname/crash.n/vmunix
rm /stand/dlkm/mod.d/hsx
rm /stand/dlkm/mod.d/swsp
rm /stand/dlkm/mod.d/swspBus
```

If you are running HP-UX 11i v2.0

To analyze a crash dump if you are running HP-UX 11i v2.0:

1. Enter the following command:

```
cp /tmp/vmunix.CPQswsp /.../crash.n/vmunix
```

The: /.../crash.*n*/ is the complete path to the crash directory.

Note: Before installation (`./stand/vmunix`), Secure Path saves the backup of `vmunix` in `/tmp/vmunix.CPQswsp`.

If the system was booted with a `vmunix` different from the default path `/stand/vmunix`, HP recommends that you take the backup of the `vmunix` from which the system was booted. Use this backup of `vmunix` instead of `/tmp/vmunix.CPQswsp` to recover from the crash.

If the system has been rebooted at least once since a new installation of Secure Path, then the previously mentioned problem should not occur

Managing Event Monitoring Service (EMS)

This section contains information about Secure Path's event monitoring services, including:

- High-availability EVA environment recommendations
- EVA
- HSG80 controller
- Disabling hardware monitoring

High-availability EVA environment recommendations

In high-availability environments with heavy I/O loads, you may experience I/O time-out conditions. If I/O timeouts occur, HP recommends that you use the `pvchange` command to increase the `IO_timeout` value from a default of 30 seconds to no more than 60 seconds for LUNs (virtual disks) on V2.0 of the

Enterprise Virtual Array (EVA). Under heavy I/O load conditions, the increased `IO_timeout` value allows for longer I/O completion times and for LUN access delays if a controller failover condition occurs.

Note: Make sure that you have HP MC/ServiceGuard configured properly. Refer to your HP MC/ServiceGuard documentation for configuration information or go to the HP web site at <http://docs.hp.com>.

EVA

Disable the Event Monitoring Service (EMS) for all of the devices/LUNs in an EVA.

HSG80 controller

EMS logs erroneous HSG80 LUN errors due to an incompatibility issue between EMS and the HSG80 controllers. The HSG80 devices do not have operating problems, and you can ignore the messages.

If these `syslog` events are objectionable, you can avoid the erroneous error message by disabling EMS monitoring of the HSG80 devices. Use the procedure in the “[Disabling hardware monitoring](#)” on page 24 to disable the EMS hardware monitor for HSG80 devices.

Disabling hardware monitoring

This section describes how to disable the EMS hardware monitor. Use this procedure to prevent the EMS from logging erroneous HSG80 LUN errors.

About the `disabled_instances` file

The `startmon_client` program reads the following `disabled_instances` file:

```
/var/stm/data/tools/monitor/disabled_instances
```

The `startmon_client` program reads the `disabled_instances` file before reading the `*.sapcfg` file. Therefore, there is no startup of the monitor for the specific instance listed in the `disabled_instances` file.

The `disabled_instances` file is a text file that lists each fully qualified instance, one instance per line. You can use wild cards in the instance names to specify more than one instance. For example, the following entry specifies all the instances associated with the default disk resource names:

```
/storage/events/disks/default/*
```

For those instances listed in the `disabled_instances` file, no monitoring requests will show in the display for the `monconfig (C)heck monitors` command.

Note: This does not mean that the monitor stops polling the device. It means that any events will not be forwarded to the log files, based on information in the `*.sapcfg` files.

Using the `disabled_instances` file to disable hardware monitoring

The following steps describe using the `disabled_instances` file to disable an EMS hardware monitor for a single instance (enabled in IPR0009):

1. Run `/etc/opt/resmon/sbin/monconfig` at the monitoring request manager main menu.
2. Choose **(K)ill (disable) monitoring**.
3. With an editor of your choice, add instances to the `disabled_instances` file in the following directory:

```
/var/stm/data/tools/monitor/
```

4. Add the string located at the top of the EMS event message, similar to the following example:

```
/storage/events/disks/default/0_0_254.0.0.5
```

5. Save the file.
6. Run `monconfig` again and choose **(E)nable monitoring**.
7. Wait for monitoring to be re-enabled, and then choose **(C)heck monitors**.

The resource class that was disabled should display in the list, with no monitoring requests.

Procedure for determining the standby path's hardware path

The *HP StorageWorks Secure Path V3.0F for HP-UX 11i v1.0, 11i v2.0 and HP-UX 11i v1.0, 11i v2.0 Workgroup Edition installation guide*, section “Installing Secure Path on a SAN Boot Device” instructs you to determine the hardware path of a standby path by using the `spmgr display` and `ioscan` commands.

Use the following procedure to determine the hardware path of a standby path.

1. Enter the `spmgr display -dv boot_device` command on the host. In the following example, the boot device is `/dev/dsk/c12t1d2`:

```
spmgr display -dv c12t1d2
```

The following output is displayed:

```
Server:aphn1.india.hp.comReport Created: Fri, Jan 30 18:44:42 2004
Command: spmgr display -dvc12t1d2
```

```
Device:c12t1d2
Status:Operational[4 paths (1/0/2)]
Storage: 5000-1FE1-0015-0AE0
LUNID: 6005-08B4-0001-4920-0001-6000-04EA-0000
Preferred Controller: None
HBAs:td4td6
```

Item	Device	Controller	HBA	H/W_Path	Instance
0	c12t1d2	P4889B49IM403L	td4	255/255/0/2.3	c4t1d3
WWPN: N/A Path State: Active					
1	c12t1d2	P4889B49IM403L	td6	255/255/0/2.3	c8t1d3
WWPN: N/A Path State: Available					
2	c12t1d2	P4889B49IM403A	td4	255/255/0/2.3	c6t1d3
WWPN: N/A Path State: Standby					
3	c12t1d2	P4889B49IM403A	td6	255/255/0/2.3	c10t1d3
WWPN: N/A Path State: Standby					

The output in this example shows four operation paths; one is in active path state, one is in available path state, and two are in standby path state. Choose one of the standby instances to determine the hardware path, for example `c6t1d3`. Note the values of `c(6)`, `t(1)` and `d(3)` in the instance.

2. Execute the `ioscan -kfnC ext_bus` command. Output similar to the following is displayed

```
# ioscan -kfnC ext_bus
```

```

Class   I  H/W Path Driver S/W State  H/W Type  Description
=====
ext_bus 0  0/0/1/0 c720 1 CLAIMED  INTERFACE SCSI C896 Ultra
Wide Single-Ended
ext_bus 1  0/0/1/1 c720  CLAIMED  INTERFACE SCSI C896 Ultra
Wide Single-Ended
ext_bus 2  0/0/1/1 c720  CLAIMED  INTERFACE SCSI C87x Ultra
Wide Single-Ended
ext_bus 3  0/0/1/1 c720  CLAIMED  INTERFACE SCSI C87x Ultra
Wide Single-Ended
ext_bus 4  0/3/0/0.1.10.0.0 fcparray CLAIMED INTERFACE FCP Array
Interface
ext_bus 6  0/3/0/0.1.11.0.0 fcparray CLAIMED INTERFACE FCP Array
Interface
ext_bus 12 255/255/0 swsp  CLAIMED  VIRTBUS HSV110 (C)COMPAQ
0x50001FE1500049B0

```

Use the second (instance) and third (H/W path) fields of the output to help determine the hardware path. Find the `ext_bus` device that has the same instance number as the value of `c` in [step 1](#). In this case, it is `ext_bus 6`.

```

ext_bus 6  0/3/0/0.1.11.0.0 fcparray CLAIMED INTERFACE FCP Array
Interface

```

- Append the `t` and `d` values from [step 1](#) `t(1)`, `d(3)` to the end of the hardware path determined in [step 2](#) to determine the hardware path of the standby path. In this case, the hardware path for the standby path `c6t1d3` is `0/3/0/0.1.11.0.0.1.3`.

Secure Path driver for active-passive disk arrays

- On HSG80-based systems, the `restart this_controller` and `restart other_controller` commands result in a change in the active controller. You may notice that there are no critical message reports that a failure has occurred or a different path has been selected. This is because the restart takes less time than required to validate a path failure.
- The rolling upgrade method, which upgrades ACS 8.7 to ACS 8.8 and is described in the *Maintenance and Service Guide of the Solution Software V8.8 for HP-UX*, fails if the server is running application I/O to the array being upgraded. You must quiesce all I/O to the array before starting the rolling upgrade procedure.

- On a server reboot, the active path comes up on the last path probed and *not necessarily on the preferred path*, regardless of the status of auto-restore or whether a preferred path has been selected. To restore the active paths to their preferred paths, enter the `spmgr restore all` command.
- After a LUN has been deleted with a `spmgr delete` command and the LUN is unrepresented at the array, any re-presenting of that device and an `ioscan` results in the device showing in the `spmgr display -u` unattached list. The Secure Path driver keeps track of the device WWLUNID deleted status.
- Using the `spmgr select` and `spmgr restore` commands on LUNs that are part of a partitioned HSG80 storageset results in all LUNs of that partition being selected or restored. If the path being selected or restored is on the opposite controller from the currently active path, the operation causes the HSG80 to move control of the storageset to that controller. All LUNs that are partitions of that storageset will also be moved.

Note: In a subsequent `spmgr display`, the LUN being operated on shows that the requested paths moved immediately. However, all the other LUNs of the partitioned HSG80 storageset must be polled either by path verification or by an I/O operation before `spmgr display` shows their movement.

- Do not make any SAN configuration changes to the system when upgrading or installing Secure Path. For example, do not add any new LUNs, or delete any arrays or LUNs.
- When the system is booting, do not execute any Secure Path commands until the Secure Path start-up services has started.
- If you configure some Secure Path devices under volume groups and reboot the system, the volume groups are not activated as part of the system's volume group configuration during boot time. This situation occurs because the Secure Path persistence module is loaded (at `init level 1`) only after the LVM configuration completes (before `init level 1`). The volume groups are activated by Secure Path's `init script` at `init level 2`.

- HSG80-based array settings for SCSI mode and operating system mode must be set properly for the array's version of ACS firmware, so that Secure Path 3.0F can work. The supported combinations of SCSI and operating system modes are shown in [Table 5](#).

Table 5: Supported SCSI and operating system modes

Secure Path version	ACS version	SCSI mode	Operating system mode
3.0F	8.6 or later	SCSI-2	HP
3.0F	8.7 or later	SCSI-3	HP_VSA

[Table 6](#) shows unsupported version/mode combinations with resulting error conditions and problem solutions.

Table 6: Unsupported SCSI and operating system modes

Secure Path version	ACS version	SCSI mode	Operating system mode	Error conditions and problem solution
3.0F	8.6 or 8.7	SCSI-3	HP	There are 17 paths claimed for every real path and the LUNs are not accessible. To resolve this problem, set the SCSI mode to SCSI-2 and reboot.
3.0F	8.7	SCSI-2	HP_VSA	No LUNs claimed by Secure Path. To resolve this problem, set the SCSI mode to SCSI-3 and run <code>ioscan</code> .

- Concurrent or overlapping `ioscans` can result in the first `ioscan` reporting intermediate path states of the second `ioscan`. The second `ioscan` will correctly reports the state of the paths. An application that is doing `ioscan` compares could erroneously detect an error when another `ioscan` overlaps.
- During an `ioscan`, `sdisk` drivers attach to `swsp` interface drivers instead of `fcpararray` (SCSI-3) or `fcpdev` (SCSI-2). Be careful with applications that use `ioscan` outputs that depend on the hardware tree that existed prior to the installation of Secure Path.

- When a path to a device managed by LVM becomes unavailable because of a controller, path link, switch, or host bus adapter failure, I/O requests can be delayed by up to one minute immediately after the failure. As a result, the responsiveness of mirrored logical volumes could be briefly affected.

When a physical volume becomes unavailable, applications normally experience a delay while an I/O request to that physical volume times out. By default, this delay is 30 seconds, but you can change the delay time with the `pvchange(1M)` command.

- In the case of a read command, LVM selects another mirror and tries again.
- In the case of a write command, LVM records the error and continues, as long as the data has been successfully written to at least one mirror.

In either case, with Secure Path installed, this initial timeout could take up to one minute. Afterwards, LVM keeps track of the physical volume status as unavailable and future I/O requests will not suffer this delay.

Note: Before deactivating the volume group, ensure that all the logical volumes of the volume group are unmounted.

Upgrading from Secure Path 3.0E to 3.0F in SCSI-3 mode results in loss of all preferred paths. The 3.0F.0 I/O stack routes SCSI-3 `hscx` paths through the `fcpdev` driver and 3.0F routes through the `fcpararray` driver. Because the `fcpdev` paths do not exist after the upgrade, the upgraded LUN paths are assigned new different instance numbers. This results in all preferred paths being lost in the upgrade because the new `space.h` persistent parameter file contains the old v3.0 preferred path instances. To avoid this problem, make a copy of the `spmgr display` output before upgrading to 3.0F and re-establish the desired preferred paths after the upgrade and before rebuilding the kernel.

Secure Path Manager (spmgr)

- If there are a large number of Secure Path devices configured to the system, the Secure Path startup service can take longer because device scanning is initiated to synchronize Secure Path persistence data.
- If a preferred path to a device is in the failed state and you issue a `spmgr restore -d device` command, the command line responds with the prompt only. The path remains in a failed state and no path change is made. This is the expected response to the command.

- The `spmgr alias` command is used to reference a large cumbersome old name with a shorter or clearer alias name. Reversing the argument order in `spmgr alias alias_name old_name` results in the alias name replacing the old name. Henceforward, any command using the old name results in an error. You must delete the alias for the old name to work correctly.

- The `spmgr alias` command checks a table of reserved words to prevent you from using words in an alias name that would result in unexpected behavior. However, this list is not comprehensive. Be careful to avoid using special characters that could be misinterpreted by the shell, such as a leading “-” or “\$.” The current list of reserved words maintained by `spmgr` is:

```
add    alias    client    delete    display    help    log
notify on      off      password prefer    quiesce restart
restore select set      spmgr     unalias  unprefer
```

- The `spmgr restore -r 0000-0000-0000-0000` command should produce an error for an invalid WWNN, but instead it successfully restores all preferred paths on all attached arrays just like `spmgr restore all`.
- If you enable auto-restore using the `spmgr set -a on` command, and select a new path using the `spmgr select -p path_instance` command, the user-selected path remains selected and will not be auto-restored. Auto-restore returns to the currently active path only if that path has failed and the failure has been repaired.
- The `spmgr add any_arg any_arg WWLUNID` command results in the following error message:

```
Lun should be 0-7
```

The error message should read:

```
Unable to locate an unclaimed unit with that World Wide LUN ID.
```

- The `spmgr display -d device` command requires a device (`c##d##`) as an argument, but accepts a WWLUNID as the argument and responds with missing or incorrect data. Use only *device* with the `-d` option.
- The `spmgr select -c controller -d device` command requires a *device* (`c##d##`) as the last argument but accepts a WWLUNID as the argument and accurately selects the controller of the LUN pointed to by the WWLUNID. Although the command works with the WWLUNID argument, use only *device* with the `-d` option.

- The `spmgr select` and `spmgr restart` commands occasionally respond with the following error message:

Error: Invalid Argument

However, the command completes correctly. If you see this error, verify command success with the `spmgr display` command.

- Notification event messages that contain fields for the adapter instance (`td#`), array WWNN, or LUN WWLUNID sporadically report either `DON'T CARE` or `**` as the identifier. This reporting error has no impact on Secure Path operation and specific failure or change parameters can be viewed with the `spmgr display` command.

Using `spmgr set -p on|off WWNN`, `spmgr set -a on|off WWNN` or `spmgr set -b on|off WWNN` without the `on|off` argument or using `spmgr set -f interval` without the `interval` argument always returns that parameter to the installation default values. That is, omitting the `on|off` argument returns path verification to on, auto-restore to off, load balancing to off, and the verification interval to 30 seconds.

Inter operability with Ignite-UX software

Ignite-UX software does not support Secure Path 3.0F for the following reasons:

1. When Secure Path 3.0F is installed on a system, the hardware addresses of all EVA disk LUNs change. During the recovery process, importing LVM volume groups existing on the EVA array may fail.
2. If the boot disk resides on an EVA array, the system will fail to boot due to an LVM configuration failure panic.
3. Secure Path 3.0F is not included in the installation kernel and is not part of the core HP-UX Operating System.

Secure Path 3.0F for active-active disk arrays

Differences between Secure Path 3.0E and 3.0F for active-active disk arrays

Listed below are the features supported in this version of Secure Path for active-active disk arrays:

- The Secure Path for active-active disk array now supports XP12000, EVA4000, EVA6000, and EVA8000.
- A new `autopath add` command is available to add devices that you have deleted from autopath control.
- A new `autopath delete` command is available to delete devices from autopath control.
- A new `autopath set` command is available to set the Load Balance Policy.
- This version of Secure Path for active-active disk array supports upto 32 paths to a LUN.
- The Secure Path for active-active disk array now supports multiple new options for `autopath display` command.
- The display format has been enhanced to distinguish the LUNs with respect to LUNWWID instead of the primary device path (`/dev/dsk`) format.
- In this version of Secure Path for active-active disk array, the LUNs of capacity zero bytes is not discovered.
- The manpage is updated to reflect all the above changes.

The following issues have been resolved in this release of Secure Path for active-active disk arrays:

- The SST algorithm has been enhanced to sample the alternate paths periodically. This helps in avoiding scenarios where all the I/O are pumped to one device path of an end LUN for a long time without considering the alternate paths.
- The timing window issue due to race conditions between `ioctl`s, device closure, and I/O has been resolved.
- The `Mode` value issue during an autopath device open from a character device, is now fixed.

Operating system support

Table 7 shows the system features and requirements for Secure Path 3.0F for active-active disk arrays. For additional support information, check the HP web site: <http://www.hp.com/support>.

Table 7: Secure Path 3.0F for active-active disk arrays requirements

System feature	Requirement
Operating system versions	HP-UX 11i v1.0 (64 bit) HP-UX 11i v2.0
HP-UX server system types	A-class: rp24xx K-class (64-bit only): Kx60, Kx70, Kx80 L-class: rp54xx N-class: N4000, rp74xx V-class: V2200, V2250, V2500 V2600 rp7410, rp8400 rx1600, rx2600, rx5670, rx4640, rx7650, rx8620 zx2000, zx6000 Superdome, Superdome Integrity
File systems	HFfs (UFS) JFS (VxFS) ¹
Fibre Channel adapters	HP A6826A HP A9782A HP A9784A HP A5158A HP A6795A HP A6685A (K-class server only)
Volume managers	HP Logical Volume Manager
Clusters	HP MC/Service Guard v A 11.15 or later
Fibre Channel modes	Switched Fabric and Arbitrated Loop

- Secure Path 3.0F for active-active disk array supports VxFS file system only on devices configured under LVM, for EVA 4000, EVA 6000, and EVA 8000 disk arrays. For devices which are not under LVM, VxFS file system is not supported with SecurePath, for these arrays.

Table 8 lists the supported devices and minimum driver requirements for this release and earlier releases. Notice that the entire list of storage arrays is supported for each HP-UX version.

Table 8: Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11i v1.0	A5158A A6795A A6685A	Fibre Channel B.11.11.01	XP 128 XP 256 XP 512
11i v1.0	A6826A A9782A A9784A A6685A	Fibre Channel B.11.11.03	XP 1024 XP 48 XP 12000 VA 7400
11i v2.0	A6795A A6826A A9782A A9784A	Fibre Channel B.11.23.01	VA 7410 VA 7100 VA 7110 EVA 4000 EVA 6000 EVA 8000 HP OpenView Continuous Access Storage Appliance

Table 9 lists the patch revisions for this release and earlier releases.

Table 9: Patch revisions for Secure Path 3.0F

HP-UX version	Patch revisions (minimum)
11i v1.0	Hardware Enablement Bundle june 2004 HWEnable11iB.11.11.0406.5 or later ULM-SERVICE B.11.11.01 SCSI Upper Layer Module Service PHKL_32670 1.0 SCSI Upper Layer Module Service Patch PHKL_30257 1.0Fibre Channel Mass Storage Patch
11i v2.0	N/A

Table 10 shows the configuration limits for Secure Path.

Table 10: Configuration limitations for Secure Path 3.0F

Parameter	Minimum	Max qualified	Max supported
Adapter support	Single HBA	4	Platform limit
Storage arrays per host	1	4	Platform limit
LUNs per storage array per host	1	Array limit	Array limit
Paths per LUNs	1	32	N/A

Avoiding problem situations

- PVLINKS is the preferred method to configure paths to an end LUN with LVM devices. Using a configure method other than PVLINKS could result in invalid LVM path status messages.
- The status of a path is updated only when I/O is performed through that path.
- Only Fibre Channel connectivity is supported.
- When all paths to an end LUN fail in the case of non-LVM devices with VXFS filesystem, I/O to the LUN aborts. The system reacts the same whether or not Secure Path is used.
- When all paths to an end LUN fail in the case of I/O to non-LVM devices with HFS filesystem, or for async I/O to non-LVM devices, I/O to the LUN waits until the connectivity through these paths is restored. I/O will start only if the original path (the path on which I/O was started) comes back, and not if any of the alternate paths comes back.
- Enter the `autopath discover` command before using newly added paths or devices. Secure Path does not recognize newly added paths or devices that are in use before the `autopath discover` command is executed.
- Discovery of New Paths / LUNs is effective only if `ioscan` and `insf -e` are executed prior to `autopath discover`
- If `ioscan` and `insf -e` are not run before the `autopath discover` command is run, and there are changes made in the SAN, `autopath discover` may take a very long time to complete because of attempted retries by the lower level layers on the device paths.

- Secure Path 3.0F for active-active disk arrays does not support devices configured under Veritas Volume Manager.
- Secure Path 3.0F for active-active disk arrays does not support wild card characters. For example, you cannot use the question mark (?) along with a command to invoke the `help` command.
- If `HPswsp` is marked for uninstallation using `swremove` and if uninstallation is aborted, Load Balance Policy settings defaults back to NLB.
- In a LUN collision scenario the new LUN is discovered through the paths used by the old LUN, provided the old LUN is not mounted or open. If the old LUN is mounted or open, the paths to the old LUN are marked failed since the LUN is unrepresented. To recover the old LUN, assign the same `SCSI LUN ID` to the old LUN. To access the new LUN, present it at a different `SCSI LUN ID` or unmount or close the old LUN and run `autopath discover` command.
- If the unattached list contains deleted LUN that you have configured under volume group, upon reboot the `autopath retrieve` command fails to retrieve the LUN back. As a workaround, deactivate the volume group till the retrieve functionality gets completed.

Secure Path 3.0F for Workgroup Edition Virtual Array (VA) disk arrays

Differences between Secure Path 3.0E and 3.0F for Workgroup Edition

Listed below are the features supported in this version of Secure Path for Workgroup Edition VA disk arrays:

- A new `autopath add` command is available to add devices that you have deleted from autopath control.
- A new `autopath delete` command is available to delete devices from autopath control.
- A new `autopath set` command is available to set the Load Balance Policy.
- The Secure Path for Workgroup Edition VA disk array now supports multiple new options for `autopath display` command.
- The display format has been enhanced to distinguish the LUNs with respect to LUNWWID instead of the primary device path (`/dev/dsk`) format
- This version of Secure Path for Workgroup Edition VA disk array supports upto 32 paths to a LUN.
- In this version of Secure Path for Workgroup Edition VA disk array, the LUNs of capacity zero bytes is not discovered.
- The manpage is updated to reflect all the above changes.

The following issues have been resolved in this release of Secure Path for Workgroup Edition VA disk arrays:

- The SST algorithm has been enhanced to sample the alternate paths periodically. This helps in avoiding scenarios where all the I/O are pumped to one device path of an end LUN for a long time without considering the alternate paths.
- The timing window issue due to race conditions between `ioctl`s, device closure, and I/O has been resolved.
- The `Mode` value issue during an autopath device open from a character device, is now fixed.

Operating system support

Table 11 shows the system features and requirements for Secure Path 3.0F Workgroup Edition for VA arrays. For more support information, check the HP web site: <http://www.hp.com/support>.

Table 11: Secure Path 3.0F Workgroup Edition for VA requirements

System feature	Requirement
Operating system versions	HP-UX 11i v1.0 (64 bit) HP-UX 11i v2.0
HP-UX server system types	A-class: rp24xx K-class (64-bit only): Kx60, Kx70, Kx80 L-class: rp54xx N-class: N4000, rp74xx V-class: V2200, V2250, V2500 V2600 rp7410, rp8400 rx1600, rx2600, rx5670, rx4640, rx7650, rx8620 zx2000, zx6000 Superdome, Superdome Integrity
File systems	HFfs (UFS) JFS (VxVfs)
Fibre Channel adapters	HP A6826A HP A9782A HP A9784A HP A5158A HP A6795A HP A6685A (K-class server only)
Volume managers	HP Logical Volume Manager
Clusters	HP MC/Service Guard v A 11.15 or later
Fibre Channel modes	Switched Fabric and Arbitrated Loop

[Table 12](#) lists the supported devices and driver requirements for this release and earlier releases. Notice that the all of the listed storage arrays are supported on all versions of HP-UX.

Table 12: Secure Path 3.0F for HP-UX 11i v1.0, 11i v2.0 requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11i v1.0	A5158A A6795A A6685A	Fibre Channel B.11.11.01	VA 7400
11i v1.0	A6826A A9782A A9784A A6685A	Fibre Channel B.11.11.03	VA 7410 VA 7100
11i v2.0	A6795A A6826A A9782A A9784A	Fibre Channel B.11.23.01	VA 7110

[Table 13](#) lists the patch revisions for this release and earlier releases.

Table 13: Patch revisions for Secure Path 3.0F

HP-UX version	Patch revisions (minimum)
11i v1.0	Hardware Enablement Bundle june 2004 HWEnable11iB.11.11.0406.5 or later ULM-SERVICE B.11.11.01 SCSI Upper Layer Module Service PHKL_32670 1.0 SCSI Upper Layer Module Service Patch PHKL_30257 1.0Fibre Channel Mass Storage Patch
11i v2.0	N/A

[Table 14](#) shows the configuration limits for Secure Path.

Table 14: Configuration limitations for Secure Path 3.0F

Parameter	Minimum	Max qualified	Max supported
Adapter support	Single HBA	4	Platform limit

Table 14: Configuration limitations for Secure Path 3.0F (Continued)

Parameter	Minimum	Max qualified	Max supported
Storage arrays per host	1	4	Platform limit
LUNs per storage array per host	1	Array limit	Array limit
Paths per LUNs	1	32	N/A

Avoiding problem situations

- PVLINKS is the preferred method to configure paths to an end LUN with LVM devices. Using a configure method other than PVLINKS could result in invalid LVM path status messages.
- The status of a path is updated only when I/O is performed through that path.
- Only Fibre Channel connectivity is supported.
- When all paths to an end LUN fail in the case of non-LVM devices with VXFS filesystem, I/O to the LUN aborts. The system reacts the same whether or not Secure Path is used.
- When all paths to an end LUN fail in the case of I/O to non-LVM devices with HFS filesystem, or for async I/O to non-LVM devices, I/O to the LUN waits until the connectivity through these paths is restored. I/O will start only if the original path (the path on which I/O was started) comes back, and not if any of the alternate paths comes back.
- Enter the `autopath discover` command before using newly added paths or devices. Secure Path does not recognize newly added paths or devices that are in use before the `autopath discover` command is executed.
- Discovery of New Paths / LUNs is effective only if `ioscan` and `insf -e` are executed prior to `autopath discover`
- If `ioscan` and `insf -e` are not run before the `autopath discover` command is run, and there are changes made in the SAN, `autopath discover` may take a very long time to complete because of attempted retries by the lower level layers on the device paths.
- Secure Path 3.0F for Workgroup Edition VA disk arrays does not support devices configured under Veritas Volume Manager.

- Secure Path 3.0F for Workgroup Edition VA disk arrays does not support wild card characters. For example, you cannot use the question mark (?) along with a command to invoke the `help` command.
- If `HPswsp` is marked for uninstallation using `swremove` and if uninstallation is aborted, Load Balance Policy settings defaults back to NLB.
- In a LUN collision scenario the new LUN is discovered through the paths used by the old LUN, provided the old LUN is not mounted or open. If the old LUN is mounted or open, the paths to the old LUN are marked failed since the LUN is unrepresented. To recover the old LUN, assign the same `SCSI LUN ID` to the old LUN. To access the new LUN, present it at a different `SCSI LUN ID` or unmount or close the old LUN and run `autopath discover` command.
- If the unattached list contains deleted LUN that you have configured under volume group, upon reboot the `autopath retrieve` command fails to retrieve the LUN back. As a workaround, deactivate the volume group till the retrieve functionality gets completed.