

release notes

HP StorageWorks Secure Path 3.0F Service Pack 1 for HP-UX 11.00 and Secure Path 3.0F Service Pack 1 Workgroup Edition for HP-UX 11.00



Part number: T3549-96501
Fifth edition: December 2005



Legal and notice information

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

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

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

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.

Printed in the U.S.

<http://www.hp.com>.

HP StorageWorks Secure Path 3.0F Service Pack 1 for HP-UX 11.00 and Secure Path 3.0F Service Pack 1 Workgroup Edition for HP-UX 11.00

About this document

This document summarizes the most recent product information about the HP StorageWorks Secure Path 3.0F SP1 for HP-UX 11.00 systems, including:

- [Release notes information](#)
- [Intended audience](#)
- [Accessing future products updates](#)
- [Other documentation](#)

Release notes information

This release notes contain the following topics:

- [Secure Path 3.0F SP1 kit contents](#)
- [Secure Path 3.0F SP1 for Active-Passive disk arrays](#)
 - [Differences between Secure Path for Active-Passive 3.0F and 3.0F SP1](#)
 - [Operating system support](#)
 - [Avoiding problem situations](#)
 - [Managing Event Monitoring Service \(EMS\)](#)
 - [Secure Path driver for Active-Passive disk arrays](#)
 - [Secure Path Manager \(spmgr\)](#)
 - [Interoperability with Ignite-UX software](#)
- [Secure Path 3.0F SP1 for Active-Active disk arrays](#)
 - [Differences between Secure Path 3.0F and 3.0F SP1 for Active-Active disk arrays](#)
 - [Operating system support](#)
 - [Avoiding problem situations](#)
- [Secure Path 3.0F SP1 for Workgroup Edition Virtual Array \(VA\) and Modular Smart Array \(MSA\) 1500 disk arrays](#)
 - [Differences between Secure Path 3.0F and 3.0F SP1 for Workgroup Edition](#)
 - [Operating system support](#)
 - [Avoiding problem situations](#)
- [Secure Path device path representation and usage](#)
 - [Device path representation of Secure Path for Active-Passive disk arrays](#)
 - [Device path representation of Secure Path for Active-Active disk arrays](#)
 - [Differences between Secure Path for Active-Active disk arrays and LVM PVLINKS](#)
 - [HP recommends](#)

Intended audience

This document is intended for customers who have purchased the HP StorageWorks Secure Path 3.0F SP1 for HP-UX 11.00 and are responsible for installing, configuring and maintaining this product in their HP-UX server environment.

Accessing future product updates

HP recommends that customers sign up online using the Subscriber's choice web site: <http://www.hp.com/go/e-updates>.

- Subscribing to this service provides you with e-mail updates on product enhancements, newer versions of drivers, and firmware documentation updates, as well as instant access to other product resources.
- After signing up, you can quickly locate your products by selecting Business support and then Storage under Product Category.

Other documentation

Additional documentation that you may find helpful includes:

- *HP StorageWorks Secure Path 3.0F Service Pack 1 for HP-UX 11.00 and Secure Path 3.0F Service Pack 1 Workgroup Edition for HP-UX 11.00 installation and reference guide, part number AA-RV17D-TE*
- Whitepapers and best-practices documents, are available at: <http://www.hp.com/country/us/eng/prodserv/storage.html>.

Secure Path 3.0F SP1 kit contents

The Secure Path 3.0F SP1 for HP-UX 11.00 kit includes:

- Secure Path 3.0F Service Pack 1 for HP-UX 11.00 readme.txt document.
- *HP StorageWorks Secure Path 3.0F Service Pack1 for HP-UX 11.00 and Secure Path 3.0F Service Pack1 Workgroup Edition for HP-UX 11.00 installation and reference guide, part number AA-RV17D-TE.*
- Secure Path 3.0F SP1for HP-UX 11.00 CD-ROM.

The Secure Path 3.0F SP1 for HP-UX 11.00 web kit includes:

- Secure Path 3.0F SP1 for HP-UX 11.00 readme.txt document.
- HP StorageWorks Secure Path 3.0F SP1 for HP-UX 11.00 compressed tar package, which includes the software and the release notes.

NOTE:

For Secure Path 3.0F SP1, `swlist` displays the version as A.3.0F.1F.0F.

Secure Path 3.0F SP1 release notes supersede all earlier versions of the release notes. Refer to your Secure Path 3.0F SP1 kit documentation for Secure Path operating details.

Secure Path 3.0F SP1 for Active-Passive disk arrays

This section contains the following information:

- [Differences between Secure Path for Active-Passive 3.0F and 3.0F SP1](#)
- [Operating system support](#)
- [Avoiding problem situations](#)
- [Managing Event Monitoring Service \(EMS\)](#)
- [Secure Path driver for Active-Passive disk arrays](#)
- [Secure Path Manager \(spmgr\)](#)
- [Interoperability with Ignite-UX software](#)

Differences between Secure Path for Active-Passive 3.0F and 3.0F SP1

This section contains the following information:

- [Issues resolved in Secure Path 3.0F SP1](#)
- [Changes made in this release](#)

Issues resolved in Secure Path 3.0F SP1

The following issues have been resolved in Secure Path 3.0F SP1 for Active-Passive disk arrays:

- The `spmgr add` command used to display an incorrect warning message in HP-UX 11.0 when there were no LUNs to add from the unattached list. This problem has been fixed and now the system displays an appropriate warning message when this issue occurs.
- The `spmgr delete` command used to display an incorrect message when it was not able to delete all the LUNs. This problem has been fixed and now the system displays an appropriate error message when this issue occurs.
- Under certain scenarios, if LUN collision occurs, after running the `ioscan` and `insf` commands, `sdisk` claims the device paths. This issue has been fixed in the current release. See [Avoiding problem situations](#) section for more information about LUN collision.
- The `spmgr select` command used to display a warning message indicating that a LUN belongs to a LUN group, even though the selected LUN was not part of a LUN group. This issue has been fixed in this version of Secure Path.
- The issue in removing the depot files from `/tmp` directory after un-installation, has been resolved.
- Under certain scenarios, the `spmgr add` command used to corrupt the data structures and hanged the system after a subsequent issue of `ioscan` command. This issue has been fixed in this version of Secure Path.
- Now, Secure Path for Active-Passive disk array no longer logs and displays the incorrect message (Configuration error. Invalid or missing target/LUN WWID entry for 60001FE1000FE8600009105071230009 on array 50001FE1000FE860.) when a new LUN is presented to the host and `ioscan` is run.

Changes made in this release

This release of Secure Path includes the following new feature:

- A new `spmgr refreshdisplay` command is available to update the serial numbers of all the available array controllers.

Operating system support

Table 1 lists the system features and requirements for Secure Path 3.0F SP1 for Active-Passive disk arrays. For additional support information, check the HP web site: <http://www.hp.com/support>.

Table 1 Secure Path 3.0F SP1 for Active-Passive disk arrays system feature and requirements

System feature	Requirement
Operating system versions	HP-UX 11.0 64-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 rp 3440, rp 4440, rp 7420
File systems	HFS (UFS) JFS (VxFS)
Fibre Channel Host Bus Adapters	HP A5158A HP A6795A HP A6685A (K-class–KX60, KX70, KX80 64-bit OS servers only)
Controllers	Dual HSG60 controllers operating ACS V8.6L or later Dual HSG80 controllers operating ACS V8.6F or later Dual HSV110 controllers operating VCS V3.010 or later Dual HSV100 controllers operating VCS V3.010 or later
Volume managers	HP Logical Volume Manager
Clusters	HP MC/Service Guard v A 11.13 or later
Fibre Channel modes	Switched fabric

NOTE:

Secure Path 3.0F SP1 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 for Active-Passive disk arrays.

Table 2 Secure Path 3.0F SP1 for Active-Passive disk arrays supported devices and driver requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11.00	A5158A A6795A A6685A	Fibre Channel B.11.00.10	RA8000/ESA12000 (HSG80) MA8000/EMA12000 (HSG80) MA6000 (HSG60) EMA16000 (HSG80)

Table 3 lists the patch revisions for this release of Secure Path for Active-Passive disk arrays.

Table 3 Patch revisions for Secure Path 3.0F SP1 for Active-Passive disk arrays

HP-UX version	Patch revisions (minimum)
11.00	<p>Hardware Enablement Bundle March 2004—HWE1100 B.11.00.0403.5</p> <p>Quality Pack Bundle Sept 2003 QPK1100 B.11.00.62.4</p> <p>Support Tools Bundle Sept 2003 - Online Diag B.11.00.26.07</p> <p>Kernel Patch (asyncio)—PHKL_30709—async disk driver, only required if running databases using raw (nonfile system) data access.</p> <p>NOTE: The asyncio patch number (formerly PHKL_27759 and PHKL_30709) has been updated to PHKL_33500.</p> <p>PHCO_27514 – mountall (1M) cumulative</p> <p>PHCO_27515 – umountall (1M) cumulative—Device IDs Enablement</p> <p>PHCO_27516 – fscclean (1M) Device IDs Enablement</p> <p>PHCO_29765 – umount (1M) cumulative</p> <p>PHCO_29769 – umount (1M) cumulative</p> <p>PHCO_30698</p> <p>PHKL_30607</p> <p>PHKL_32854</p> <p>PHKL_18543</p> <p>PHKL_30218</p>

Table 4 lists the configuration limits for Secure Path 3.0F SP1 for Active-Passive disk arrays.

Table 4 Configuration limitations for Secure Path 3.0F SP1 for Active-Passive disk arrays

Parameter	Minimum	Max qualified	Max supported
Adapter support	1	8	Platform limit
Storage arrays per host	1	8	128
LUNs per storage array per host	1	128	128

Avoiding problem situations

The following section lists problems that may arise during Secure Path operation and how to avoid those problems, including:

- [General problems](#)
- [LUN collision](#)
- [Installing Secure path in vPars environment](#)



IMPORTANT:

For Secure Path device path representation and usage, refer to [Secure Path device path representation and usage](#) section.

General problems

This section describes the general problem situations that may arise during Secure Path operation and how to avoid the problems:

- 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 avoid 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/HSVxx 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 assumes 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)`.

LUN collision

If path verification 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 device 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` command before unrepresenting the device.

Installing Secure path in vPars environment

This section provides information about the installation of Secure Path in vPars environment on an EVA boot LUN. Follow the steps below to have a flawless installment:

1. Install the HP-UX operating system on an EVA LUN.
2. Install Kernel Patch `PHKL_33581 (s700_800 11.23 USB DVD Boot, EFI Device Path, HW Enablement)`

 **NOTE:**

You must install the patch PHKL_33581 on each partition.

3. Install the HP-UX Virtual Partitions software A.04.02.01 and above.
 4. Create Virtual Partitions by running `vparcreate` command and then boot individual partitions.
-

 **NOTE:**

Refer to *Installing and Managing HP-UX Virtual Partitions* for more information on vPars.

5. Install Secure Path 3.0F SP1 in each partition.
-

 **NOTE:**

If you have installed Secure Path on an EVA boot LUN, you cannot install vPars on the same boot LUN.

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 EVA v2.0 or v3.0. 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 or 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 mentioned in the [Disabling hardware monitoring](#) 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, including:

- [About the disabled_instances file](#)
- [Using the disabled_instances file to disable hardware monitoring](#)

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 shows 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 not all the events are forwarded to the log files, based on information in the `*.sapcfg` files.

Using the disabled_instances file to disable hardware monitoring

The following procedure 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. Select (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 select (E)nable monitoring.
7. Wait for monitoring to re-enable, and then select (C)heck monitors.

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

Secure Path driver for Active-Passive disk arrays

Following are the problems that may arise for Secure Path driver for Active-Passive disk arrays:

- 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`.
- On HSG80-based systems, the `restart this_controller` and `restart other_controller` commands results 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 8.6 to ACS 8.7 and is described in the *Maintenance and service guide of the solution software 8.7 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.
- If a device is deleted using the `spmgr delete` command, without being unrepresented at the array, and then `ioscan` is run, the device is shown as unattached by the `spmgr display -u` command.

However, event notification messages written to each `spmgr` logging facility set to include informational events show the device as misconfigured until a new kernel is built and the server is rebooted. A message similar to the following example is displayed:

```
Configuration error. Invalid or missing target/lun wwid entry for
60001FE1000FE8600009105071230009 on array 50001FE1000FE860.
```

The message indicates the missing target or number for the device and not a problem with the configuration. The message repeats for any subsequent `ioscan` and ceases after the kernel rebuild or reboot has been done.

- 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.
- Using a known failed path to reboot results in unknown status of that path. For example, a system with four paths to a LUN with three active paths and one disabled path as seen with `spmgr display` is rebooted. The system `spmgr display` command displays only the three active paths. A subsequent repair of the path and an `ioscan` allows `spmgr` to again recognize the fourth path, but `spmgr notify` has no record of a repair event.
- Using the `spmgr select` and `spmgr restore` commands on LUNs that are part of a partitioned HSG80 LUN 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 LUN to that controller. All LUNs that are partitions of that LUN also gets 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 LUN must be polled either by path verification or by an I/O operation before `spmgr display` shows their movement.

- 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 SP1 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 SP1	8.6 or later	SCSI-2	HP
3.0F SP1	8.7 or later	SCSI-3	HP_VSA

Table 6 shows unsupported version or 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 SP1	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 SP1	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` 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, you can delay the I/O requests 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 using 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 do not suffer this delay.

 **NOTE:**

Before deactivating the volume group, ensure that all the logical volumes of the volume group are unmounted. See [Secure Path device path representation and usage](#) for more details.

Secure Path Manager (spmgr)

Following are the problems that may arise in `spmgr` for Active-Passive disk arrays:

- 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 run 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 use to refer 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` are listed below:

```
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` command.
- 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##t##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##t##d#*) as an 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.

Interoperability with Ignite-UX software

Ignite-UX software does not support Secure Path 3.0F SP1 for the following reasons:

- When Secure Path 3.0F SP1 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.
- Secure Path 3.0F SP1 is not included in the installation kernel and is not part of the core HP-UX operating system.

Secure Path 3.0F SP1 for Active-Active disk arrays

This section contains the following information:

- [Differences between Secure Path 3.0F and 3.0F SP1 for Active-Active disk arrays](#)
- [Operating system support](#)
- [Avoiding problem situations](#)

Differences between Secure Path 3.0F and 3.0F SP1 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 MSA1500 disk arrays.
- The Secure Path Active-Active disk arrays now supports a new option (-t) for `autopath set` command that allows you to make unlimited number of retries for a failed I/O of an inaccessible LUN. You can also specify a time interval for performing the number of retries.
- This version of Secure Path for Active-Active disk array lets you exclude few LUN's from Secure Path control.

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 `ioctls`, 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 lists the system features and requirements for Secure Path 3.0F SP1 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 SP1 for Active-Active disk arrays system features and requirements

System feature	Requirement
Operating system versions	HP-UX 11.00 64 bit only
HP-UX server system types	K-class (64-bit only): Kx60, Kx70, Kx80 L-class: rp54xx N-class: N4000, rp74xx rp 3440, rp 4440, rp 7420
File systems	HFfs (UFS) JFS (VxFs) ¹
Fibre Channel adapters	HP A5158A HP A6795A HP A6685A (K-class server only)
Volume managers	HP Logical Volume Manager
Clusters	HP MC/Service Guard v A 11.13 or later
Fibre Channel modes	Switched Fabric and Arbitrated Loop

¹Secure Path 3.0F SP1 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 Secure Path, for these arrays.

Table 8 lists the supported devices and minimum driver requirements for this release and earlier releases of Secure Path 3.0F SP1 for Active-Active disk arrays.

Table 8 Secure Path 3.0F SP1 for Active-Active disk arrays supported device and driver requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11.00	A5158A A6795A A6685A	Fibre Channel B.11.00.10	EVA 4000 EVA 6000 EVA 8000 MSA 1500 VA 7100 VA 7110 VA 7400 VA 7410 XP 48 XP 128 XP 256 XP 512 XP 1024 XP 10000 XP 12000 HP OpenView Continuous Access Storage Appliance

 **NOTE:**

The entire list of storage arrays is supported for each HP-UX version.

Table 9 lists the patch revisions for this release and earlier releases of Secure Path 3.0F SP1 for Active-Active disk arrays.

Table 9 Patch revisions for Secure Path 3.0F SP1 Active-Active disk arrays

HP-UX version	Patch revisions (minimum)
11.00	Hardware Enablement Bundle March 2004-HWE1100 B.11.00.0404.5 Quality Pack Bundle March 2004 Support Tools Bundle March 2004 ULM-SERVICE B.11.00.01 SCSI Upper Layer Module Service

Table 10 lists the configuration limits for Secure Path 3.0F SP1 Active-Active disk arrays.

Table 10 Configuration limitations for Secure Path 3.0F SP1 Active-Active disk arrays

Parameter	Minimum	Max qualified	Max supported
Adapter support	1	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

Following are the problems that may arise during Secure Path operations:

- 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 file system, 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 file system, 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 starts only if the original path (the path on which I/O was started) comes back, and not if any of the alternate path 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 or LUNs is effective only if `ioscan` and `insf -e` are executed prior to `autopath discover` command.
- If `ioscan` and `insf -e` are not run before running the `autopath discover` command, and if there are changes made in the SAN, `autopath discover` may take very long time to complete because of attempted retries by the lower level layers on the device paths.
- Secure Path 3.0F SP1 for Active-Active disk arrays does not support devices configured under Veritas Volume Manager. However, you can exclude few LUNs from Secure Path control and can use them in Veritas Volume Manager or other similar applications.
- Secure Path 3.0F SP1 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 removing using `swremove` and if remove process is aborted, Load Balancing Policy settings defaults back to NLB.
- Secure Path 3.0F SP1 for Active-Active disk arrays does not support assigning the `scsi LUN ID` (different from `WWLUN ID`) of an unrepresented LUN to another LUN. Running the `autopath discover` command in such a scenario may put the system in a highly inconsistent state.

 **NOTE:**

- Secure Path 3.0F SP1 for Active-Active disk array supports infinite retry only for VxFS file systems.
 - If a device configured under HFS file system encounters an *All Paths Fail* condition, the I/O restarts only if the path on which original I/O is sent down by Secure Path is active.
 - If the file system changes from VxFS to HFS, Secure Path 3.0F SP1 for Active-Active disk arrays does not automatically set the timeout value for a LUN as *infinite retry*.
-

 **IMPORTANT:**

For Secure Path device path representation and usage, refer to [Secure Path device path representation and usage](#) section.

Secure Path 3.0F SP1 for Workgroup Edition Virtual Array (VA) and Modular Smart Array (MSA)1500 disk arrays

This section contains the following information:

- [Differences between Secure Path 3.0F and 3.0F SP1 for Workgroup Edition](#)
- [Operating system support](#)
- [Avoiding problem situations](#)

Differences between Secure Path 3.0F and 3.0F SP1 for Workgroup Edition

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

- The Secure Path Workgroup Edition disk array now supports MSA1500 disk arrays.
- The Secure Path Workgroup Edition now supports a new option (`-t`) for `autopath set` command that allows you to make unlimited number of retries for a failed I/O of an inaccessible LUN. You can also specify a time interval for performing the number of retries.
- This version of Secure Path for Workgroup Edition disk array lets you exclude LUN's from the Secure Path controls.

The following issues were resolved in this release of Secure Path:

- 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 lists the system features and requirements for Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 disk arrays. For more support information, check the HP web site: <http://www.hp.com/support>.

Table 11 Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 system features and requirements

System feature	Requirement
Operating system versions	HP-UX 11.00 64 bit only
HP-UX server system types	K-class L-class: rp54xx N-class: rp74xx
File systems	HFfs (UFS) JFS (VxFs)
Fibre Channel adapters	HP A5158A HP A6795A HP A6685A (K-class server only)
Volume managers	HP Logical Volume Manager
Clusters	HP MC/Service Guard v A 11.13 or later
Fibre Channel modes	Switched Fabric and Arbitrated Loop

Table 12 lists the supported devices and minimum driver requirements for this release and earlier releases of Secure Path 3.0F SP1 for Workgroup Edition for VA disk arrays. Notice that the entire list of storage arrays is supported for each HP-UX version

Table 12 Secure Path 3.0F SP1 for Workgroup Edition VA and MSA1500 disk arrays supported device and driver requirements

HP-UX version	Supported HBAs	Minimum revision drivers	Supported storage arrays
11.00	A5158A A6795A A6685A	Fibre Channel B.11.00.10	MSA 1500 VA 7100 VA 7110 VA 7400 VA 7410

Table 13 lists the patch revisions for this release and earlier releases of Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 disk arrays.

Table 13 Patch revisions for Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 disk arrays

HP-UX version	Patch revisions (minimum)
11.00	Hardware Enablement Bundle March 2004-HWE1100 B.11.00.0404.5 Quality Pack Bundle March 2004 Support Tools Bundle March 2004 ULM-SERVICE B.11.00.01 SCSI Upper Layer Module Service

Table 14 lists the configuration limits for Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 disk arrays.

Table 14 Configuration limitations for Secure Path 3.0F SP1 Workgroup Edition for VA and MSA1500 disk arrays

Parameter	Minimum	Max qualified	Max supported
Adapter support	1	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

Following are the problems that may arise during Secure Path operations:

- 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 file system, 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 file system, 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 starts only if the original path (the path on which I/O was started) comes back, and not if any of the alternate path 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 or LUNs are effective only if `ioscan` and `insf -e` are executed prior to `autopath discover` command.
- If `ioscan` and `insf -e` are not run before running the `autopath discover` command, and if there are changes made in the SAN, `autopath discover` may take very long time to complete because of attempted retries by the lower level layers on the device paths.
- Secure Path 3.0F SP1 Workgroup edition does not support the devices configured under Veritas Volume Manager. However, you can exclude few LUNs from Secure Path control and can use them in Veritas Volume Manager or other similar applications.
- Secure Path 3.0F SP1 Workgroup Edition 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 removing using `swremove` command and if uninstallation is aborted, Load Balancing Policy settings defaults back to `NLB`.
- The Secure Path Workgroup Edition does not support assigning the `scsi LUN ID` (different from `WWLUN ID`) of an unrepresented LUN to another LUN. Running the `autopath discover` command in such a scenario may put the system in a highly inconsistent state.



IMPORTANT:

For Secure Path device path representation and usage, refer to [Secure Path device path representation and usage](#) section.

Secure Path device path representation and usage

This section provides information about device path representation, usage, and the best practice recommended by HP for the devices controlled by Secure Path, including:

- [Device path representation of Secure Path for Active-Passive disk arrays](#)
- [Device path representation of Secure Path for Active-Active disk arrays](#)
- [Differences between Secure Path for Active-Active disk arrays and LVM PVLINKS](#)
- [HP recommends](#)

Device path representation of Secure Path for Active-Passive disk arrays

Secure Path for Active-Passive disk array uses single virtual path to represent an end device. The operations on the device are carried out on the virtual device path. You cannot view or access the physical paths present to an end device, as they are hidden.

Example:

```
# spmgrp display
=====
Storage: 5000-1FE1-5002-EB30
Load Balance: Off   Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: fcd0 fcd1
Controller: P5849D5AAPL033, Operational
            P5849D5AAPL076, Operational
Devices: c40t0d0
TGT/LUN   Device WWLUN_ID                               #_Paths H/W path
0/ 0     c40t0d0 6005-08B4-0001-2DB3-0000-D000-03AC-0000 4255/255/0/0.0

          Controller Path_Instance   HBA      Preferred? Path_Status
          P5849D5AAPL033
          c47t0d1       fcd0     no        Active
          c43t0d1       fcd1     no        Available

          Controller Path_Instance   HBA      Preferred? Path_Status
          P5849D5AAPL076
          c45t0d1       fcd0     no        Standby
          c41t0d1       fcd1     no        Standby
```

 **NOTE:**

c40t0d0 is the virtual path for physical path instances c47t0d1, c43t0d1, c45t0d1, and c41t0d1 through different controllers.

Device path representation of Secure Path for Active-Active disk arrays

Secure Path for Active-Active disk array uses the real physical paths to an end device. The alternate paths are presented via actual device files as seen by HP-UX and you can view and access these paths.

Example:

```
#autopath display
=====
HPswsp Version      : A.3.0F.01F.00F
=====
Auto Discover       : ON
=====
Array Type         : XP
Array WWN          : 2747
```

```

=====
Lun WWN                : 50_0-2747-0121
Load Balancing Policy : No Load Balancing
Lun Timeout            : Infinite Retry (-1)
=====
Device Path            Status
=====
/dev/dsk/c30t0d0      Active
/dev/dsk/c35t0d0      Active
/dev/dsk/c37t0d0      Active
/dev/dsk/c39t0d0      Active
/dev/dsk/c41t0d0      Active
/dev/dsk/c43t0d0      Active
/dev/dsk/c45t0d0      Active
/dev/dsk/c47t0d0      Active

```



NOTE:

You can use any of the alternate device paths to an end device, as there is no alias device concept.

Differences between Secure Path for Active-Active disk arrays and LVM PVLINKS

This section provides information about Secure Path for Active-Active disk arrays with LVM and LVM PVLINKS, including:

- [Secure Path for Active-Active disk arrays with LVM](#)
- [Secure Path for Active-Active disk arrays with LVM PVLINKS](#)

Secure Path for Active-Active disk arrays with LVM

For a device configured under LVM, if the LVM primary path fails, then Secure Path failovers to an alternate path and continues the Input/Output (I/O) till the primary path gets restored. Once the primary path is restored, the I/O resumes on the primary path of LVM.

Secure Path for Active-Active disk arrays with LVM PVLINKS

Secure Path takes control of the device configured under LVM with PVLINKS for alternate paths, and overrides LVM PVLINKS to provide automatic I/O path failover and fail back functionality. LVM PVLINKS provides alternate path for the device during system reboot.

HP recommends

HP recommends that you specify the physical volume paths while configuring LVM with PVLINKS and using LVM PVLINKS with Secure Path for Active-Active disk arrays. The physical paths for the alternate paths are a combination of paths that emerge from different HBAs, pass through different switches, and map to different controller ports on the disk array.

This configuration allows:

- Secure Path to provide high availability and load balancing to the volume group when the system is up and running.
- LVM PVLINKS to provide high availability if the LVM primary path has failed during system boot.

The following example displays the list of devices managed by Secure Path, after Secure Path is installed.

```

# autopath discover
# autopath display

```

```

=====
HPswsp Version      : A.3.0F.01F.00F
=====
Auto Discover       : ON
=====
Array Type          : XP
Array WWN           : 2747
=====
Lun WWN             : 50_0-2747-0121
Load Balancing Policy : No Load Balancing
Lun Timeout         : Infinite Retry (-1)
=====
Device Path          Status
=====
/dev/dsk/c30t0d0    Active
/dev/dsk/c35t0d0    Active
/dev/dsk/c37t0d0    Active
/dev/dsk/c39t0d0    Active
/dev/dsk/c41t0d0    Active
/dev/dsk/c43t0d0    Active
/dev/dsk/c45t0d0    Active
/dev/dsk/c47t0d0    Active
=====

```

The following example displays how to set load balancing policy for all the devices managed by Secure Path:

```
# autopath set_lbpolicy < {policy name} {path} >
```

Policy name: The load balancing policy to set. Valid policies are

```

RR      : Round Robin.
SST     : Shortest Service Time.
SQL     : Shortest Queue Length.
NLB/OFF : No load balancing.

```

Path: Device Special File e.g./dev/dsk/c#t#d#

Example: `autopath set_lbpolicy RR /dev/dsk/c30t0d1`

The following example displays how to configure PVLINKS using the `vgextend` command:

```

vgextend - extend an LVM volume group by adding physical volumes
SYNOPSIS
  /usr/sbin/vgextend [-f] [-A autobackup] [-g pvg_name]
                    [-x extensibility] [-z sparepv] vg_name pv_path ...

```

The following example displays how to add physical volumes `/dev/dsk/c0t1d0` and `/dev/dsk/c0t2d0` to volume group `/dev/vg03`:

```
#vgextend /dev/vg03 /dev/dsk/c0t1d0 /dev/dsk/c0t2d0
```

 **NOTE:**

You can determine the alternate paths `/dev/dsk/c0t1d0` and `/dev/dsk/c0t2d0` for `vg03` using the `autopath display` command.
