release notes

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

Product Version: 3.0F

Fourth Edition (April 2005)

Part Number: T3549–96401

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

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.

Printed in the U.S.

Secure Path 3.0F for HP-UX 11.00 and HP-UX 11.00 Workgroup Edition release notes
Fourth Edition (April 2005)
Part Number: T3549–96401

About this document

This section describes the content reflected in this document, including:

Intended audience

This document is intended for customers who purchased the HP StorageWorks Secure Path 3.0F for HP-UX V11.00 and are responsible for installing, configuring and maintaining this product in their HP-UX server environment.

Secure Path 3.0F kit contents

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

- *Secure Path 3.0F for HP-UX 11.00 readme.txt* document (CD-ROM only).
- *HP StorageWorks Secure Path 3.0F for HP-UX 11.00 and HP-UX 11.00 Workgroup Edition Installation and Reference Guide*, part number AA-RV17C-TE.
- Secure Path 3.0F for HP-UX 11.00 CD-ROM.

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

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

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

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

Additional documentation is available via the HP web site at http://www.hp.com.

Secure Path 3.0F for active-passive disk arrays

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

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

- The Path polling threads that were getting inadvertently terminated, during parallel execution of ioscan and `spmgr delete` command is now fixed.
- The I/O errors in all paths failed condition during I/O to a non-LVM HFS lun is now resolved.
- The device special file name in the message that is logged into syslog when all the paths to a LUN fails, is fixed. Now, the device special file name corresponds to the lun and not to the path for that device.
- Losing path verification period and deleted LUN information during the upgradation 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 earlier version of Secure Path 3.0E to 3.0E, is now fixed
- The issue related to failback resulting a new CTD for the same WWLN has been resolved. Now, the host displays the same C T D when failback happens.
- The installation failure issue when multiple paths exist in your local disk, has been fixed.
- The `spmgr delete` command used to cause core dump when any Secure Path communication issues occurred. This problem has been fixed and now the system displays an appropriate error message when any issue occurs.
- The issue in retriving the verification interval after upgrading from 3.0BSP1 to later versions, has been resolved.
- Moving of LUNs to discovered list from unattached list after upgrade has been fixed.
- When you replace an array controller online, the `spmgr display` command used to display the previous controller's ID till the system is rebooted. This problem has been resolved, and now the controller IDs are updated to reflect the new controller's ID without a system reboot. (Enable the proactive path polling while doing the controller replacement).
- The memory leak issue while the event or mail notification is enabled in `spagent` has been fixed.

- The `spagent` core dump caused by un-handled exception has been fixed.

Changes in this release of Secure Path include the following:

- A new LUN gets added as a new C T D on LUN collision.

Operating system support

Table 1 lists the features and requirements of HP Secure Path 3.0F for HP-UX. For additional support information, check the HP web site: http://www.hp.com/support.

Table 1: Secure Path 3.0F for HP-UX 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)
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 1: Secure Path 3.0F for HP-UX requirements (Continued)

Controllers	Dual HSG80 controllers operating ACS V8.6F or later Dual HSG60 controllers operating ACS V8.6L 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 and Arbitrated Loop

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

Table 2: Secure Path 3.0F for Hsx supported devices and drivers

HP-UX version	HBAs	Supported storage arrays	Minimum driver revision
11.0	A5158A A6795A A6685A	RA8000/ESA12000 (HSG80) MA8000/EMA12000 (HSG80) MA6000 (HSG60) EMA16000 (HSG80) EVA5000 (HSV110)	Fibre Channel B.11.00.10

Table 3 lists patch revisions.

Table 3: Patch revisions

HP-UX version	Patch revisions (minimum)
11.00	Hardware Enablement Bundle March 2004—HWE1100 B.11.00.0404.5 Quality Pack Bundle Sept 2003 QPK1100 B.11.00.62.4 Support Tools Bundle Sept 2003 - Online Diag B.11.00.26.07 Kernel Patch (asyncio)–PHKL_30709–async disk driver, only required if running databases using raw (nonfile system) data access. **NOTE:** The asyncio patch number (formerly PHKL_27759) has been updated to PHKL_30709. PHCO_29765 umount (1M) cumulative PHCO_27514 mountall (1M) cumulative PHCO_27515 umountall (1M) cumulative–Device IDs Enablement PHCO_27516 fsclean (1M) Device IDs Enablement PHCO_29769 umount (1M) cumulative

Table 4 shows configuration limitations.

Table 4: Configuration limitations

Parameter	Minimum	Max Qualified	Max Supported
Adapter Support	Single HBA	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.

General

- 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 the `spagent` utility using the `spinit stop` command and then starting the `spagent` utility using the `spinit start` command results in `stderr` messages. To keep messages from being printed, 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, take care to avoid misconfiguring 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, snapshots or clones appear to LVM to be an alternate path to the original physical volume. This misconfiguation could lead to data corruption if the snapshot or clone were later added to the volume group by means of `vgextend(1M)`, `vgimport(1M)`, or `vgscan(1M)`.

LUN Collision

If a device is unpresented 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 operation 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 the 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 unpresenting the device.

High-availability EVA environment recommendations

In high-availability environments, under heavy I/O loads, you may experience I/O time-out conditions. If I/O timeouts occur, HP recommends that you increase the `IO_timeout` value with the `pvchange` command 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.vent monitoring service

---

EVA

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

HSG80 controller

EMS logs erroneous HSG80 LUN errors due to an incompatibility issue between EMS and the HSG80 controllers. At the time of these EMS notifications, 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 messages by disabling the EMS monitoring of HSG80 devices. Use the procedure “Disabling hardware monitoring” on page 11 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` 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. In addition, 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/lbin/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 be displayed in the list, with no monitoring requests.

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 run any Secure Path commands until the Secure Path start-up services are run.
- 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.
- For 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 is no critical message that a failure has occurred or a different path has been selected. This is due to the restart taking less time than required to validate a path failure.
- The rolling upgrade method, that upgrades ACS V8.6 to ACS V8.7 and is described in the *Maintenance and Service Guide of the Solution Software V8.7 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 unpresented 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 60001FE1000FE860000910507123000 9 on array 50001FE1000FE860.
```

The message indicates the missing target/LUN number for the device and not a problem with the configuration. The message repeats for any subsequent `ioscan` and ceases after the kernel rebuild/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 `spmgr select` and `spmgr restore` 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 are also 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.

- 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 `ioscan`.

- 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 `fcparray` (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.

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#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 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. 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 set` command is available to set the Load Balance Policy.
- 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.
- This version of Secure Path for active-active disk array supports upto 32 paths to a LUN.
- 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 `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 shows the system features and requirements for Secure Path 3.0F for active-active disk arrays. For more information about supported features, check the HP website: http://hp.com/support.

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

1. 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 Secure Path, for these arrays.

Table 8 lists the supported devices and the driver requirements for this release, and earlier releases.

Table 8: Secure Path 3.0F for active-active disk arrays supported devices and drivers

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

Table 9 lists patch revisions.

Table 9: Patch revisions

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 shows configuration limitations for this version.

Table 10: Configuration limitations

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 starts only if the original path (on which IO was started) is restored. It does not start if any of the alternate paths is restored.
- 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 (`?`) with a command to display help for the command.
- If `HPswsp` is marked for uninstallation using `swremove` and if uninstallation is aborted, Load Balance Policy settings defaults back to `NLB`.
- Secure Path 3.0F for active-active disk arrays does not support assigning the `scsi` LUN ID (different from `WWLUN` ID) of an unpresented LUN to another LUN. Running the `autopath discover` command in such a scenario may put the system in a highly inconsistent state.

Secure Path 3.0F for Workgroup Edition 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 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 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 `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 11 shows the system features and requirements for Secure Path 3.0F Workgroup Edition for VA arrays.

For more information about system support, check the HP web site: http://hp.com/support.

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

System feature	Requirement
Operating system versions	HP-UX 11.00 64 bit only
HP-UX server system types	rp54xx (L-class) rp74xx (N-class) K-class
File systems	HFs (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 the driver requirements for this release, and earlier releases.

Table 12: Secure Path 3.0F Workgroup Edition devices and drivers

HP-UX version	HBAs	Supported storage arrays	Minimum driver revision
11.0	A5158A, A6795A, A6685A	VA 7400 VA 7410 VA 7100 VA 7110	Fibre Channel B.11.00.10

Table 13 lists patch revisions.

Table 13: Patch revisions

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 shows configuration limitations.

Table 14: Configuration limitations

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 starts only if the original path (on which IO was started) is restored. It does not start if any of the alternate paths is restored.

- 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 VA disk array does not support devices configured under Veritas Volume Manager.
- Secure Path 3.0F for Workgroup VA disk arrays does not support wild card characters. For example, you cannot use the question mark (`?`) with a command to display help for the command.
- If `HPswsp` is marked for uninstallation using `swremove` and if uninstallation is aborted, Load Balance Policy settings defaults back to `NLB`.
- Secure Path 3.0F for Workgroup Edition VA disk arrays does not support assigning the `scsi` LUN ID (different from `WWLUN` ID) of an unpresented LUN to another LUN. Running the `autopath discover` command in such a scenario may put the system in a highly inconsistent state.