hp surestore secure manager virtual array

Installation and User's Guide

Version 1.00

Edition July 2001
Order No. T1003-90903
Printed in U.S.A.

Notice

Safety Instructions

	Denotes:
WARNING	**A hazard that can cause personal injury**
Caution	A hazard that can cause hardware or software damage

Format Conventions

	Denotes
Note	Significant concepts or operating instructions
`this font`	Text to be typed verbatim: all commands, path names, file names, and directory names
`this font`	Text displayed on the screen
<*this font*>	Variables used in commands

Trademark Information

Red Hat is a registred trademark of Red Hat Co.

C.A. UniCenter TNG is a registered trademark of Computer Associates Inernational, Inc.

Microsoft, Windows NT, and Windows 2000 are registered trademarks of Microsoft Corporation

HP, HP-UX are a registered trademarks of Hewlett-Packard Company.
Command View, Secure Manager, Business Copy, Auto Path, Smart Plug-Ins are trademarks of Hewlett-Packard Company

Adobe and Acrobat are trademarks of Adobe Systems Inc.

Java and Java Virtual Machine are trademarks of Sun Microsystems Inc.

AIX is a registered trademark of IBM Co.

NetWAre is a registered trademark of Novell Co.

Table of Contents

1 Product Description

2 Installing Upgrade Licenses

3 Using The Command Line User Interface

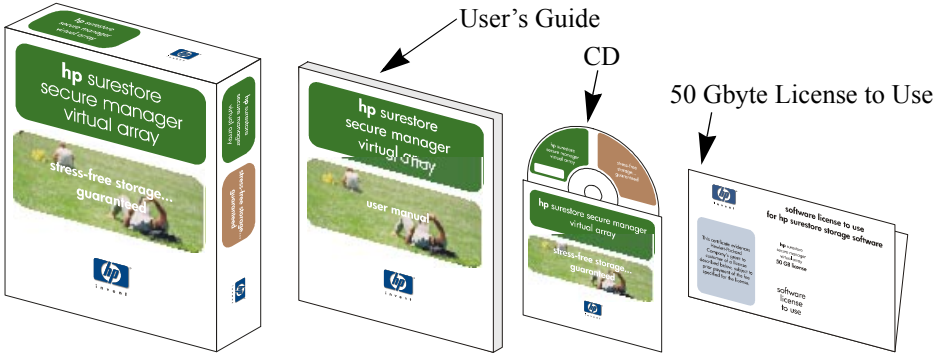
1 PRODUCT DESCRIPTION

Secure Manager VA Overview

Congratulations on your purchase of the HP Surestore Secure Manager Virtual Array product. This product allows you to create secure LUNs up to a maximum of 50 Gbytes of usable capacity (for up to 128 World Wide Names).

The contents of this product include:

- HP Surestore Secure Manager Virtual Array User's Guide
- Software CD
  - Secure Manager Installation & User Guide pdf (for Adobe Acrobat Reader V 3.0 or greater)
  - Secure Manager Virtual Array E-mail Template.txt (system specific file)
  - readme.txt
- License-to-Use (50 Gbyte)



Secure Manager Features

Secure Manager provides the following features:

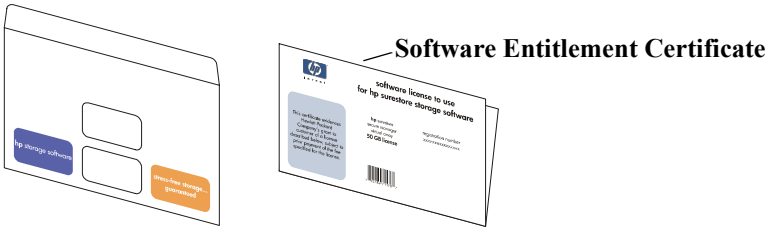
- Secure LUNs for up to 128 World Wide Names (WWN's)
- Ability to manage security from a Command Line User Interface (CLUI) or Graphical User Interface (GUI)

Secure Manager Upgrade Licenses

Secure Manager Upgrade Licenses provide additional capacity for the Secure Manager VA product. These upgrade licenses increase the capacity for LUN security up to either, 500 Gbytes or 1000 Gbytes, depending on the license purchased (refer to Table 1 on page 11). Prior to enabling a license, you need to complete the information on the Software Entitlement Certificate and return the information to HP. Upon receipt of the certificate information, HP will return a License Key. The License Key is used to enable the additional capacity (refer to Obtaining the License Key on page 16, for additional information).

The contents of the Upgrade License include:

- Software Enablement Certificate (for either a 500 Gbyte or 1000 Gbyte license)
- Storage envelope



IMPORTANT Keep the Software Entitlement Certificate you received, with this product, in a safe place. You will need the Registration Number on this certificate to obtain the software license key that is used to enable this products software feature.

This product is licensed to you according to the standard licensing terms defined on the “Software License Agreement”, located on the back of the Software Entitlement Certificate.

If you did not purchase a Secure Manager VA upgrade product, you can begin setting security using the 50 Gbyte, “demo” version, available with the product. For additional information on managing

security, refer to chapter 3, Using The Command Line User Interface. If you purchased an additional capacity upgrade, you must first install this upgrade before you begin setting security. For additional information on the License Key, refer to Obtaining the License Key on page 16.

Note If a capacity license is purchased for only a portion of the array's total capacity, additional capacity licenses can be purchased and added at a later date (refer to Upgrading Capacity on page 21).

HP Modular Storage Software Products

Several product options are available that enhance the operation of the Command View SDM software. These optional products are listed in Table 1 on page 11. For the most up-to-date product information, access the HP web site (refer to Web Support on page 13).

Table 1 Command View SDM Software Products

SOFTWARE PRODUCTS	HP SALES OFFICE	HP RESELLERS
Command View SDM: Storage device management enables array device configuration and management, and value-added software products. Software Package and 1 Host LTU*	T1001A	T1020A
Enterprise Management Smart Plug-Ins: Enables Command View SDM in HP Openview NNM for HP-UX, Windows 2000 and Windows NT 4.0. It also enables command view sdm for HP Top Tools, and CA-Unicenter TNG. Software Package and 1 Host LTU*	T1002A	T1021A
Business Copy Virtual Array: Enables online data replication or LUN copying within the array for testing and backup, and requires the same physical space to be available in the array as the LUN(s) being copied. Software Package and 50 GB LTU* 500 Gbyte Upgrade LTU 1000 Gbyte Upgrade LTU	T1007A T1008A T1009A	T1026A T1027A T1028A
Secure Manager Virtual Array: Enables LUNs to be locked into a secure shared environment. Software Package and 50 GB LTU* 500 Gbyte Upgrade LTU 1000 Gbyte Upgrade LTU	T1003A T1004A T1005A	T1022A T1023A T1024A
Auto Path Virtual Array for Win2K: Enables I/O path fail-over in MSCS Windows 2000 environments with the benefit of I/O load balancing in both failed and non-failed states. Software Package and 1 Host LTU* 1 Host Upgrade LTU 5 Host Upgrade LTU 10 Host Upgrade LTU 25 Host Upgrade LTU	T1011A T1012A T1013A T1014A T1015A	T1030A T1031A T1032A T1033A T1034A

* - License to Use

Requirements

This product is designed to operate with the HP Surestore Command View SDM software. The Command View SDM software must be installed and operating for this product to operate. Array security is managed using the command line user interface or the graphical interface provided with the Command View SDM software (as described later in this document).

Warranty Statement

This software package comes with a 90 day media defect warranty. If you have any problems with the quality of the CD or the supporting documentation, you may return it for exchange through any HP Sales Office or authorized HP reseller.

Technical Support

Technical support is provided for this product through an HP Support Contract, purchased at the time you purchased this product. For details regarding support information, refer to that contract.

For a list of the most current support phone numbers, access the following HP web site:

```
www.hp.com/support/smva
```

Web Support

New product offerings, product updates, support software, and options are continually becoming available. For the most current product information, access the HP web site. Two sites are available: one for general product information and one for technical support information (software updates, firmware updated, documentation, and more). To access this information, go to the HP home page, and follow the pages indicated to the specific information you need:

www.hp.com

For general product offerings and product information, follow these links:
(The bold "support" identifies a web page; "➞" represents a link to be selected, on a page.)

➞ products & services
products and services
➞ disks, disk arrays - storage
disks, disk arrays
then either:
➞ hp modular storage software **(for software product information)**
OR,
➞ midrange arrays
mid-range arrays
➞ hp surestore VA 7100 **(for hardware product information)**

For technical support information, follow these links:

➞ support
support
➞ disks, disk arrays
hp disk & disk arrays
then either:
➞ hp disk arrays
hp disk arrays
➞ hp surestore VA7100 (**for hardware support information**)
OR:
➞ hp modular storage software (**for software support information**)

From these pages, you can find additional information pages about the software and related products.

Note Additional information is available on the readme file provided on the product CD-ROM.

2 INSTALLING UPGRADE LICENSES

Overview

This chapter describes how to install Upgrade Licenses, purchased for Secure Manager VA product. Installation involves obtaining a License Key from HP before the capacity upgrade can be installed, and installing the key.

Note It is important that you keep your Registration Number, identified on the Software Entitlement Product, in a secure place until you redeem it for the License Key.

License Key

An Upgrade License is enabled using a License Key. The License Key, issued by HP (as described later), is based on the entitlement certificate **Registration Number** and an array's **serial number**. Also, the following items should be noted regarding the License Key:

- **The License Key must be installed on the array with the serial number that matches the one used to obtain the License Key.**
- Once the license is obtained, it cannot be transferred.
- Once a license is installed in the array, it cannot be removed.

Obtaining the License Key

Before you can use the additional capacity provided by the Upgrade License, you must obtain a License Key. To obtain this key you will need to complete the information on the Software Entitlement Certificate, in the software Upgrade License envelope, and communicate it to HP. HP will use the information to generate a License Key and return it to you. You must then install the License Key to enable the additional capacity.

To obtain the License Key, fill out the Software Entitlement Certificate (or at least have all the information requested available). The two primary items required for obtaining the License Key are the:

- Registration Number (located on the Software Entitlement Certificate)
- Serial Number - of the array that the License will be installed on (see note on previous page) . It is important to verify the serial number using the HP Command View SDM software (such as the graphical interface **Identity** page (refer to Appendix A for information on identifying the array's serial number.)

Note

When identifying the serial number, it is important to verify it using the Command View SDM software, as described in Appendix A.

When entering or communicating the serial number:

- The serial number letters are case sensitive: if they are upper case they must be entered as upper case; if they are lower case they must be entered as lower case letters.
- The serial number must be 12 characters, for example: 00XY00000000.

Next, communicate this information to HP. Four communication methods are available: World Wide Web, phone, Fax, or E-mail. Information for the specific communication methods is listed below (this information is also listed on the Software Entitlement Certificate).

	US & Canada 6:00 am-6:00 pm U.S. MST, M-F	Europe 9:00am-6:00pm Netherlands local time, M-F	Asian 9:00am-5:00pm Japan local time, M-F
World Wide Web	www.webkey.external.hp.com		
Call the HP Authorization Center	(801) 431-1451 (800) 861-2979	+31-555-384-210	+81-03 -3227-5289 +81-3 -3227-5289 (outside Japan)
Fax the Completed Form	(800) 431-3654	+31-555-434-645	+81-03 -3227-5289 +81-3 -3227-5289 (outside Japan)
E-mail*	Americas_password@cnd.hp.com	Europe_password@cnd.hp.com	Asia_password@cnd.hp.com

If you are e-mailing your information, use the e-mail template form located on the software CD.

Note The Feature Description and the License Key entries on the Software Entitlement Certificate are blank. You should fill them in when HP returns these values to you. If you are registering multiple products, please use the secure manager email template (located on the installation CD-ROM). Using the template makes it easier to enter and send the information.

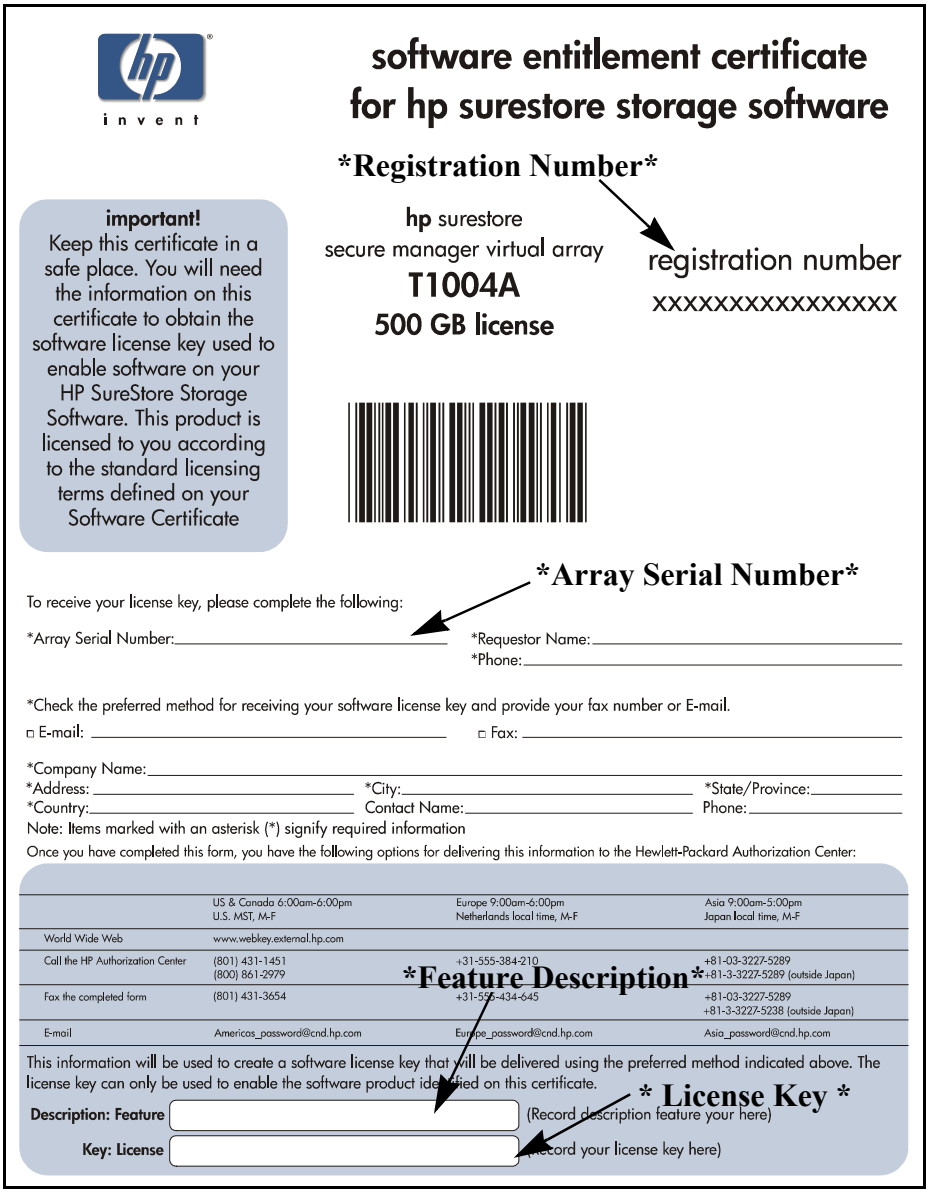


Figure 1 Software Entitlement Certificate

Installing the License

Once you have completed the Software Entitlement Certificate, communicated the information to HP, and received your License Key, you must install the key into the array to enable the feature capacity. The key is installed using the armfeature command, as described below.

Note Once the license key is obtained, it cannot be transferred; once it is installed in an array, it cannot be removed.

To install the license, complete the following steps:

1. Identify the array's ID (<*array-id*>), it can be an: alias name, serial number, device path, or world wide name (for information on identifying the serial number, refer to Appendix A).
2. Identify the installed features of the array using the armfeature command with the -r option (armfeature -r <array-id>). Enter, for example:

   ```
   armfeature -r 00XY00000000
   ```

   This example uses a **sample** serial number (00XY00000000) for the <array-id>. When using the serial number, it must consist of 12 digits, plus, the letters must be entered in the proper case (upper vs. lower). Use the Command View SDM software graphical user interface to identify the serial number, again, refer to Appendix A. For additional information about the armfeature command, refer to Appendix B.
3. Now, download the License Key to the array.

   From the command line, enter the armfeature command with the -a option (armfeature –a –f <*featurestring*> -k <*key*> <*array-id*>). The feature description (<*featurestring*>), from your Software Entitlement Certificate, and the License Key, returned to you from HP, are entered in this command.

   For example, to enter the license for a 500 Gbyte capacity upgrade, with a License Key (<*key*>) of "`XXX000X000X00`", for an array with the serial number "`00XY00000000`", enter:

   ```
   armfeature -a -f LUN_SECURITY_500GB -k XXX000X000X00 00XY00000000
   ```

Note The capacity license **must** be installed on the array with the serial number that matches the serial number used to request the feature (the serial number entered on the Software Entitlement Certificate).

Also, when entering the serial number, the letters ("SG" in the example above) are case sensitive, that is: if they are upper case, they must be entered as upper case; if they are lower case then they must be entered as lower case letters.

Once this command has completed, a list of installed features will be displayed. If the feature is successfully installed, it will be displayed in the list as "Enabled" (as shown below); if it was not installed, it will be displayed as "Disabled" or will not appear in the list at all.

```
  FEATURE                    KEY                    STATE
================================================================
LUN_SECURITY_500GB        XXX000X000X00         Enabled
```

Once the installation is successful, you will be able to create secure LUNs for, up to, the capacity of the license. For example, if you installed a 500 Gbyte license, you will be able to assign security for 10, 50 Gbyte LUNs; two 250 Gbyte LUNs; or, any number of LUNs (up to 63) for which the total capacity does not exceed 500 Gbytes. If the array has a total of one Tbyte of storage, you would not be able to create secure LUNs for the additional 500 Gbytes.

Note Any number of LUNs can be assigned security as long as the total capacity of the secure LUNs does not exceed the license capacity. If an attempt is made to add security to a LUN that would cause the total capacity to exceed the license capacity, that LUN will not be assigned security; all hosts will have access to that LUN.

If the Installation Fails

If the installation fails, check the following:

- Verify that the Feature Description and the License Key entered in the command are correct.
- Verify that the license is being installed on the array with the serial number that matches the serial number provided to HP to obtain the License Key.
- Verify that the serial number is 12 digits, for example “00XY00000000”.
- Verify that the case of the serial number and License Key letters is correct.

Upgrading Capacity

Capacity Upgrade Licenses can be installed at any time. If you initially installed a license that did not cover the entire capacity of the array; or, if you have increased the array’s storage capacity beyond the original license, you can add additional capacity licenses, as needed.

The process for adding capacity is identical to the process for obtaining and installing the first license (refer to Installing Upgrade Licenses on page 15).

Note When additional capacity is purchased for an array and, the Software Entitlement Certificate information is returned to HP, a new License Key will be returned along with a new feature description. The new feature description will identify the sum of your new license request plus, all previous installed license capacities. For example if you purchased a “LUN_SECURITY_500GB” capacity license, then later you purchased another license for 500 Gbytes for the same array (same serial number), HP would return a License Key with a new feature description of “LUN_SECURITY_1000GB”.

3 USING THE COMMAND LINE USER INTERFACE

Overview

This chapter describes procedures for managing security using the CLUI armsecure command. These procedures include creating and setting permissions, viewing installed permissions, changing permissions, clear security table, changing password and enabling and disabling array security. All security management operations can be performed from the command line (using the armsecure command). It is also possible to perform some security operations using the graphical user interface, however, the GUI has very limited security management features (for information on the graphical user interface management operations, refer to chapter 4, Using the Graphical User Interface).

Array Security Table

The array identifies the permission a host will have for a specific LUN using a security table which is maintained in the array's internal memory. Entries in this table are of two types: Secure or Generic.

Secure entries contain a World Wide Name (WWN) to identify a specific host (principal type), a LUN, and a permission of W (read/write). Generic entries use DEFAULT to identify all hosts (principal type), a LUN, and, a permission that the specified host will have for that LUN. (Permissions are described in more detail in the section Creating the Permissions file on page 26.) A representation of the array security table is shown in Table 2 on page 25.

The array uses the World Wide Name (WWN) to identify a host. For security, the array will support a maximum of 128 World Wide Names (WWNs). If an attempt is made to add security for a WWN that exceeds 128 the error "LUN number greater than the maximum supported" will be displayed.

A representation of the array's security table is shown in the example below (note that entries 1, 2, 7, 12, and 17 are generic and all others are secure.) Entries in this table identify security support for three hosts (A, B, and C) and five LUNs (0 through 4).

Note that host A has two HBAs with WWNs: WWN1 and WWN2. Host B and C each have a single HBA with WWNs WWN3 and WWN4 respectively. Since host A has two paths to the array (through its two HBAs) both HBAs must be included in the Security table. In addition, both HBAs for the host A must be assigned identical permission for each LUN the host supports.

Table 2 Array Security Table

Line	Principal_Type	LUN #	Permission	Comments
1	DEFAULT	LUN 0	None	All Hosts have access to LUN 0 (This is the default for LUN 0)
2	DEFAULT	LUN 1	None	All Hosts have access to LUN 1 (This is the default for LUN 1)
3	WWN1	LUN 1	Config	Host-A with two HBAs (HBA - WWN1)
4	WWN2	LUN 1	Config	Host-A with two HBAs (HBA - WWN2)
5	WWN3	LUN 1	None	Host-B
6	WWN4	LUN 1	None	Host-C
7	DEFAULT	LUN2	None	All Hosts have access to LUN 0 (This is the default for LUN 2)
8	WWN1	LUN 2	Write	Host-A with two HBAs (HBA - WWN1)
9	WWN2	LUN 2	Write	Host-A with two HBAs (HBA - WWN2)
10	WWN3	LUN 2	Config	Host-B
11	WWN4	LUN 2	None	Host-C
12	DEFAULT	LUN3	None	All Hosts have access to LUN 0 (This is the default for LUN 3)
13	WWN1	LUN 3	None	Host-A with two HBAs (HBA - WWN1)
14	WWN2	LUN 3	None	Host-A with two HBAs (HBA - WWN2)
15	WWN3	LUN 3	Write	Host-B
16	WWN4	LUN 3	Config/Write	Host-C
17	DEFAULT	LUN4	None	All Hosts have access to LUN 0 (This is the default for LUN 4)
18	WWN1	LUN 4	Write	Host-A with two HBAs (HBA - WWN1)
19	WWN2	LUN 4	Write	Host-A with two HBAs (HBA - WWN1)
20	WWN3	LUN 4	Write	Host-B
21	WWN4	LUN 4	Config/Write	Host-C

For additional information on the features discussed here, refer to Creating the Permissions file on page 26.

Security can be enabled or disabled (as described under Enabling/Disabling Security on page 33). If security is disabled, all hosts have access to all LUNs with all permissions. If security is enabled, the

settings in the array security table will be in effect. If security is enabled, it is important to have one LUN with Config (C) or Config/Write (CW) permission to be able to perform management operations.

Assigning Security

The process for assigning security involves two steps. The first step is the creation of a permissions file which identifies the host permissions for each LUN. The second step is downloading this file to the array. These procedures are described below.

Creating the Permissions file

The permissions file is an ASCII text file created by the system administrator that contains one or more text lines. Each line in the file identifies a permission. A permission specifies the level of access a host or WWN will be allowed for a LUN. Thus, each line in the file must specify a World Wide Name (WWN) and an associated LUN plus the permission level (one additional entry is required as defined below). When downloaded to the array, these lines become entries in the array's security table.

The format for a line in this file is:

<Participant Type> <Node WWN> <LUN-ID> <Permissions>

(Note there must be a space between each field.)

Where:

<Participant Type> is either: DEFAULT or NODEWWN.

DEFAULT - specifies that the permission for the LUN is for all WWNs.
NODEWWN - specifies that the permission for the LUN is for one WWN.

<Node WWN> is the World Wide Name for which the permission is being set.
If DEFAULT is specified for *<Participant Type>* then *<Node WWN>* must be a character, such as "-" (it can be any character, except blank spaces).

<LUN-ID> is the number of the LUN for which permissions are being set.

<Permissions> can be any one of the following values:

W - Enables Write permission: this permission allows the specified host (WWN) to perform reads and writes to the specified LUN.

C - Enables Config permission: this permission allows the specified host (WWN) to perform array management commands (such as Create LUN and Delete LUN and more) to **all** LUNs in the array. It does not give the host Write (read and write) permission to the LUN.

0 - Zero -No permission: No information about the specified LUN is available to the specified host (WWN).

CW - Enables Config/Write permission: this permission allows the specified host (WWN) to perform array management commands (such as Create LUN and Delete LUN and more) to **all** LUNs in the array, plus gives the host Write (read and write) permission to all LUNs.

Example: Permissions File

When LUN 0 is created, the default permissions (access) should be WC to allow the command view sdm software access to the LUN. The following example sets up four LUNs (0-3):

```
DEFAULT null 0 WC
DEFAULT null 1 W
DEFAULT null 2 W
DEFAULT null 3 W
```

To modify the LUN Security Table for security, the Node WWN of the hosts that are allowed access need to be added to the LUN Security Table. The following example updates the previous table to add security:

```
NODEWWN 50060b0000017ee0 1 W
NODEWWN 50060b00000158f8 2 W
NODEWWN 50060b0000006964 3 W
DEFAULT null 0 WC
DEFAULT null 1 0
DEFAULT null 2 0
DEFAULT null 3 0
```

Once the entries are made to the file, save the file. Next the file must be downloaded to the array to set the permissions, as described in the following section.

Example: Permissions File - Adding a New LUN and Adding Permissions

When a new LUN is added, the permissions are automatically set to W. The following example adds LUN 4 to the previous example:

```
NODEWWN 50060b0000017ee0 1 W
NODEWWN 50060b00000158f8 2 W
NODEWWN 50060b0000006964 3 W
DEFAULT null 0 WC
DEFAULT null 1 0
DEFAULT null 2 0
DEFAULT null 3 0
DEFAULT null 4 W
```

To add security on the new LUN, you need to change the permissions to zero (0) and update the table with the NODEWWN of the hosts that will access the LUN. The following adds security to the previously added LUN.

```
NODEWWN 50060b0000017ee0 1 W
NODEWWN 50060b00000158f8 2 W
NODEWWN 50060b0000006964 3 W
NODEWWN 50060b0000007538 4 W
DEFAULT null 0 WC
DEFAULT null 1 0
DEFAULT null 2 0
DEFAULT null 3 0
DEFAULT null 4 0
```

Viewing LUN Permissions

It is important when assigning permissions to identify what entries are already assigned in the array's security table. To identify the permissions, you can read the table from the array, write it to a file, and then view it using a text editor. The table is read from the array and written to a file using the armsecure command with the –r option (armsecure –r –f <filename> –p <*password*> <*array-id*>, for additional information about this command refer to armsecure Command on page 49).

The following example shows how to view the security table. This example assumes the security table will be read from an array with the alias of "xyzArray", and saved to the file "secureTbl.txt". A password "myPassWd" has been previously assigned and must be used.

Note The array's default password is "AUTORAID". If this password has not been changed, this password must be used, otherwise use the assigned password. If this password has not been changed, it should be changed as soon as possible to prevent unwanted access violations (refer to Changing the Security Password on page 34).

To view the array's permissions, perform the following steps:

1. Read the security table from the array, for example, enter:

```
armsecure –r –f /arraySecurity/dev/secureTbl.txt –p myPassWd xyzArray
```

Note If a path is not included as part of the -f <*filename*> when using the armsecure -r (read) or -w (write) options, the file will be placed in the path specified by the user at the time of Command View SDM software installation. If a path is was not specified during installation or is not included with the -f <*filename*>, the file will be located in the default directory:

`/opt/sanmgr/client/sbin/<filename>` for HP-UX and Linux
`C:\sanmgr\client\sbin\<filename>` for Windows

2. View `secureTbl.txt` using a text editor (such as, Word or Word Pad for Windows, or vi for HP-UX).

Setting Security Permissions

To set permissions, the permissions file must be downloaded to the array. Two basic methods that can be used. One method is to clear the array security table and download an entire new file (security table); the second method is to maintain and modify the array security table, downloading a file which contains only the lines which require modification.

These two procedures are described below.

Note Some examples include a path with the file name. The examples show only one path, using either Windows path separators "\" or UNIX -Linux separators "/". You need to use the correct file separator for your operating system.

Downloading New Security Permission

Downloading a new permission file to the array requires that a permissions file be created with all entries needed for all host/LUN combinations. Prior to creating the file, it is advisable to view the current security table to identify the current entries in the table. This file might be used as the basis for the new permissions file. When downloading a new file to the array, the array security table should be cleared, as described in the steps below.

The following example provides the steps for downloading a new security file to the array's security table.

1. View the security table permissions (for information on viewing an array security table, refer to Viewing LUN Permissions on page 30).
2. Create a new permissions file (for information on creating a permissions file, refer to Creating the Permissions file on page 26).
3. Download the file, "securityFile.txt" for example, to the array and clear the existing security table, using the armsecure command with the -w and -c options:

   ```
   armsecure –w –c –f /devSecurity/dev/securityFile.txt –p pwsecret xyzArray
   ```

   Where the path and <filename> of the permissions file is "/devSecurity/dev/securityFile.txt" and the <*password*> is "pwsecret" using an alias of "xyzArray" for the <array-id>.

Note When the armsecure command is used with the -c option, to clear the array security table, the array automatically disables security.

4. Enable security using the armsecure command with the -e option:

   ```
   armsecure –e –p pwsecret xyzArray
   ```

Modifying Existing Security Permissions

The entries in the array's security table can be modified by creating and downloading a permissions file that contains only the entries used to modify the existing table. This method is similar to the Downloading New Security Permission described above, except that the armsecure command is used without the -c option (leave the security table in the array).

When a line from a file is written to the security table, it will either be added as a new line or overwrite an existing line, depending on whether or not a WWN/ LUN# entry exists. If the download file contains a WWN/ LUN# combination that matches one in the table, the table entry will be overwritten; if the WWN/ LUN# combination does not exist, a new line will be added to the table.

The following example provides the steps for downloading a permission file to the array's security table that will either overwrite existing lines or add new line entries.

1. View existing security table permissions (refer to Viewing LUN Permissions on page 30).
2. Create a new permissions file, adding only the WWN/ LUN# entries that need to be added or modified in the array's security table (refer to Creating the Permissions file on page 26).
3. Download the file "securityFile2.txt" to the array, using the armsecure command with the -w option:

   ```
   armsecure –w –f /devSecurity/dev/securityFile2.txt –p pwsecret xyzArray
   ```

   Where the path and <filename> of the permissions file is "/devSecurity/dev/securityFile2.txt" and the <*password*> is "pwsecret" using an alias of "xyzArray" for the <array-id>.

Copying LUN Permissions

This procedure describes how to duplicate the permissions of an existing LUN, by copying them to a new LUN just created.

1. Read the security table from the array to a file (refer to Viewing LUN Permissions on page 30).
2. Open the file using a text editor.
3. Create the entries for the new LUN that match the existing LUN. Basically duplicate, or copy, the lines in the security file for the existing LUN to the end of the file. Then, change the LUN number for each entry just copied to that of the new LUN.
4. Delete the DEFAULT entry in the security file for the new LUN (this entry is automatically added for a new LUN when it is created).
5. Download the file to the array using the armsecure command (refer to Setting Security Permissions on page 31).

Enabling/Disabling Security

Security for the array can be enabled or disabled. If security is disabled, all hosts have all permissions for all LUNs; if security is enabled then the permissions in the array's security table are in effect. The factory default setting for security is disabled.

Security is enabled or disabled using the armsecure command with the –e or –d option (armsecure –d/–e –p *<password>* *<array-id>*, for additional information about this command refer to armsecure Command on page 49).

Note Security will be automatically disabled when using the armsecure command with the -c option (clear the array security table).

This following example uses a password "abcxyz" and the serial number "00XY00000000" for the array's ID.

For example, to enable security, enter:

```
armsecure –e –p abcxyz 00XY00000000
```

For example, to disable security, enter:

```
armsecure –d –p abcxyz 00XY00000000
```

Changing the Security Password

To ensure that the permissions are protected, a password is assigned to the armsecure command operation. This password is required to run the command. If the password is not included you will be prompted for it.

The password must be from one to eight characters. Any printing character is legal, however, it is best to avoid blanks and other special characters. Initially, the factory default password is “AUTORAID”. When the array is first brought on line, this password should be set to a new password.

The array’s security password is changed using the armsecure command (armsecure –n <newPassword> -p <oldpassword> <array-id>, for additional information about this command refer to armsecure Command on page 49). For example, to change the password from “AUTORAID” to “drowssap”, for any array with an alias of “xyzArray”, enter the following command:

```
armsecure -n drowssap -p AUTORAID xyzArray
```

No response is given for a successful completion of this command.

Note If you have forgotten the security password, and cannot access the security command, the password can be reset. To reset the password, refer to chapter 5, Resetting the Password on page 41.

4 USING THE GRAPHICAL USER INTERFACE

Overview

Some array security functions can be performed using the Command View SDM graphical user interface (GUI). However, the GUI is limited to enabling or disabling security and copying previously created permissions of one LUN to another LUN. These operations are described in this chapter. For additional information on the operation of the graphical interface, refer to the GUI on-line help.

If you need to perform all the security management functions, you must use the command line user interface (for more information on using the command line user interface for management operations, refer to chapter 3).

Enabling and Disabling Array Security

Overall security of the array can be enabled or disabled using the GUI. To perform this operation requires the password. (All descriptions in this document assume the GUI is running. For additional information on the GUI, refer to the Command View SDM software, Installation and User Guide, chapter 2 and 3, for information on starting and operating the GUI).

To enable or disable security, then, perform the following steps:

Caution When security for the array is disabled, any host can write to or delete any LUN.

1. Click the **Configuration** tab (refer to the figure, GUI General Settings Page, below).
2. Click the **General Settings** page.
3. Click either the **Enable** or the **Disable** check box under **Secure Manager** to enable or disable security.

   The GUI will present the password box.
4. Enter the security password (the password used when downloading the permissions file to the array, refer to Assigning Security on page 26).
5. Click **Done** (the new settings will take effect immediately).

Refer to the GUI help for additional information about enabling or disabling security.

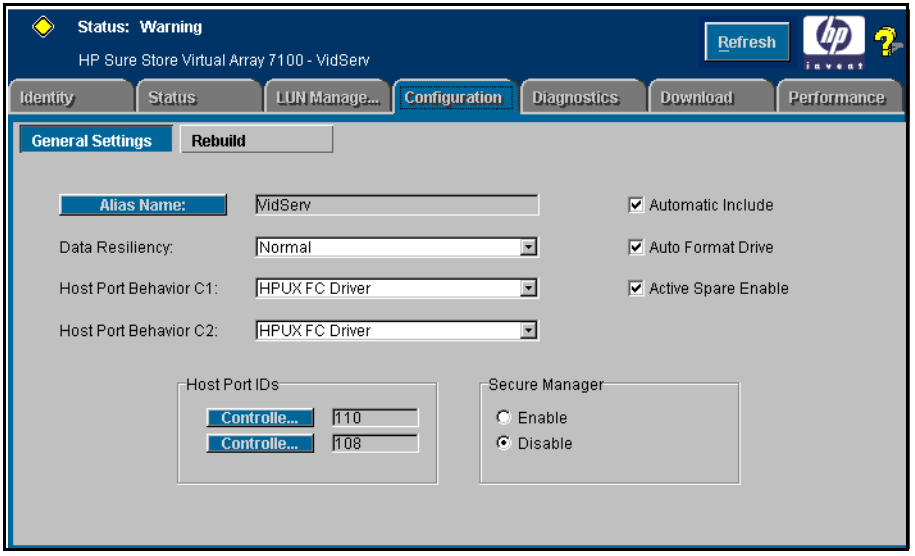


Figure 2 GUI General Settings Page

Copying Permissions

When a LUN is created using the GUI, permissions can be assigned to that LUN by copying the permissions of any existing LUN to the new, or an existing, LUN. If a LUN does not exist with the desired permissions, permissions must be created using the armsecure command (refer to Assigning Security on page 26). To copy permissions to a LUN, perform the following steps:

1. Click the **LUN Management** tab (see LUN Management Page on page 38).
2. Click either the **Logical LUNs** or the **Business Copy** page (depending on the type of LUN being created).
3. Click a **LUN ID** from the numbered list on the left side of the screen.
4. Click the **Permissions** button.
   The LUN Permissions screen will be displayed.
5. Enter a LUN number of the LUN that has permissions that you want to copy (Copy permissions from LUN); then, enter the number of the LUN you want to copy those permissions to (Set them onto LUN); and finally, enter the array security password (the password used to download permissions, refer to Setting Security Permissions on page 31).
6. Click **OK**.

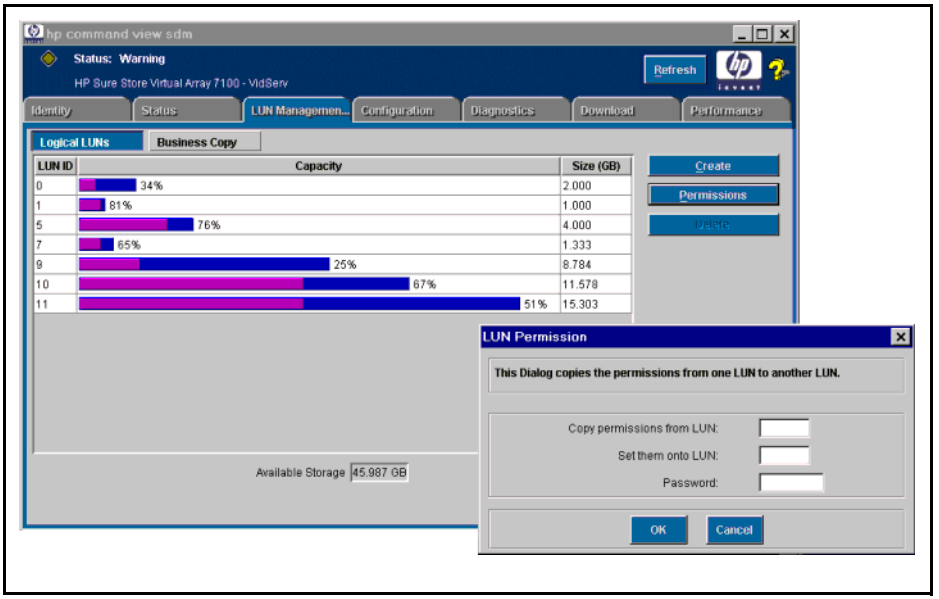


Figure 3 LUN Management Page

5 USING THE VIRTUAL FRONT PANEL

Overview

This chapter describes the security management functions that can be performed using the Virtual Front Panel (VFP). These operations include resetting the password, enabling and disabling security, and view the security mode to determine if it is enabled or disabled.

The Virtual Front Panel is a set of special commands in the array that are accessed through the RS-232 connections on the back of the array's controllers. Access to the array's RS-232 port requires a portable PC (or terminal) and a RS-232 cable. (No special software is required for this process other than a terminal emulator, or equivalent). **This procedure can be performed while the array is on-line.**

Caution Physical security should be implemented to prevent misuse of this virtual front panel.

Connecting a PC or RS-232 Device

To use the VFP command, connect any device that supports RS-232, a portable PC, for example. To connect the portable PC, perform the following steps:

1. Connect one end of an RS-232 null modem cable to the RS-232 port on the back of either array controller (either, controller 1 or controller 2).

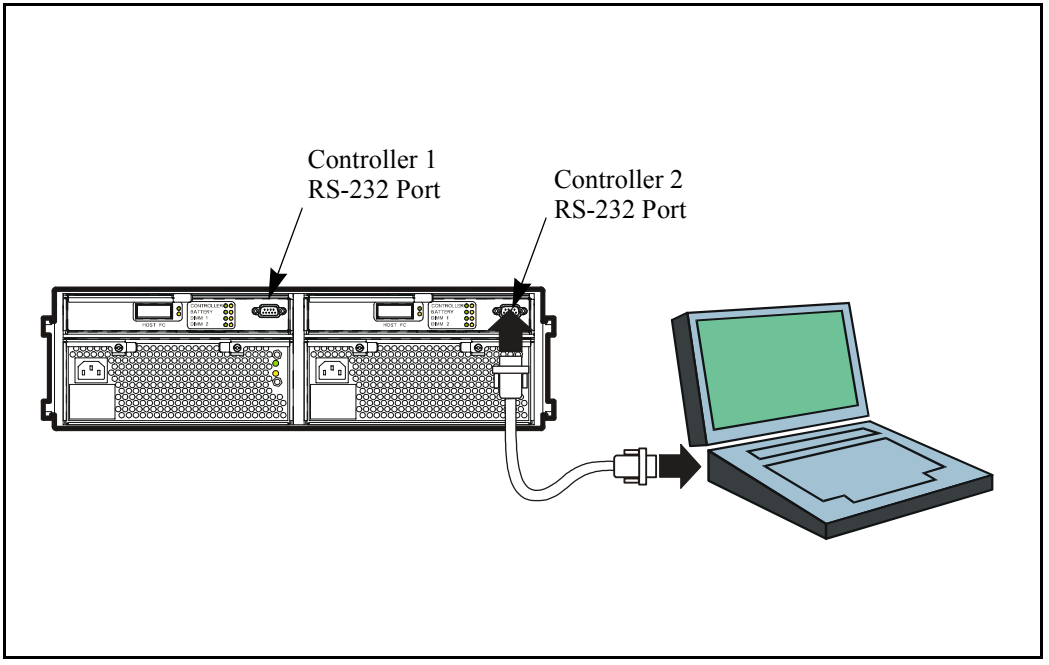


Figure 4 Virtual Front Panel Connection

2. Connect the other end of the RS-232 null modem cable to the RS-232 port on a portable PC or terminal.
3. Power up the portable PC or terminal.

The RS-232 settings should be:

- Port: Com 1 or Com 2 as appropriate
- Baud: 9600
- Data Bits: 8
- Stop Bits: 1
- FlowControl: none

4. On the portable PC initiate a terminal emulation program, such as HyperTerminal.
5. Press <return>. The array should display the `<Ready>` prompt.

Resetting the Password

If your password does not work or you have forgotten it, reset the array password to the default, "AUTORAID." To reset the password, complete the following steps (this procedure assumes that the array is powered up).

1. Connect the portable PC or other device that supports RS-232, to the array controller port (refer to Connecting a PC or RS-232 Device on page 40).
2. Enter the following command:

   vfpsecure -R

The VFP should respond:

```
Password reset to AUTORAID
```

3. Disconnect the portable PC or other device.

It is advisable to change the password from the default to a secure password, as soon as possible (refer to Changing the Security Password on page 34).

Enabling / Disabling Security

Security can be enabled for disabled using the VFP, as described below:

1. Connect a portable PC or other device that supports RS-232, to the array controller port (refer to Connecting a PC or RS-232 Device on page 40).
2. Enter the following commands to enable or disable security:

   To enable security, enter:

   ```
   vfpsecure -e
   ```

   or, to disable security, enter:

   ```
   vfpsecure -d
   ```

3. The VFP should respond:

   ```
   LUN Security Enabled
        OR
   LUN Security Disabled
   ```

4. Disconnect the portable PC or terminal.

Note **Security should not be enabled** unless the array's security table has a Config or Config/Write (CW) setting for at lease one WWN/ LUN combination. Without this setting, no host will be allowed to perform management operations on the array.

Viewing Security Mode

To determine if the array security is enabled, or disabled, perform the following steps:

1. Connect a portable PC or other device that supports RS-232, to the array controller port (refer to Connecting a PC or RS-232 Device on page 40).
2. Enter the following command to view security mode:

   ```
   vfpsecure -s
   ```

   Depending on the state, the VFP will return the following:

   ```
   Security Enabled: FALSE
          or
   Security Enabled: TRUE
   ```

3. Disconnect the portable PC or terminal.

APPENDIX A - IDENTIFYING ARRAY SERIAL NUMBER

Overview

This section describes how to obtain the array serial number using the Command View SDM software. Two methods are described here, one using the graphical user interface (GUI) and one using the command line user interface (CLUI).

When using serial number ensure that the following points are observed:

- Always enter the alpha characters of the serial number in the same case as they are presented
- A serial number is 12 characters

Note When using the array serial number to obtains a License Key for the Modular Storage Software upgrade products, if you use the serial number from the Serial Number Tag on the array chassis, it is **important** to verify the serial number using the software, one of the methods described here.

Identifying the Serial Number Using the GUI

To identify the array serial number using the GUI, launch the GUI from the launcher by clicking on the desired array ICON (for additional information on starting the GUI, refer to chapter 4). Once the interface is displayed, the serial number will be listed on the main, **Identity**, tab.

World Wide Name: xxxxxxxxxx
Serial Number: 00XY00000000
Alias: xxxxxxxxx
Device File: xxxxxxxxxx

Identifying the Serial Number Using the CLUI

The array serial number can be identified using the armdsp utility command with the -i option. To identify the serial number, enter the command:

```
armdsp -i  <hostname>
```

<hostname> is optional and is only needed it you are requesting information about an array connected to a remote host; if you are a client.

This command will provide the following response:

```
Device File: xxxx
Serial Number: 00XX00000000
World Wide Name:xxxxxxx
Alias Name: xxxxx
```

Note The armdiscover command can also be used to identify the array IDs. However, this command performs a discovery on the network which may be time consuming. The results of this command operation are displayed and also, saved to a file. The armdsp -i command displays the array ID information from the file created by the armdiscover command. An armdiscover command should be used if new array's have been added to the network.

APPENDIX B - SECURE MANAGER CLUI COMMANDS

Overview

This section describes the two Command View SDM command line user interface (CLUI), utility, commands used to set-up and manage array security feature. These commands include: armfeature and armsecure.

Command Syntax Conventions

The following conventions are used in the command syntax descriptions in this document.

Symbol	Meaning
< >	Variable
|	Select one or the other (exclusive OR)
[ ]	Items enclosed are optional
{ }	Items enclosed are required

armfeature Command

The armfeature command installs enablement licenses for additional capacity purchased for Business Copy and Secure Manager. This command also allows you to get a list of the installed enablement licenses. Entitlement licenses are purchased as separate options. With the purchase of an option, you receive a license key which is installed using this command.

armfeature {–r} <*array-id*>

armfeature {–a –f <*featurestring*> -k <key>} <*array-id*>

armfeature -?

Option	Description
-a	This specifies that the new feature as indicated by the -f parameter, with a key value as indicated by the -k parameter is to be written to the array. The, <featurestring> and the <key> values are taken from the Enablement License certificate (or as provided by the supplier)
-f <*featurestring*>	This specifies the string corresponding to the feature to be added. This string typically comes from the license certificate of the feature.
-k <key>	This specifies the key value for the new feature to be added. This string typically comes from the license certificate of the feature.
-r	This specifies that the feature table should be read from the array and displayed on the standard output.
-?	Display extended help message. Overrides all other switches.
<*array-id*>	<array-id> can be the array's serial number, World Wide Name, alias name or the Array File Name of the array. If the array is connected to a remote host then it can be accessed by prefixing it with the Host Name <HostAddr>:<array-id> where <HostAddr> can be either a DNS name or the IP address of the host.

armsecure Command

The armsecure command manages the security features of the array.

armsecure {–r –f <*filename*> -p <*password*>} <*array-id*>

armsecure {–w [-c] –f <*filename*> -p <*password*>} <*array-id*>

armsecure {–c | –e | –d } {-p <*password*>} <*array-id*>

armsecure {–n <*newPassword*> -p <*oldpassword*>} <array-id>

armsecure -?

Option	Description
-c	This specifies that the array security table in the array is to be cleared and the Secure Manager feature is to be disabled. It may be used alone, or it may be combined with the -w option to clear the table and disable Secure Manager feature just prior to a write. The user will have to explicitly enable the Secure Manager feature after using the -w -c option combination.
-d	This disables the secure manager feature of the array. The table is not altered. If the secure manager feature is disabled, all LUNs are accessible to all hosts.
-e	This enables the secure manager feature of the array.
-f <*filename*>	This specifies the file which contains (or will contain) the array security table. This file will be written to the array security table; or, the table read from the array will be written to this file. If a path is not included as part of the -f <filename> when using the armsecure -r (read) or -w (write) options, the file will be placed in the path specified by the user during the Command View SDM installation. If a path was specified at installation and no path is included with the -f <filename>, the file will be located in the default directory: opt/sanmgr/client/sbin /<filename>.
-n <*newPassword*>	This sets the password in the array to <*newPassword*>.

-p <password>	Specify the password needed to run the command. This command will present the given <*password*> to the array during the operation. The password given must match the one known to the array, or the command will fail. This is required for all forms of the command. The password <*password*> can be from one to eight characters long. Any printing character is legal, but it is best to avoid blanks and other special characters. The password “AUTORAID” is special. This password denotes the initial password as set at the factory. This is also the password set from the front panel whenever the real password is lost.
-r	This specifies that the array security table should be read from the array and written to the file specified by the –f parameter.
-w	This specifies that the array security table should be read from the file specified by the –f parameter and written to the array.
-?	Display extended help message. Overrides all other switches.
<*array-id*>	Identifies the array attached to the host. <*array-id*> can be the array’s serial number, World Wide Name, alias name or the array File Name (array path) of the array. If the array is connected to a remote host then it can be accessed by prefixing it with the Host Name <HostAddr>:<array-id> where <HostAddr> can be either a DNS name or the IP address of the host.

APPENDIX C - IDENTIFYING WWN'S

Some of the array utility commands require the World Wide Name be identified for the host's HBA. Procedures for identifying these WWN's are provided for the supported HBAs. The method used to determine the WWN depends on the operating system and the HBA.

Obtaining the WWN for Windows 4.0 and 2000 HBAs

To identify the WWN for an HBA on a Windows system depends on the type of HBA installed. Procedures are provided for QLogic (three procedures), Emulex, and Tachlite HBAs

Obtaining the WWN for QLogic HBAs

To obtain the world wide name of the host bus adapter there are three methods:

- QLview for Fibre Application
- QLconfig for Fibre Application
- QLogic's command line interface by pressing "Alt-Q" when booting up the host

QLview for Fibre Application

QLview.exe is a Windows utility that displays parameters for the host bus adapter.

Caution Care should be taken when using QLview.exe since critical settings for the host bus adapter can be modified!

To start the program, double click the QLview.exe program (Use “QLview for Fibre Setup.exe” that comes with QLA2x00 the driver software package).

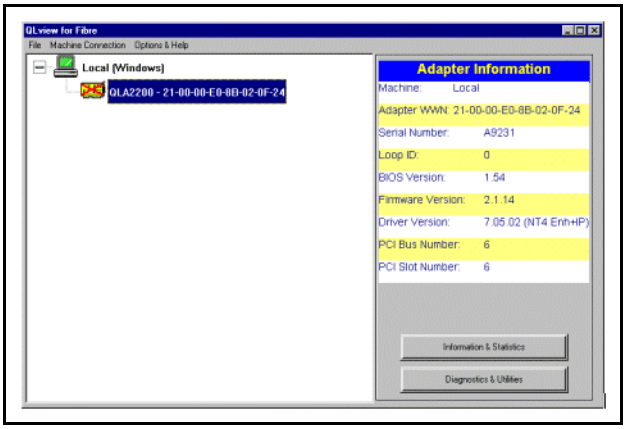


Figure 5 QLview WWN Screen

QLconfig for Fibre Application

QLconfig.exe is a Windows utility that displays parameters for the host bus adapter.

Caution Care should be taken when using QLconfig.exe since critical settings for the host bus adapter can be modified!

To start the program, double click the QLconfig.exe program (use "QLconfig's standard Setup.exe" that comes with QLA2x00 driver software package to install this utility).

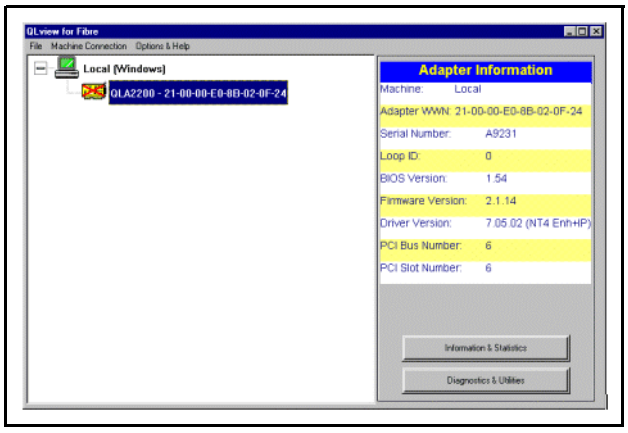


Figure 6 QLConfig WWN Screen

QLogic's Alt-Q During Boot

Pressing <Alt-Q> at bootup will start the command line utility for the host bus adapter.

Caution Care should be taken when using the command line utility since critical settings for the host bus adapter can be modified!

To obtain the World Wide Name from QLogic host bus adapter cards, use the following BIOS procedure:

1. Reboot the system.
2. When the Q-Logic card is discovered by the BIOS, press Alt-Q to enter Fast!UTIL. Once in Fast!UTIL, use arrow keys to navigate menus, and the Enter key to select.
3. Fast!UTIL will present a list of Q-Logic HBAs if there are more than one. Select the desired HBA from the list.
4. Choose **Configuration Settings** from the Options menu.
5. Now choose **Host Adapter Settings** from the Configuration Settings menu.
6. The Node WWN is displayed as 16 hexidecimal digits under the label **Adapter Node Name**. Record these digits.
7. To exit, press the ESC key three times and then select **Reboot system** to restart the boot process.

Obtaining the WWN for Emulex HBAs

To obtain the world wide name for the host bus adapter, use the **Lputilnt.exe** utility. This utility is installed when you install the LPx000 host bus adapter driver.

Caution Care should be taken when using Lputilnt.exe since critical settings for the host bus adapter can be modified!

To start the program, double click the Lputilnt.exe program (this program is usually placed in the \windows\system32 directory).

After the program starts, select Configuration data, Portname, Nodename.

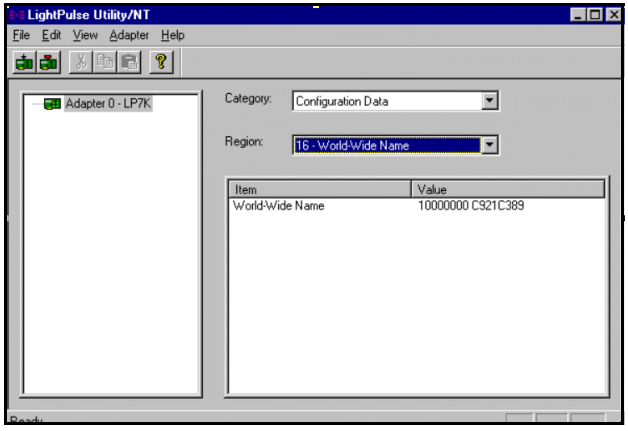


Figure 7 Lputilnt.exe Screen

Obtaining the WWN for HP Tachlite HBAs

For Tachlite HBAs the World Wide Name can be obtained in the advanced error logging feature by setting the “EventLogLever” to 4 or higher on Windows 2000. As of this writing, no method is available to obtain the WWN from the HPD8602A host bus adapter on Windows NT.

Obtaining the WWN for Linux Red Hat HBAs

The procedure for Linux is similar for many host bus adapter vendors and is OS independent on the Intel platform.

Caution Care should be taken when using the command line utility since critical settings for the host bus adapter can be modified!

To obtain the World Wide Name from QLogic host bus adapter cards, use the following BIOS procedure:

1. Reboot the system.
2. When the Q-Logic card is discovered by the BIOS, press Alt-Q to enter Fast!UTIL. Once in Fast!UTIL, use arrow keys to navigate menus, and the Enter key to select.
3. Fast!UTIL will present a list of Q-Logic HBAs if there are more than one. Select the desired HBA from the list.
4. Choose **Configuration Settings** from the Options menu.
5. Now choose **Host Adapter Settings** from the Configuration Settings menu.
6. The Node WWN is displayed as 16 hexidecimal digits under the label **Adapter Node Name**. Record these digits.
7. To exit, press the ESC key three times and then select **Reboot system** to restart the boot process.

Obtaining the WWN for HP-UX HBAs

To obtain the host bus adapter world wide name for most HP-UX run fcmsutil command without any options. The man page and output listing for the fcmsutil command is show below.

Note that device_file refers to the host bus adapter device file (/dev/fcms [12345…]) created during boot, that is independent of the target devices on the loop and not one of the raw disk devices in /dev/rdsk.

Man Page for fcmsutil

```
fcmsutil(1M)
NAME
fcmsutil -  Fibre Channel Mass Storage Utility Command
for the A3591A, A3404A, and A3636A Fibre Channel Host Bus Adapters.
SYNOPSIS
/opt/fcms/bin/fcmsutil device_file
/opt/fcms/bin/fcmsutil device_file echo remote-N-Port-ID [data-
size]
/opt/fcms/bin/fcmsutil device_file rls remote-N-Port-ID
/opt/fcms/bin/fcmsutil device_file test remote-N-Port-ID [data-
size]
/opt/fcms/bin/fcmsutil device_file read offset
/opt/fcms/bin/fcmsutil device_file lb plm|tachyon
/opt/fcms/bin/fcmsutil device_file get local|fabric
/opt/fcms/bin/fcmsutil device_file get remote N-Port-ID
/opt/fcms/bin/fcmsutil device_file get_lgn N-Port-ID
/opt/fcms/bin/fcmsutil device_file reset
/opt/fcms/bin/fcmsutil device_file read_cr
/opt/fcms/bin/fcmsutil device_file lgninfo_all
/opt/fcms/bin/fcmsutil device_file stat
/opt/fcms/bin/fcmsutil device_file disable
/opt/fcms/bin/fcmsutil device_file enable
DESCRIPTION
The fcmsutil command is a diagnostic tool to be used for the A3591A,
```

A3404A, and A3636A Fibre Channel Host Bus Adapters. This command provides the ability to perform Fibre Channel Test and Echo functionality, provides the ability to read the card's registers, etc.

This command requires the use of a device file to indicate the interface over which the requested command needs to be performed. fcmsutil can be used only by users who have an effective user ID of 0. Some of the options require detailed knowledge of the device specific adapter.

Options

fcmsutil recognizes the following options as indicated in SYNOPSIS. All keywords are case-insensitive and are position dependent.

Hewlett-Packard Company - 1 - HP-UX Release

10.20: November 1997

Example of Running fcmsutil

A sample listing for fcmsutil using a C200 workstation running HP-UX 11.0 is shown below:

```
# sys ./fcmsutil  /dev/fcms0
  Local N_Port_ID is = 0x000001
  N_Port Node World Wide Name = 0x1000001083B8AF21
  N_Port Port World Wide Name = 0x1000001083B8AF21
  Topology = IN_LOOP
  Speed = 1062500000 (bps)
  HPA of card = 0xF2FFC000
  EIM of card = 0xFFFFFFFF
  Driver state = READY
  Number of EDB's in use = 0
  Number of OIB's in use = 0
  Number of Active Outbound Exchanges = 1
  Number of Active Login Sessions = 2
```

INDEX